Michigan Journal of International Law

Volume 24 | Issue 3

2003

Yahoo! Cyber-Collision of Cultures: Who Regulates?

Horatia Muir Watt
University of Paris I

Follow this and additional works at: https://repository.law.umich.edu/mjil

 Part of the Conflict of Laws Commons, Internet Law Commons, Jurisdiction Commons, and the Science and Technology Law Commons

Recommended Citation

Horatia M. Watt, *Yahoo! Cyber-Collision of Cultures: Who Regulates?*, 24 MICH. J. INT'L L. 673 (2003).
Available at: https://repository.law.umich.edu/mjil/vol24/iss3/2

This Article is brought to you for free and open access by the Michigan Journal of International Law at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Journal of International Law by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

YAHOO! CYBER-COLLISION OF CULTURES: WHO REGULATES?

*Horatia Muir Watt**

An interesting aspect of cyberspace is the role it is playing in reviving the conflict of laws in the international arena—long relegated to quasi-oblivion in the U.S. experience[1] and now, too, a dying species in Europe, where private international law is now largely devoted to the

* Professor at the University of Paris 1 (Panthéon-Sorbonne), Co-director, Institute of Comparative Law, Paris (UMR de droit comparé, Paris I – CNRS); Secretary General of the "Revue critique de droit international privé"; Regular visitor at the University of Texas at Austin.

1. An important exception concerns conflicts of economic regulation, such as in the fields of securities or antitrust, which are more properly considered issues of prescriptive jurisdiction. For the distinction between the conflict of laws and prescriptive jurisdiction, see *infra* note 11.

interpretation of Community instruments.[2] Few and far between are the cases in which European courts are called upon to determine the law applicable to truly international issues arising in the real world[3]—and even then, they tend to be confined to very specific categories of litigation, such as in the field of family law, where they are clearly linked to the continuing use of nationality as a connecting factor in countries which are now home to large immigrant populations.[4]

However, while some of the conflicts now arising in cyberspace bear a familiar aspect, such as those arising in the course of electronic commerce, and require little more than mere technical adjustment of rules or methods applicable in analogous real-world situations,[5] a growing number of conflicts involve clashing fundamental public values in the international arena. These are typically cases in which freedom of expression, particularly as protected by the First Amendment of the U.S. Constitution, collides with the protection of concurrent values in States where information deemed offensive is made available. Of course, regulatory conflicts involving the clash of public values also take place in the real world, where publications or broadcasts originating in a foreign jurisdiction may also be perceived to contain material offensive to fundamental values in the receiving State, which may then take defensive or retaliatory measures.[6] However, if the cultural stakes appear

2. Most European case law concerns the implementation of Council Regulation 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 2001 O.J. (L 12) 1. The 1980 Rome Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, 1972 J.O. (L 299) 32, as amended by 1990 O.J. (C 189) 2, which gives rise, relatively infrequently, to issues of interpretation, is not (as yet) a Community instrument. The rise of international commercial arbitration has removed much international contract litigation from European courts.

3. The term "real world" is used here in opposition to cyberspace.

4. Case law concerns adoption of children issuing from States which either do not recognize or expressly prohibit adoption, although, in France at least, recent legislation seems to have put an end to litigation. *See* C. CIV. arts. 370–3 to 370–5 (Fr.). Another source of litigation relates to the effect to be given to Muslim unilateral marriage repudiations. In France, the impact of the European Convention on Human Rights remains uncertain on this point. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221.

5. Such conflicts concern the validity of electronic signatures, consumer protection, or advertising practice. Traditional territorial connecting factors may require adjustment. *See, e.g.*, Paul Lagarde, *La Loi du le Février 2001 Relative à l'Adoption Internationale: Une Opportune Clarification*, 2001 REVUE CRITIQUE DE DROIT INTERNATIONAL PRIVÉ 774, 776–77 (Proposals of the *Groupe européen de droit international privé* on the reform of article 9 of the Rome Convention on conflicts relating to requirements for formal validity, session of September 21–23, 2001).

6. For a rare example of a "real-world" transAtlantic conflict involving freedom of expression and defamation, see the decision of the highest French civil law court, Cass. 1e Civ., Jan. 14, 1997, *Soc. Gordon and Breach Science Publishers c. Association The American Institute of Physics*, 1997 REVUE CRITIQUE DE DROIT INTERNATIONAL PRIVÉ 504 (Jean-Marc Bischoff). Here, for instance, the court ordered the seizure of the publication in France.

infinitely higher in cyberspace—a conclusion supported by the violence of reactions which the *Yahoo!* decision generated on both sides of the Atlantic[7]—it may well be that these conflicts implicate an additional ideological dimension unparalleled outside the Internet. Indeed, the *Yahoo!* litigation seems to point to the limits of analogy between cyberconflicts and their real-world counterparts.

This Article furthers this comparison of cyberconflicts and the real world, attempting to ascertain what lessons, if any, can be drawn from it. Part I of the Article explores the interests at stake in cyberconflicts and the relationship between technology and the law. Part II uses the French *Yahoo!* court's decision to show that real-world conceptions of prescriptive jurisdiction retain their legitimacy in cyberspace. Finally, Part III notes that the prospect of near perfect compliance offered by Internet technology provides the opportunity to engineer mature, well-calibrated solutions to international regulatory conflicts, which might then even serve as a model in the real world.

I. AN OVERVIEW OF INTERNATIONAL CYBERCONFLICTS ISSUES

A. *Prescriptive Jurisdiction in the International Context*

Cases such as *Yahoo!*,[8] *CompuServe*,[9] or more recently the *Barron's*

---

7. For an example of the (needlessly) aggressive comments by Ben Laurie, see Ben Laurie, *An Expert's Apology* (Nov. 21, 2000), *available at* http://www.apache-ssl.org/apology.html (denouncing the French court's ruling as "half-assed and trivially avoidable"); *see also* Joel Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 261, 277–78 (2002) (critiquing Laurie's response to the ruling).

8. UEJF et LICRA v. Yahoo! Inc., Ordonnance Référé, T.G.I. Paris, Nov. 20, 2000, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm; *see also* Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, 145 F. Supp. 2d 1168, 1179 (N.D. Cal. 2001) (declaring the French judgment contrary to Yahoo!'s freedom of expression as protected by the First Amendment).

