The Shape of Governance:

Analyzing the World of Internet Regulation

Viktor Mayer-Schönberger*

TABLE OF CONTENTS

Cyberlaw, the area of Internet regulation,[1] has become a booming

* Assistant Professor of Public Policy, John F. Kennedy School of Government, Harvard University. I would like to thank Alexander Somek, the participants in the Yale Law and Technology Society Seminar Series, the John B. Moore International Law Symposium at the University of Virginia School of Law, and the participants in the cyberlaw panel at the American Society of International Law's 2000 Annual Meeting for many helpful suggestions. I gratefully acknowledge the invaluable help of Matthew Bates as well as the research assistance of Norbert Weinrichter and Anatole Papadopoulos and the editing assistance of Michael Harrup.

field. What used to be at the outer fringes of the legal landscape has now taken center stage.[2] News websites catering to the Internet generation are full of stories recounting the latest legal twists in cyberspace.[3] Journalists and readers vocally take positions on both sides of contentious domain name disputes,[4] fights over Napster and peer-to-

1. *Black's Law Dictionary* defines cyberlaw as "[t]he field of law dealing with computers and the Internet, including such issues as intellectual-property rights, freedom of expression, and free access to information." BLACK'S LAW DICTIONARY 392 (7th ed. 1999). There is, however, no unanimity on the definition or the use of the term "cyberlaw." Traditionally, a list of issues substitutes for an abstract definition.

2. *See*, *e.g.*, Needham J. Boddie, II et al., *A Review of Copyright and the Internet*, 20 CAMPBELL L. REV. 193, 193 (1998) ("The expansion of the Internet in size, usage and influence has generated a variety of novel legal questions."); Allison Roarty, *Link Liability: The Argument For Inline Links And Frames As Infringements Of The Copyright Display Right*, 68 FORDHAM L. REV. 1011, 1011 (1999) (stating that "[a]s the Internet continues to expand exponentially, so do the corresponding legal issues"); *cf.* Steven R. Salbu, *Who Should Govern The Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J.L. & TECH. 429, 430 (1998) (reviewing the many different cyberlaw issues that have received significant attention).

3. *See*, *e.g.*, Brian Krebs, *Global E-Copyrights Treaty to Take Effect in March 2002*, Newsbytes, *at* http://www.us-tradelaw.com/Article.Copyright%20Treaty%20(12.7.2001).doc (Dec. 7, 2001); Patricia Jacobus, *Court: Programming Languages Covered by First Amendment*, CNET News.com, *at* http://news.com.com/2100-1023-238844.html/legacy=cnet (Apr. 4, 2000); Patricia Jacobus, *Judge Sides with Net Filtering Firm in Copyright Case*, CNET News.com, *at* http://news.com.com/2100-1023-238544.html/legacy=cnet (Mar. 28, 2000); Jen Muehlbauer, *Judge Says E-Books Aren't Books,* The Industry Standard, *at* http://www.thestandard.com/article/0,1902,27858,00.html (July 12, 2001); ZDNN Staff, *EFF on DeCSS: Hackers' Rights at Stake*, ZDNet News, *at* http://zdnet.com/2100-11-527367.html (Jan. 18, 2001). Conventional newspapers have also taken up these issues. *See*, *e.g.*, George Black, *Call for Controls: The Internet Must Regulate Itself*, FIN. TIMES, Apr. 1, 1998, pt. 4, at 12; Vinton G. Cerf, *Building an Internet Free of Barriers*, N.Y. TIMES, July 27, 1997, § 3, at 12; Thomas E. Weber, *The Internet (A Special Report): Debate: Does Anything Go? Limiting Free Speech on the Net: Five Players Debate the Issue*, WALL ST. J., Dec. 8, 1997, at R29. For a similar observation, see David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1371 (1996) [hereinafter Johnson & Post, *Law & Borders*].