9. When faced with the threat of criminal prosecution, CompuServe eliminated all access to news groups that fell under Germany's antipornography laws. It then attempted to provide "filtering" software in the form of "installment mechanisms," which were designed to allow parents to prevent children from viewing indecent material. CompuServe intended this solution to demonstrate a willingness to comply with German law while committing to provide continued access to users elsewhere. German authorities, however, found the installment mechanisms insufficient because the statute outlawed the dissemination of pornography, whether distributed to adults or children. For an abundant literature in English documenting all these events, generally disapproving German regulatory claims as excessive, see Asaad Siddiqi, *Welcome to the City of Bytes? An Assessment of the Traditional Methods Employed in the International Application of Jurisdiction over Internet Activities—Including a Critique of Suggested Approaches*, 14 N.Y. INT'L L. REV. 43, 89–90 (2001); Steven M. Hanley, Comment, *International Internet Regulation: A Multinational Approach*, 16 J. MARSHALL J. COMPUTER & INFO. L. 997 (1998); Mark Konkel, Note, *Internet Indecency, International Censorship, and*

litigation,[10] exemplify the rapidly expanding category of specifically international conflicts, which, by reason of their public interest dimension, are more appropriately described in terms of prescriptive jurisdiction than in traditional "conflict of laws" terms.[11] National regulations that conflict over activities conducted on the Web express fundamental cultural values for each of the States concerned; indeed, the colliding values are very often embodied in constitutional texts, international instruments dealing with human rights, or penal legislation. Typically, an assertion of freedom of expression in the State in which the website is located clashes with restrictive legislation in the receiving State, designed to protect such values as the right of privacy, to restrict hate speech or libel, or to prohibit indecency or pornography. The free availability of information collides with the negative right of the receiving State to protect itself against outside interference, thus creating a "true" regulatory conflict: If the receiving State can prohibit the emission of information, this comes

---

Service Providers' Liability, 19 N.Y.L. SCH. J. INT'L & COMP. L. 453 (2000); Kim Rappaport, Note, *In the Wake of Reno v. ACLU: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech Online*, 13 AM. U. INT'L L. REV. 765 (1998); Kristina M. Reed, Comment, *From the great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce*, 12 TRANSNAT'L LAW. 543 (1999); Amber Jene Sayle, Note, *Net Nation and the Digital Revolution: Regulation of Offensive Material For a New Community*, 18 WIS. INT'L L.J. 257 (2000).

10. The *Barron's* decision has just been handed down by the Australian High Court. *See* Patti Waldmeir, *Regulating Cyberspace*, FIN. TIMES, Dec. 16, 2002. It ruled that Australian courts had jurisdiction to entertain a libel claim brought by an Australian businessman against Dow Jones, the U.S. publisher of the allegedly libelous material, loaded onto a server in New Jersey. *Id.*

11. Prescriptive jurisdiction is expressed in unilateral terms, allowing no room for applying foreign law. *See, e.g.*, William S. Dodge, *Extraterritoraility and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism*, 39 HARV. INT'L L.J. 101 (1998). This approach characterizes conflicts of public law, or perhaps more exactly (as far as the United States is concerned), the reach of federal legislation in the international arena. The Restatement (Third) of Foreign Relations defines prescriptive jurisdiction, leaving the conflict of laws (whether international or interstate) to the Restatement (Second) on the Conflict of Laws. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 402–03 (1986) [hereinafter RESTATEMENT (THIRD) OF FOREIGN RELATIONS]; RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 2 cmt. d (1969) (referring questions of public international law to the Restatement of Foreign Relations); *id.* § 3 cmt. c (defining "state"). Lea Brilmayer explains that the real distinction between the Restatement of Foreign Relations and the Restatement on the Conflict of Laws lies in the source of domestic law: the former deals with conflicts involving federal law while the latter concerns solely state law conflicts. Lea Brilmayer, *The Extraterritorial Application of American Law*, 50 LAW & CONTEMP. PROBS. 11, 12–13. Thus, some international conflicts are subject to choice of law under the Restatement of Conflicts, when they arise in a field such as tort, which is not subject to federal legislation. On the other hand, when a claim is governed by federal regulation, federal courts have subject matter jurisdiction, and approach conflict-of-laws situations in terms of "prescriptive jurisdiction." For the moment, at least, little thought has been given to the potential role of foreign law in the solution of regulatory conflicts in cyberspace; courts assert adjudicatory jurisdiction with a view to applying forum law.

close to interference in the regulation of activities covered by constitutional immunity in the State where the website is located; conversely, not to do so looks very much like allowing cultural expansionism. Either way, the regulatory claim of one State will appear pernicious or intrusive to the other: For example, the United States jurisdiction in which the website is located will object to any corrective action taken by the receiving State as curtailing fundamental freedom of expression, while the latter, in turn, has no reason to accept that First Amendment protection should extend to activities conducted within its virtual borders in violation of its own constitutional or criminal law. Thus, on the one hand, persons in the United States denounce European regulations restricting the content of public expression as extraterritorial meddling with democratic values;[12] on the other, the same values cause European observers to denounce the perverse race to the bottom generated by First Amendment liberalism, as neo-Nazi websites seeking safe haven relocate massively across the Atlantic.[13]

B. *How Internet Technologies Exacerbate Traditional Difficulties*

Although such conflicts can and do occur through the use of traditional media, new communication technologies have sharply exacerbated the difficulties encountered in the real world. Indeed, data circulate instantaneously over the Internet, making the damage caused by the harmful use of information potentially far greater and far more difficult to prevent than in cases of data traveling through more traditional channels. Conversely, given the ubiquity of such effects, there is a risk that multiple courts will assert jurisdiction simultaneously over activity conducted on the Web, with potentially devastating consequences in the form of overregulation and contradictory decisions. Observers frequently express fear that the mere "press of a button" suffices to subject a given activity to foreign extraterritorial jurisdiction without proper notice.[14]

---

12. Some Europeans share this reaction. *See, e.g.*, Ben Laurie, *supra* note 7. A French author recently described the French *Yahoo!* court's decision as "exorbitant." *See generally* Daniel Arthur Laprès, *L'exorbitante affaire Yahoo*, 4 JOURNAL DU DROIT INTERNATIONAL 975 (2002).

13. This is not to suggest that the flocking of Nazi websites to the United States is not also denounced in this country. *See* Lisa Guernsey, *Mainstream Sites Serve as Portals to Hate*, N.Y. TIMES, Nov. 30, 2000, at G1; Reidenberg, *supra* note 7, at 275.

14. *See, e.g.*, Robert M. Harkins, Jr., *The Legal World Wide Web: Electronic Personal Jurisdiction in Commercial Litigation, or How to Expose Yourself to Liability Anywhere in the World with the Press of a Button*, 25 PEPP. L. REV. 451 (1997). The courts themselves sometimes express similar ideas. *See, e.g.*, Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 171 (S.D.N.Y. 1997) (concluding that "no user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a website, receiving a mail exploder message, or participating in a chat room"); Jack L. Goldsmith & Alan O. Sykes, *The Internet and the*

However, if the conflict is more acute in virtual space, it is not only because of the inherent ubiquity of information and the magnified spillover effects of corrective action, but also and primarily because of the philosophical premises on which the World Wide Web is actually perceived to function, at least in the United States. For many, the Web's very architecture, which favors the free flow of information, anonymity, and geographical indeterminacy, embodies the United States' values of free expression, of which it constitutes the technological projection. Subsequently, any foreign regulatory attempt to inhibit the flow of information is considered not only as a violation of First Amendment immunity, but as vitiating the democratic values embedded in the structure of the Web.[15] Typically, the French decision in *Yahoo!* drew criticism in the Unites States as a claim to "control thinking" in cyberspace.[16]

C. *A Paradox: Technology in Lieu of Enforcement*

At first glance, therefore, cyberconflicts might seem to have little to teach private international law in the real world, and as little to gain from recourse to traditional analytical tools. In view of the acute ideological charge of international conflicts involving fundamental freedoms, nothing appears to prevent litigation from escalating into primitive *Laker*-type judicial warfare,[17] where the winner is clearly the most effective enforcer.[18] It may, however, be time to stop and consider that the free-flowing architecture of the Web results from man-made software, whereas real world constraints are given or, at least, tend to be perceived as inexorable. To what extent does this difference shed any light on the way in which *Yahoo!*-type conflicts could be managed? Paradoxically,

---

Dormant Commerce Clause, 110 YALE L.J. 785, 790–93 (2001) (discussing the *Pataki* court's application of the Dormant Commerce Clause to state criminal laws concerning Internet transmissions of pornography to minors).

15. Reidenberg, *supra* note 7, at 272–75.

16. *See infra* text accompanying note 24.

17. The complex *Laker Airways* antitrust litigation presents a notorious example of transAtlantic judicial warfare, in which British and U.S. courts exchanged anti-suit and counter-anti-suit injunctions to protect prescriptive jurisdiction. Laker Airways, Ltd. v. Pan Am. World Airways, 235 U.S. App. D.C. 207 (1984); *see also* ANDREAS F. LOWENFELD, INTERNATIONAL LITIGATION AND THE QUEST FOR REASONABLENESS 5 (1996) (analyzing this "struggle over jurisdiction").

18. The respective strengths of the contenders would thus appear to be measured exclusively in real-world terms; enforcement will involve the seizure of the defendant's assets located within the regulating State, diverse forms of injunctive relief, or more troubling forms of pressure applied directly on network participants. On the real dangers of exerting pressure through censorship on network participants, see Reidenberg, *supra* note 7, at 277, warning against the danger of overrating the chilling effect of State regulation of Internet communications, when far more troubling avenues are available. These may include "denial-of-service" attacks with a view to shutting down foreign websites, creation of viruses to cripple foreign computers, and more generally deployment of cyberenforcement agencies. *Id.*

whereas conflicts involving the exercise of free expression over the Web initially might appear infinitely more difficult to resolve than their real-world counterparts, the converse is probably true. This Article shows that, if man-made technology shapes cyberspace, it makes achieving a balanced solution of international regulatory conflicts potentially far easier on the Web than in geographical space. This is simply because transnational compliance is clearly more attainable than in the real world, through the use of technology itself. A regulating State now has the means to prevent given data from being made accessible within its borders simply by ensuring that adequate gateway software is put into place;[19] technology readily bypasses slippage, cost, and all the familiar difficulties generally linked to international enforcement of legislative prescriptions or judicial decisions in the real world. This means, in turn, that it is all the more important that States assert prescriptive jurisdiction only when it is clearly reasonable to do so, since unjustified technological interference with the free flow of information in cyberspace would be both destructive and counterproductive. To the extent that technology lends greater credibility to regulatory claims over cyberspace than in the real world, great care should be taken to see that such claims are properly calibrated.

D. *Two-Way Relationship Between Law and Technology*

This is where the real world may have much to teach about the relationship between law and technology. It has been witness in recent times to the gradual common acceptance of the effects doctrine[20] as a legitimate basis for international prescriptive jurisdiction. Similarly, the exercise of regulatory jurisdiction based upon the effects suffered within the forum State seems eminently reasonable in cyberspace. Adopting this approach would optimally regulate cross-border flows of information by allowing restrictions only when the regulating State has a substantial interest in preventing the flow of data within its territory, and only to the extent necessary to implement the protective policy involved. Technology increases the credibility of regulatory claims, but it also allows a State asserting prescriptive jurisdiction to adjust the scope of such claims functionally, so as to allow only those restrictions strictly necessary to prevent harm within its borders. The French *Yahoo!* court fully understood this complex relationship between law and technology on the Web.

19. The difficult question of who should bear the burden is discussed in the text below. *See infra* Section III.B. Here, we focus on the technical possibility of ensuring near-perfect compliance.

20. The "effects" doctrine will be described below. *See infra* Section II.B.1. This doctrine allows the regulating State to exercise prescriptive jurisdiction over foreign conduct with impacts on interests located within its borders.

It asserted regulatory jurisdiction on the basis of offensive effects of the data accessible on the Yahoo! Inc. website within French territory, but ordered that the data be made unavailable only to French-based internauts. The constraints it imposed on the free flow of information in the name of the fundamental values of French society did not affect access to that website from any other territory. Virtual space thus evidences a two-way relationship between international jurisdiction and technology. On the one hand, technology can make the assertion of jurisdiction effective to an extent unattainable in the real world. Conversely, proper definition of the limits of prescriptive jurisdiction is crucial to the coherence of State regulation of cyberspace.

II. LESSONS FROM THE REAL WORLD: THE LEGITIMACY OF INTERNATIONAL "EFFECTS" JURISDICTION

To show that real world yardsticks retain their legitimacy in cyberspace, this Part first examines the "separatist" claim that the use of a borderless medium in some way modifies the bases of regulatory jurisdiction as designed for the real world. Relayed by conventional wisdom about the structure of cyberspace, the separatist claim draws normative conclusions from the freedom with which data can circulate over the Web.[21] Because the Internet provides a technical medium for unfettered expression, restrictive regulation is made to appear illegitimate—a denial of the democratic values it embodies.[22] In the international arena, the perception of Internet architecture as a given also creates important implications for the solution of regulatory conflicts. Thus, the free flow of information similarly gives rise to implicit normative conclusions regarding the allocation of international prescriptive jurisdiction. Assertion of regulatory authority by States seeking to impose restrictions on freedom of expression is seen as incompatible with the very structure of cyberspace. But it will be shown that such a perception reverses the proper relationship between law and technology, allowing separatist values to dictate the scope of international jurisdiction. Indeed, Section A shows that, on closer scrutiny, the design of the Internet depends entirely on the ideological choices that dictate technological development. So, as Section B demonstrates, no plausible reason exists to displace the yardsticks of regulatory authority as defined in the real world.

---

21. *See* Goldsmith & Sykes, *supra* note 14 (discussing conventional wisdom about cyberspace found in the cases).

22. Reidenberg, *supra* note 7, at 273–74.

A. *Cyberspace as Ideology*

This Section shows that the separatist claim is sustainable only insofar as the borderless quality of the Internet is accepted as a given. As Lawrence Lessig has demonstrated, the development of filtering technology for purely commercial purposes belies this premise, exposing conventional wisdom about the Web as ideology, not fact.