4. *See*, *e.g.*, Jennifer Balderama, *Coca-Cola Caps Net Name Dispute with Fan Site*, CNET News.com, *at* http://news.com.com/2100-1023-236794.html?legacy=cnet (Feb. 10, 2000); Cecily Barnes, *Sex.com domain name battle heads back to court*, ZDNet News, *at* http://zdnet.com.com/2100-11-528731.html (March 7, 2001); *First Cybersquatting Case Under WIPO Process Just Concluded,* World Intellectual Property Organization (WIPO), *at* http://www.wipo.org/pressroom/en/releases/2000/p204.htm (Jan. 14, 2000); Craig Francis, *Madonna Bids to Win Domain Name Game*, CNN.com, *at* http://www.cnn.com/2000/WORLD/europe/09/13/switzerland.madonna/index.html (Sept. 14, 2000); Joseph Gomes, *Aimster Has One Last Chance to Keep Its Name*, The Industry Standard, *at* http://www.thestandard.com/article/0,1902,27038,00.html (June 8, 2001); Stephanie Grunier & John Lippman, *Warner Bros. Claims Harry Potter Sites,* ZDNet News, *at* http://zdnet.com.com/2100-11-503255.html (Dec. 20, 2000); *Shell Beats Shell to Win Web Address,* New Zealand Herald Online, *at* http://www.nzherald.co.nz/latestnewsstory.cfm?storyID=229963&thesection=business&thesubsection=latest (Nov. 25, 2001). Both the Electronic Frontier Foundation (www.eff.org) and the Center for Democracy and Technology (www.cdt.org) give overviews of interesting articles and legal sources.

peer networking,[5] content regulation crusades,[6] and trade wars[7] on Internet privacy. Given the intensity of the debates and the media attention they receive, it seems cyberlaw is not just the application of existing legal rules to cyberspace, but a new legal domain to be explored, analyzed and taught.[8]

Judge Frank H. Easterbrook has questioned this premise.[9] In a stinging critique, Easterbrook takes aim at what he perceives is largely a phenomenological approach to regulation of cyberspace and asks

5. *See*, *e.g.*, HASSAN M. FATTAH, P2P: HOW PEER-TO-PEER TECHNOLOGY IS REVOLUTIONIZING THE WAY WE DO BUSINESS (2002); Clay Shirky, *Listening to Napster*, *in* PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 21 (Andy Oram ed., 2001); *The Artist Must Get Paid*, BOSTON HERALD, July 30, 2000, at O24; *Musicmakers Deserve Copyright Protection on Web*, NEWSDAY, Aug. 1, 2000, at A30; *Napster Agonistes*, WALL ST. J., June 19, 2000, at A46; John Heilemann, *David Boies: The Wired Interview*, Wired Magazine, *at* http://www.wired.com/wired/archive/8.10/boies.html (Oct. 2000); Hane C. Lee, *Another Voice Enters the Napster Debate*, TheStandard.com, *at* http://www.thestandard.com/article/display/0,1151,15718,00.html (June 5, 2000) (describing the debate in the press surrounding Napster as "always black and white"); Siva Vaidhyanathan, *MP3: It's Only Rock and Roll and The Kids Are Alright,* The Nation, *at* http://www.thenation.com/docprint.mhtml?i=20000724&s=vaidhyanathan (July 24, 2000).

6. *See*, *e.g.*, Rose Aguilar, *ISP Shuts Down Antiabortion Site*, CNET News.com, *at* http://news.cnet.com/news/0-1005-200-338353.html (Feb. 5, 1999) (reporting on MindSpring's shutdown of the controversial antiabortion Nuremberg Files website after a federal jury ruled that the site threatened the lives of about 200 abortion providers); Courtney Macavinta, *Officials Debate Posting EPA Data*, CNET News.com, *at* http://news.cnet.com/news/0-1005-200-333513.html (Sept. 23, 1998) (reporting on Clinton Administration's opposition to online posting of chemical manufacturers' "worst-case" accident scenarios by EPA after terrorist attacks on U.S. embassies in Africa); *Tiananmen Activists Launch Net Crusade*, CNET News.com, *at* http://news.cnet.com/news/0-1005-200-341032.html (Apr. 12, 1999) (describing use of the web to counter Chinese censorship in reporting on student protests); *see also* Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. REV. 23 (2001); Thomas W. Hazlett & David W. Sosa, *"Chilling" the Internet? Lessons from FCC Regulation of Radio Broadcasting*, 4 MICH. TELECOMM. & TECH. L. REV. 35 (1997); Kim L. Rappaport, *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, 766-67, 788-90 (1998); Janet Kornblum, *Challenge Promised Over Library Filters*, USA TODAY, Dec. 19, 2000, at 3D; Dave Wilson, *Child-Proofing the Net Still an Unsettled Issue,* L.A. TIMES, May 31, 2001, pt. T, at 1; Nicole Yeong, *Code to Deal with Electronic Content*, NEW STRAITS TIMES – COMPUTIMES (Malaysia), Aug. 2, 2001, at 1; Keith Perine, *Online Child Porn Act Ruled Unconstitutional,* The Industry Standard, *at* http://www.thestandard.com/article/0,1902,16312,00.html (June 23, 2000).