1. The "Safe Haven" Argument

As reactions to *Yahoo!* and similar litigation illustrate, many believe that the very design of the Internet carries strong normative implications for solutions of regulatory conflicts. In a borderless medium, claims by a State to restrict the flow of data perceived to affect welfare within its territory appear to lose their real-world legitimacy. Thus, when activities covered by freedom of expression at the place the website is located are considered elsewhere to undermine concurrent fundamental values such as privacy or the prohibition of hate speech, the defendant systematically invokes the "safe haven" argument. As Joel Reidenberg explains, the fact that the Web, instead of some other, more traditional medium, carries the cross-border effects of the regulated activity would seem to modify accountability, as though activities in borderless space somehow surmount local laws.[23] Favoring the free flow of data, the Internet is seen as conferring on expression carried through its medium a status that remains mysteriously beyond the thrust of the laws of the States in which users access the information. Thus, the geographical indeterminacy of cyberspace seems to set aside the principles governing prescriptive jurisdiction in the real world.

The explanation resides in the fact that the technological architecture of the Web clearly embodies values expressed in the First Amendment, making the very idea that the free movement of data might encounter the regulatory claims of other States seem an anathema to the Web's ideological foundations. Thus Ben Laurie, computer expert consulted by the French *Yahoo!* court, states that "what is being fought over is literally what people think. No one should be able to control what I know or what I think . . . The Internet is pure information."[24] When, in the more recent *Barron's* litigation, the Australian Supreme Court ruled that Australian courts had jurisdiction to hear a claim that information loaded on a New Jersey server was libelous under Australian law, the demise of the Internet as a democratic forum of free expression was widely predicted.[25]

---

23. *Id.* at 272–75.
24. Laurie, *supra* note 7.
25. Waldmeir, *supra* note 10.

This perception of the relationship between law and technology extends beyond the international sphere. Similar attitudes exist in domestic litigation within the United States over the thrust of the Dormant Commerce Clause and in First Amendment cases. In the Dormant Commerce Clause context, restrictive regulation is perceived as unduly burdening interstate electronic commerce.[26] Where freedom of expression is involved directly, it is perceived as preempting restrictive regulation based on concurrent values, such as the protection of minors from access to pornography.[27] Whereas such a claim would hardly seem credible in a real-world context, free expression guaranteed by the First Amendment appears to acquire a worldwide immunity, to the point of excluding the regulatory claims of the State in which harmful effects are suffered. What about the Web makes such an argument appear sustainable?

2. Technology as a Given

Conventional wisdom about the Internet tends to present geographical indeterminacy and the free flow of data as givens. As Jack Goldsmith and Alan Sykes have shown, in the context of Internet litigation within the United States, courts looking for "facts" about the Web tend to find that the ubiquity of information, and the corollary risk of overreaching countervailing measures, justify giving precedence to the freedom of expression.[28] Claims about the architecture of the Internet include universal availability of information, absolute indeterminacy of geographical location and other identity factors, and indefinite exposure to liability under restrictive regulation, whatever real links exist between the exposed activities and the regulating State.[29] Correlatively, regulation itself is perceived as illegitimate. In other words, since the Web knows no frontiers, data must circulate freely; as no natural frontiers exist, States may not erect them artificially. This perception of the architecture of the Web clearly impacts the exercise of prescriptive jurisdiction in the international arena. Those who believe that the Internet represents

26. *See, e.g.*, Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997); *see also* Goldsmith & Sykes, *supra* note 14, at 790–94 (discussing relevant case law); *id.* at 802–08 (applying economic analysis of cross-border burdens to Internet communications).

27. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) (invalidating two provisions of the federal Communications Decency Act of 1996 due to the First Amendment); Am. Civil Liberties Union v. Reno, 217 F. 3d 162 (3d Cir. 2000) (upholding order preliminarily enjoining enforcement of the federal Child Online Protection Act due to likelihood that the Act violated free speech guarantees).

28. Goldsmith & Sykes, *supra* note 14, at 788.

29. Reidenberg, *supra* note 7, at 272–75.

undifferentiated space, find any attempt to introduce "zoning"[30] within its confines intolerable.

As such, arguments that tie up man-made space and law are not so unusual. Thus, free markets have obvious normative implications for the legitimacy of regulatory claims; as shown by litigation involving the Dormant Commerce Clause in the United States or the market freedoms in the European Union, risks of double burdens or overregulation are frequently invoked to limit prescriptive jurisdiction in such a context.[31] No one doubts that deliberate policy shapes free markets or that creating an economic space for the unfettered movement of goods and services requires constraints on regulatory jurisdiction. Curiously, however, the architecture of the Internet is not generally seen as being the product of software. As Ben Laurie's statement shows, the Internet is perceived as a natural space; because the Web enables the free cross-border flow of data, such a state of affairs should, as the argument goes, be taken as a *fait accompli*—an inexorable fact dictating regulatory abstention in the international arena.

3. Normative Implications of Filtering Technology

Although the vision of cyberspace as a borderless natural space still appears to carry weight, commentators also increasingly perceive it as delusional.[32] The rapid development of filtering and "zoning" techniques, now used for purely commercial reasons such as targeting advertising to a particular public, provides clear evidence that geographical indeterminacy on the Internet is not inevitable, but results from ideological choice. As the current state of Internet technology demonstrates, the borderlessness of the World Wide Web does not represent an intractable given. Concluding otherwise allows technology to disguise policy choices. We should ultimately reject the "safe-harbor" defense as having no more relevance than in the real world, precisely because the design of the Web is what we make it; if information flows freely, it is because we allow it to do so. Much of the conventional wisdom about the functioning of the Web grew out of the initial state of the art, under which "zoning" techniques were inconceivable. Improved technology, designed to identify various categories of users, means that claims of the ubiquity of information accessible on the Web, whether due to the inherent nature of the medium or to its accidental evolution, no longer ring true. This entails a

30. Lawrence Lessig & Alan Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395 (1999) (coining the expression "zoning").

31. For the impact of the "double burden" argument in the European Union, see JUKKA SNELL, GOODS AND SERVICES IN EC LAW: A STUDY OF THE RELATIONSHIP BETWEEN THE FREEDOMS (2001).

32. *See* Lessig & Resnick, *supra* note 30; Reidenberg, *supra* note 7.

fundamental consequence regarding the allocation of regulatory authority in cyberspace. If the Internet is not naturally borderless, then real-world yardsticks for the exercise of prescriptive jurisdiction retain their legitimacy.

B. *Legitimacy of Real-World Yardsticks for Prescriptive Jurisdiction*

This Section demonstrates that the regulating State may legitimately impose international "zoning" to protect itself from the effects of information made available elsewhere and perceived to be harmful. This requires showing that effects-based jurisdiction does not necessarily entail conflicting regulatory burdens, which would arise if national courts simultaneously asserted prescriptive jurisdiction over the same conduct "at the press of a button." New filtering technologies lessen the risk of accidental spillover and increase the means for preventing much-feared overregulation.

1. Effects and Targeting

Since the new types of regulatory conflicts emerging in cyberspace involve public values,[33] courts have tended to reason in terms not of conflict of laws but of prescriptive jurisdiction, using criteria developed in real-world clashes of public economic regulation.[34] In such cases, contemporary practice on both sides of the Atlantic seems to have converged more or less from a "place-of-conduct" rule to an "effects" test.[35] Indeed, recent applications of economic analysis to the conflict of laws have shown that the "effects" test seems to make the best sense in terms of

---

33. Indeed, globalization seems to have given rise to a new taxonomy of international conflicts—whether through increased interconnectedness or the use of new technologies—which now include regulatory clashes with strong public law components. On this new category of international conflicts, hitherto identified with conflicts of economic regulation, see Jurgen Basedow, *Conflicts of Economic Regulation*, 2 AM. J. COMP. L. 423 (1994); *see also* Jurgen Basedow, *Souveraineté territoriale et globalisation des marchés: le domaine d'application des lois contre les restrictions de concurrence*, 264 RECUEIL DES COURS 9 (1997).

34. *See supra* note 14.

35. On the three different tests (conducts, effects, and balancing of interests) which appear in U.S. practice, and their relationship to tests used in choice of law, see William Dodge, *Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism*, 39 HARV. INT'L L.J. 101 (1998). While the balancing test proposed by section 403 of the Restatement (Third) of Foreign Relations was not rejected in the Supreme Court's most recent ruling, Hartford Fire Ins. Co. v. California, 113 S.Ct. 2891 (1993), it is clear that the way in which the test was implemented in that case comes very close to reinstating the "effects" test. The latter seems to have been adopted in fact, if not explicitly, by the Court of Luxembourg in the *Woodpulp* case. Case 89/95, Woodpulp, 1988 E.C.R. 5193. For a discussion of section 403, see LOWENFELD, *supra* note 17, chs. 2, 3.

global welfare[36]—a consideration which should bear a particular weight in the present context of worldwide interplay of regulatory authority. Where conflicts arise in cyberspace, courts both in Europe and the United States have asserted personal jurisdiction on this basis, and have then proceeded to apply forum law.[37] "Substantial effects" within the regulating State generally justify prescriptive jurisdiction, whether they arise in the real world or cyberspace.[38] To establish personal jurisdiction over the defendant, however, deliberate targeting may be both necessary and sufficient.[39] Using targeting as a yardstick has enabled courts of various countries to exercise jurisdiction sufficient to incriminate hate speech, indecency, libel, invasions of privacy, and copyright violations.[40]

"Targeting" involves the difficult task of discriminating between active and passive websites,[41] requiring considerable thought as to the

---

36. *See, e.g.*, Joel Trachtmann, *Economic Analysis of Prescriptive Jurisidction and Choice of Law*, 42 VA. J. INT'L L. 1, 34–41 (2001). However, Andrew Guzman argues that the effects test as such will not guarantee global efficiency, since a State regulating on that basis will have taken into account exclusively local costs and benefits. As a result, a globally optimal transaction (i.e., a transaction which increases global welfare) may nevertheless be regulated restrictively by any State in which its harmful effects are in excess of its local benefits, irrespective of its positive impact elsewhere. Andrew Guzman, *Choice of Law: New Foundations*, 90 GEO. L.J. 883, 897 (2002). To be allowed under the effects test, argues Guzman, a given transaction must not only increase global welfare but be perceived as optimal in all of the States in which it generates effects. *Id.* at 906–08. Although this argument is convincing, it is also clear that a global calculus of costs and benefits could only be carried out within a cooperative framework. Failing that, the (second) best yardstick of prescriptive jurisdiction is still the one that allocates legislative authority to the States with the greatest incentive to allow or refuse a given transaction, even if incentive must rhyme here with self-interest.

37. For an analysis of the case law, see Reidenberg, *supra* note 7, at 269–71. In the *Yahoo!* case, French personal and prescriptive jurisdiction was justified either under the territorial yardstick of Code Pénal article 113-2 (because the infraction presumptively took place on French territory since the harm, an element of the infraction, took place there), or the personal criterion of the victims' French nationality under Code Pénal article 113-7. Both yardsticks endorse the "effects" test.

38. Under section 403(2)(a) of Restatement (Third) of Foreign Relations Law, one of the tests of reasonableness to be applied to international prescriptive jurisdiction lies in the "substantial, direct and foreseeable effect [of the activity] upon or in the territory." RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 403(2)(a).

39. Courts seem to use a "sliding scale" which requires either interactivity or purposeful availment in order to establish the minimum contacts required for the assertion of personal jurisdiction. For a very complete analysis of the case law on this point, see Siddiqi, *supra* note 9, at 72.

40. For an analysis of U.S. cases, see Reidenberg, *supra* note 7, at 269–71 and see *infra*, the text accompanying notes 45–48. In addition, on the trend toward an "effects" test in cyberspace, see Michael Geist, *The Legal Implications of the Yahoo! Inc. Nazi Memorabilia Dispute*, JURISCOM.NET (Jan.-Mar. 2001), *at* http://www.juriscom.net/en/uni/doc/yahoo/geist.htm.

41. The distinction is not an easy one—any more than is demonstrating purposeful available for jurisdictional purposes in real-world situations. For example, in *Panavision International*, the court required "something more" than a passive website to show that activity

weight to be given to various factors such as language, which may or may not be significant, according to the specific circumstances of each case.[42] However difficult the courts' task in defining the effects which legitimate the international assertion of prescriptive jurisdiction, targeting means that data deliberately made accessible within the forum State can lead to criminal liability there, even if it receives legal protection in the place of conduct. The fact that it is protected "at home," is no more a valid jurisdictional defense in cyberspace than it would be in the real world. Although defendants characterize such assertions of prescriptive jurisdiction as "imperialism," it is hardly necessary to show that once the ideological arguments linked to the architecture of the Web are set aside, there is nothing "exorbitant" about extraterritorial regulation on the basis of conduct targeted into the forum territory.[43] In this respect, the French court's "extraterritorial" injunction in the *Yahoo!* case is by no means exceptional: in the United States, the *Playboy* court required a website located in Italy to make material published under the United States trademark, "Playmen," inaccessible to users in the United States;[44] in *Nat'l Football League v. TVRadioNow Corp.*, a Canadian website was preliminarily enjoined from transmitting copyrighted programming into the United States;[45] the *People v. World Interactive Gaming Corp.* court ordered a casino based in Antigua to cease offering gambling over the

---

is targeted at the forum state. 141 F. 3d at 1320–22 (quoting Cybersell Inc. v. Cybersell Inc., 130 F.3d 414 (9th Cir. 1997) and distinguishing it due to a lack of targeting). In *Cybersell*, two corporations, organized in different states, used identical trade names on the Internet without specifically intending to injure each other. In Zippo Mfg. v. Zippo Dot Com, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997), Judge McLaughlin explains:

> At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer.

Id. It is of course the defining of the "middle ground" which creates difficulty. *See* Siddiqi, *supra* note 9, at 72. Courts seem to use a "sliding scale" which requires either interactivity or purposeful availment in order to establish the minimum contacts required for the assertion of personal jurisdiction.

42. The *Yahoo!* case itself illustrates this difficulty. That the website targeted a French-speaking public seems clear from the use of French-language advertisements. But if using French in California evidences the targeting of users in France, it hardly follows that the use of English necessarily targets, say, an Australian public.

43. At least one French author strongly disagrees. *See* Laprès, *supra* note 12, 993–95.

44. Playboy Enters. v. Chuckleberry Publ'g, 939 F. Supp. 1032 (1996).

45. 53 U.S.P.Q.2d 1831 (2000).

Web to New Yorkers;[46] and in *Panavision International LP v. Teoppen*, an Illinois resident was held to be subject to suit in California for registering a domain name in Illinois, when his activity was directed to the forum state.[47]

2. "Zoning" Limits Ubiquity, Negating the "Notice" Argument

As we have already seen, the objection immediately raised in Internet litigation is the "notice" argument, linked to the alleged ubiquity of information on the Web. Because given content may come under the definition of libel or hate speech in innumerable jurisdictions, there appears to be a danger of massive overregulation; although the risk of conflicting regulatory burdens also exists in the real world, conventional media do not create the same likelihood of widespread unintentional effects. Two objections show the fallacy of this notice argument, one normative, the other technological.

First, prescriptive jurisdiction carries the same limits in cyberspace and the real world—the State cannot legitimately exercise jurisdiction over activities on the basis of effects that either do not specifically target its territory or remain insubstantial.[48] The distinction, now gaining ground in court practice, between interactive and passive websites, responds to this idea, linking the legitimacy of regulatory claims to the fact that information has been made deliberately accessible in the forum State, as in the *Yahoo!* case.[49] As filtering technology improves, the risk of accidental spillover decreases: "zoning" techniques lessen the force of the argument that effects can accidentally arise anywhere. The flow of information can be mastered in cyberspace, in the same way that one can avoid sending publications via traditional media deliberately into another State. This is precisely the thrust of the French *Yahoo!* decision, which took pains to check the feasibility of limiting access in France of material loaded on the California website; if the offensive data is nevertheless made accessible in France, it cannot be the result of an accident. As the *Yahoo!* court itself recognized, this does not entirely rule out seepage, particularly as engineered by third parties. However, it has been pointed out that it would be fair to provide a "reasonable efforts" defense, to

46. 714 N.Y.S.2d 844 (N.Y. Sup. Ct. 1999).

47. 141 F.3d 1316 (9th Cir. 1998).

48. The targeting of the regulating State's "territory" is of course metaphorical. In many cases, the stigmatized activity attempts to affect the forum State's economic interest.

49. *See, e.g.*, Zippo Mfg. v. Zippo Dot Com, 952 F. Supp. 1119, 1123–24 (W.D. Pa. 1997); *see also supra* note 5. For an interesting critique of the interactivity yardstick, see Siddiqi, *supra* note 9, at 74, pointing out that the commercial value of a website is not necessarily dependent upon its interactivity.

protect service providers who have taken care to comply with legislative restrictions in targeted States.[50]

Secondly, using zoning techniques, while limiting accidental seepage of information, also allows courts to adjust the restrictions required by their local law to mitigate harmful effects without overreaching. Contrary to popular belief, overregulation can be mastered more easily in cyberspace than in the real world, which provides far less opportunity for the fine-tuning of regulatory jurisdiction. Courts can limit the restrictive effect of regulation and incriminations to activities that directly affect welfare within their own jurisdiction. Unnecessary regulatory spillover can be avoided if restrictions to the free flow of information, for example, can be limited to a given set of geographically located users. Thus, the French *Yahoo!* court ordered that the content of the contentious website should be prevented from being accessed in France, where it was illegal, without affecting its accessibility elsewhere. In other words, in exercising prescriptive jurisdiction to apply a penal statute to foreign conduct on the basis of harmful effects suffered in France, the *Yahoo!* court made sure that the impact of its own corrective action was exactly adjusted to those effects. As little as five years earlier, at the time of the *CompuServe* litigation, striking a similar balance proved less easy; responding to the threat of criminal prosecution, CompuServe eliminated access worldwide to the pornographic chat group illegal under German law before it was able to come up with software (nevertheless judged inadequate by the German courts) enabling parents to install blocking mechanisms for children.[51] But because Internet technology now makes "zoning" possible, no compelling reason exists to alter the "targeting"/"effects" test which justifies prescriptive jurisdiction in the real world. When deliberate or targeted, obnoxious consequences felt within the forum State can hardly be challenged as a valid basis for restrictive regulation. Similarly, restrictions designed to operate exclusively with respect to effects produced within the territory of the regulating State remain clearly within the bounds of international legitimacy. All in all, it is far easier, technically, to parcel out prescriptive jurisdiction optimally in cyberspace than in the real world. Technology allows courts to prescribe the least intrusive solution. At the same time, and because regulatory reaction can be fine-tuned to harmful effects, the risk of externalities in the form of overregulation can practically be eliminated. This is particularly so since zoning techniques available on the Web cause prescription and enforcement jurisdiction to coincide. Technology harnessed to the law—and not the reverse—provides the means of ensur-

50. Reidenberg, *supra* note 7, at 276.
51. *See supra* note 9.

ing perfect compliance with regulation. Given this premise, cyberspace has much to teach the real world.

III. LESSONS FROM CYBERSPACE: WHEN PRESCRIPTION AND ENFORCEMENT COINCIDE

So what's so different about regulatory conflicts on the Web? Part II showed that, as a product of technology, cyberspace should not modify real-world principles of accountability. In fact, as this part of the Article will demonstrate, the very technology that defines the structure of cyberspace provides means to ensure near-perfect correlation between the scope of regulatory authority and the power of enforcement unattainable in the real world. The real specificity of cyberconflicts lies in the potential for filtering or zoning techniques to create a Coasean space of costless compliance,[52] which could not be achieved through real-world enforcement processes. Section A shows that enhanced means for ensuring compliance should provide a correlative incentive to fine-tune prescriptive jurisdiction. Section B acknowledges, however, that despite the normative potential of technology, the difficult question as to who bears the burden of implementation remains unanswered.

A. *Creating a Coasean Space of Watertight Compliance*

This Section argues that, putting aside for the moment the issue of the burden of implementation, filtering technology has the potential of allowing a regulating State to render illegality technically impossible within its prescriptive sphere. This ability allows the State to eliminate inefficiencies stemming from the real-world differences between the scope of regulatory claims and its power to enforce, creating incentives to adjust its prescriptive jurisdiction to match those restrictions functionally necessary to bring about its protective regulatory goals. Cyberspace thus provides conditions for optimal regulatory coordination, which remains unattainable in the real world.

As Lessig and Resnick point out, rules can be inscribed into the software itself[53]—in the very same way that, conversely, Internet technology can give expression to the idea that the Web is comprised of a lawless space. In a purely domestic context, for example, filtering

52. *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 900 (1996) ("Perfectly zoned, cyberspace could be that place where there are no collective action problems—the Coasean space required by Roberto Unger's vision of plasticity; the plasticity of Unger assumed in the Coasean world.").

53. *See* Lessig & Resnick, *supra* note 30 (discussing costs and benefits of using different architectures to regulate speech); *see also* Reidenberg, *supra* note 7.

techniques that allow, say, identification of users' ages can ensure immediate near-perfect compliance with legal rules prohibiting the communication of pornographic data to minors. Software, put into the direct service of State regulation, can cause illegality to become a technical impossibility. Of obvious relevance to the domestic context, where it allows perfectly calibrated balancing of interests between conflicting values (in our example the adult freedom of expression and protection of minors), the same technology holds important potential to solve the regulatory conflicts on the international scene. Developing filtering techniques that allow geographical identification of Internet users can ensure the exact correlation of prescription and enforcement while "zoning" technology can similarly allocate regulatory authority. The end result is a far cry from the lawless space conceived by Internet separatists. Harnessed to regulatory objectives, filtering technology could free courts from the need to rely on the less-than-perfect enforcement techniques of the real world, while providing greater security to service providers, who would be protected from unwanted accountability due to accidental transgression of restriction regulation.

1. Absence of Real World Inefficiencies

In the real world, discrepancy between prescription and enforcement traditionally causes various inefficiencies, including evasion of the law. Thus, a judgment awarded in the forum State on a perfectly legitimate jurisdictional basis may nevertheless remain internationally ineffective if the defendant has no assets within forum territory on which enforcement can take place locally.[54] Since enforcement abroad will always be subject to some form of scrutiny of the content of the forum judgment by the foreign courts, it is easy for a defendant to remove assets to a safe harbor in any jurisdiction which will refuse to recognize that judgment—on public policy grounds, for instance. While obviously a cause for concern in cases where the basis for prescriptive jurisdiction is legitimate, this discrepancy between prescription and enforcement also serves as a natural check on exorbitant regulatory claims. When the regulating State overreaches its legitimate sphere of prescriptive jurisdiction, any judgment awarded in such conditions is doomed to nonrecognition abroad.

The same discrepancy between prescription and enforcement has also had important consequences on the effectiveness of regulation in cyberspace. A service provider who wishes to enjoy immunity from a given State's restrictive regulation—even if its regulatory claim is

54. Extraterritorial freezing orders and other forms of injunctive relief in common law jurisdictions can remedy this difficulty. Parties' desires to avoid being in contempt of court allow judges to effectively employ these injunctive control mechanisms.

legitimate by reason of substantial effects on welfare within its borders—may do so simply by removing all potential enforcement leverage—essentially assets—from that State's territory. Conversely, this discrepancy may act as an important check on the risk of overregulation. Not all the States claiming to regulate activities on the Web necessarily have the correlative power to enforce the restrictions they impose, so that exorbitant regulatory claims may be ignored by service providers who have no connection with the regulating State in the form of assets or other real-world bases for direct or indirect enforcement. Thus, the real world provides natural adjustment techniques for correcting exorbitant regulatory claims.

However, in cyberspace, regulating States may ensure immediate compliance by inscribing rules into the available software, even in situations where no real-world means of enforcement exist. If a regulating State employs zoning technology to block access to data it deems offensive, a content provider contemplating trading in such data can no longer choose to risk liability or criminal sanctions in the hope that enforcement processes cannot reach it. Understandably, such a perspective of immediate compliance might give rise to concern.

When the regulating State does not have any legitimate basis to assert prescriptive jurisdiction, the fact that technology nevertheless provides the means to ensure mandatory compliance might seem to herald the death of free enterprise and expression in cyberspace. However, if the regulating State does lack reasonable grounds for exercising prescriptive jurisdiction, this can only mean that effects within its territory are insubstantial or that it has not, in fact, been targeted. The filtering of access to data cannot therefore be of great import either to its own population or to the author of the regulated activity.

2. Enhanced Need for Optimal Definition of Prescriptive Jurisdiction

Nevertheless, it is true that in a world of perfect correlation between prescription and enforcement, excessive regulation can no longer be counterbalanced by real-world evasion techniques. Therefore, while the possibility of writing the rules into the software and ensuring immediate compliance presents obvious advantages, the need for an optimal definition of prescriptive jurisdiction deserves special thought. Because prescriptions can be enforced with accuracy, courts should aim at perfectly calibrated solutions, avoiding the friction that exists in the real world due to regulatory overreaching and resistance on the part of the regulated service provider. The incentive to do so should derive from the increased interconnectedness of activities conducted over the Web and

the growing interdependency of regulating States. In other words, one may hope that moderation will breed moderation in the assertion of regulatory claims, since given the varying interests of States across the board, all will stand to gain from cooperative attitudes. For example, the interest of the United States is not systematically in favor of unbridled expression in cyberspace, particularly when its interest in protecting intellectual property is involved. Conversely, these are instances where other jurisdictions will be happy to invoke the free flow of data, which they may reject when it threatens competing local values such as privacy, the prohibition of hate speech, etc. Subsequently, all should be ready to subscribe, ex ante, to a rule of reason, under which the benefit from being able to ensure protection of local policies should balance out the concessions made to other States' conflicting regulatory claims.

Indeed, many courts are fine-tuning technical solutions, striving to limit the thrust of restrictive regulation in cyberspace to cases where effects felt within the forum State are either substantial or, in the case of criminal sanctions, deliberate. Thus, the *Yahoo!* court tailored its injunction to limit its intrusiveness; it ordered access to be blocked in France, where the targeted data was considered harmful, without interfering with the other activities of the defendant with respect to the rest of the world.[55] Perfect tailoring provides both the means and the incentives for perfect compliance and for fine-tuning regulatory claims. As Lessig emphasizes, zoning on the Web has efficiency unmatched in the real world,[56] and this certainly holds true when applied to international prescriptive jurisdiction.

B. *Burden of Implementation*

This last Section evokes the remaining, and most difficult, issue, deliberately set aside in preceding developments: Who should bear the burden, including costs, of implementing the perfectly tailored solutions discussed above? Indeed, it may be easier to determine "who regulates?" than to decide who should assume the burden of filtering the data which the regulating State wishes—legitimately—to make unavailable within its borders. Although the most realistic solution probably would place the burden on the regulating State, real-world inequalities between States may well intrude upon the implementation of a perfect Coasean space.

Curiously, this issue is very often neglected. For instance, the French decision in the *Yahoo!* case generated violent criticism in the United

---

55. The U.S. cases cited *supra* note 40 also enjoined the targeting of illegal content into the forum State, but did not regulate the availability of information elsewhere.

56. Lessig, *supra* note 52, at 889 (noting that "[z]oning is coming to cyberspace, with an efficiency unmatched in real space").

States and among Internet separatists of France's regulatory claim, even if such a claim was specifically tailored to the effects suffered within its borders and can hardly be said to be unreasonable by real-world standards. Yet the fact that the court put the burden of implementing the filtering on Yahoo! attracted much less attention. Nevertheless, the real issue seems to be far less "Who regulates?" as "Who bears the burden of zoning?"

Was it right that the cost of putting into place the filtering technology should have fallen on Yahoo!? Firstly, such a solution is obviously realistic only insofar as the court's order was enforceable, in the event of noncompliance, on local assets.[57] Moreover, familiar objections arise, with a slightly different thrust. Should a service provider located in the United States, whose activity is protected by the First Amendment, have to bear the costs of restricting access to information in all the countries which object to its availability? The issue is not to deny the equal right of States affected by the data to protect what they perceive as fundamental values, but to distribute equitably the cost of establishing such protection.

The obvious answer might be to say that, to the extent the website actively attracts business from the regulating State, there is no reason why Yahoo! should not bear the costs of compliance. For instance, Yahoo! was making substantial revenue from its business contacts (such as advertising contracts) with France; requiring it to adapt its software to the regulatory requirements of the State where it is doing business does not seem particularly unreasonable. The real world provides all sorts of instances where the marketing of a product or service requires compliance with local regulations. Given, too, that the service provider is exporting offensive material into the regulating State, the "polluter pays" principle could be invoked to justify the same result.

However, more practical considerations of incentive and regulatory advantage do not necessarily support the "polluter pays" principle in this context. The State in which the effects are suffered obviously has a greater incentive to set up technology which will ensure watertight enforcement of its own restrictive regulation: it would certainly make more sense to leave it to filter the undesired data, to avoid the risk of underenforcement. The receiving State also has the greater regulatory advantage, because it can best decide the extent of the prohibition that fits its

57. Or on assets in a "friendly" foreign State (that is, a State ready to enforce the forum judgment). In the *Yahoo!* case, Yahoo! was quick to ensure that enforcement would not take place in California. *See* Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, 169 F. Supp. 2d 1181, 1184–86 (N.D. Cal. 2001) (discussing case history and Yahoo!'s arguments seeking a declaratory judgment). The revenues generated from its activities in France were arguably sufficient to ensure local enforcement.

conception of public welfare and sits in a better position to implement it. It is far less easy, from the content provider's point of view, to ensure that no information reaches users located in States where it might be considered obnoxious. Furthermore, making the receiving State bear the burden of ensuring compliance could be an efficient means of counteracting the inevitable temptation to overregulate; legislative spillover might best be avoided by imposing the cost of regulation on the regulating State.

Moreover, it may be that analogies with the real world should not be pushed too far by forcing the content provider to pay for filtering. If cyberspace is to be an area in which the rule of reason functions effectively, cooperation between regulating States might be better encouraged by a concession to conventional wisdom, which suggests that it is more "fair" for the regulating State to pay for filtering. This notion derives from separatist ideology and is relayed by traditional reliance on place-of-conduct conceptions. It no doubt felt excessively burdensome to Yahoo! to implement French regulation while protected at home by the First Amendment, as it feels burdensome to non-U.S. firms to comply with federal copyright law when their activity is perfectly legal in the place of conduct. As there is a likelihood that costs of implementation of restrictive regulation in these various fields will ultimately cancel each other out, there may be no point in insisting on a counterintuitive solution by burdening the author of cross-border effects with the cost of compliance which will inevitably be perceived as unfair—however legitimate it may be to do so in theory.

Whatever the arguments in favor of associating the right to regulate and the burden of cost, however, this is obviously far from being an easy issue. The above considerations only become valid if one supposes that access to filtering technology is equally easy (or burdensome) for all concerned. However, some regulating States with legitimate reasons to filter data may lack the technological means or public resources to do so. Real world inequalities intrude, once again, on the ways in which States eliminate regulatory conflicts. As a result, it might appear more equitable to burden private service providers generating revenue from activities directed at the regulating State rather than on the population of the regulating State. Unfortunately, however, as seen above, compliance will depend, once again, on the availability of traditional enforcement procedures.

Before the costless solutions of perfect Coasean space can be achieved, States must overcome their limited technological and pecuniary resources. This prospect leaves obvious room for real-world cooperation between States. Meanwhile, concessions necessary to sub-

ject cyberspace to a regulatory rule of reason are certainly worthwhile, if they can prevent States that feel threatened by excessive freedom of information on the Internet from taking far more radical, aggressive initiatives to control the flows of data.[58] The specter of technological warfare as a corollary to prescriptive jurisdiction should not be dismissed lightly!

CONCLUSION

Calling attention to new issues of prescriptive jurisdiction in the international arena, regulatory conflicts in cyberspace are now frequently linked to the worldwide availability in cyberspace of data perceived to be harmful or offensive to fundamental values in the regulating State, while protected by constitutional freedom of expression in the State in which they are made accessible. Looking for appropriate means of managing conflicting regulatory claims, which conventional wisdom sees as either illegitimate or irreducible, has, first of all, afforded the opportunity to confirm the legitimacy of yardsticks used to measure prescriptive jurisdiction in the real world. Effects-based jurisdiction, increasingly supported in the context of conflicts of market regulation in the real world, seems entirely appropriate here, where the assertion of prescription jurisdiction is generally designed to protect fundamental social values shared by a community living within the borders of the regulating State. Indeed, there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it. Analysis of such a claim has shown that it reverses the proper relationship between law and technology. Technology being purely manmade and thus subject to ideological choice, should in no way dictate the way in which law manages conflicting interests arising through its medium. Rather, once harnessed to the law, technology can facilitate the exercise of prescriptive jurisdiction in the international arena, by providing the means to ensure perfect compliance with regulatory claims over cyberspace, by the use of filtering techniques. In turn, the substitution of technology for enforcement should create incentives for States to calibrate their regulatory claims so as to avoid counterproductive overregulation. However, the foregoing depiction of an ideal world of costless cross-border compliance leaves several difficult issues unsolved.

58. On the possible development of spy systems, cyberenforcement agencies and other more "troubling avenues," see Reidenberg, *supra* note 7, at 277.

In particular, the burden of compliance requires additional reflection; in the present state of the world, unequal conditions of access to technology leave some States more vulnerable than others to the violation of fundamental social policies or values through the free flow of data in cyberspace. Although it may appear, therefore, that a case such as *Yahoo!* has raised as many difficulties as it suggests solutions, it must also be emphasized that it provides excellent food for thought not only on the relationship between law and technology, but on the proper calibration of prescriptive jurisdiction both in cyberspace and the real world.