7. *See*, *e.g.*, PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 170-72 (1998); Junkbusters, Junkbusters Presentations at Internet World (outlining the panel, "The Privacy Trade Wars of 1999?"), *at* http://www.junkbusters.com/world.html (last visited Dec. 19, 2002).

8. *Cf.* Johnson & Post, *Law and Borders*, *supra* note 3, at 1367, 1379, 1400 (prescribing application of distinct laws to cyberspace).

9. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

whether cyberlaw is actually different from the "law of the horse,"[10] implying that cyberlaw should qualify as an independent field of legal study only if such a question can be answered in the affirmative. Easterbrook's critique must be taken seriously. Indeed, the vast majority of cyberlaw analysis focuses on the application of existing legal norms – intellectual property, trademark, antitrust, content regulation and the like – to cyberspace issues. It is difficult to argue that a dispute over infringement of a particular trademark falls within the confines of a new field of cyberlaw rather than the existing realm of trademark law just because the trademark infringement happened on the Internet.[11] A. Michael Froomkin consequently has argued thatcyberlaw has come of age.[12] Some have even challenged whether cyberlaw or the "law of the Internet" exist as useful concepts.[13] Does that mean that cyberlaw is, as Easterbrook's provocation would have it, a transitional phenomenon?

Lawrence Lessig has a response to Easterbrook's critique. He rightly suggests that the existence of cyberlaw depends not on metaphysical considerations, but on the usefulness of joint treatment of similar problems, arguing that there indeed are practical uses to defining a separate legal field of cyberlaw.[14] But what is it about the categories of problems that cyberlaw deals with that makes it a unique field of legal study? Together with Elisabeth Holzleithner, I have suggested elsewhere that cyberlaw may be unique in three distinct ways.[15] The first, which we dubbed "cyber-structure,"[16] is focused on the indirect

10. *Id.* at 208.

11. *Cf.* Boddie, *supra* note 2 (arguing that "'Internet Law' does not represent a new field or body of law such as tort law, contract law or property law" but rather "is more or less the application of existing legal doctrines to the new technologies, avenues of commerce, and means of human interaction defined, created and experienced on the Internet"); Charles Fried, *Perfect Freedom or Perfect Control?*, 114 HARV. L. REV. 606, 621 (2000) (reviewing LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) and criticizing as an "unjustified leap into the realm of metaphor" the view of cyberspace as "a sovereignty overlapping traditional sovereignties, to be governed by a legal regime appropriate to that level").

12. A. Michael Froomkin, *The Empire Strikes Back*, 73 CHI.-KENT L. REV. 1101, 1116 (1998) [hereinafter Froomkin, *Empire*] ("I take all this normalcy as a sign that Internet Law has come of age – perhaps too soon.").

13. Easterbrook, *supra* note 9; Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1147 (2000).

14. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach,* 113 HARV. L. REV. 501, 502 (1999) [hereinafter Lessig, *Horse*] (suggesting that "unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect").

15. Viktor Mayer-Schönberger & Elisabeth Holzleithner, *Deconstructing Cyberlaw*, JURIDICUM, Feb. 1997, at 30.

16. *Id.* at 33; *see also* VIKTOR MAYER-SCHÖNBERGER, DAS RECHT AM INFO-HIGHWAY 41 (1997). A somewhat different, quite thoughtful version of this line of argument has been advanced by Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) [hereinafter Reidenberg, *Lex Informatica*].

regulation of cyberspace through technological standards and structures. The cyber-structure dimension of cyberlaw builds on William Mitchell's (and others')[17] argument that "code is the law."[18] Professor Lessig has developed and laid out the cyber-structure domain of cyberlaw most eloquently and persuasively.[19] In a recent article,[20] he explicitly responds to Easterbrook by arguing that this structural dimension is what makes cyberlaw unique.[21]

The second aspect, which we called "cyber-links,"[22] looks at what rights law grants people to give them control over information. Just as property rights are necessary to create and sustain markets for physical goods, rights to control information – intellectual property rights, privacy rights or rights to publicity – are necessary for information markets to function. To be sure, information markets have existed long before the Internet. But modern information technologies have made it possible for information to be digitized, thus rendering concepts of copy and original (and the resulting notion of value differentiation implicit in almost all traditional information markets) useless. And the 'net has provided a new, dynamic, versatile, quasi-costless and global infrastructure for such information markets. Consequently, Easterbrook himself advocates "a sound law of intellectual property"[23] as the core of a possible cyberlaw, and Kenneth Laudon has argued that information privacy in cyberspace may be better served by granting individuals property rights in their personal information than regulations limiting the use of personal information.[24]

There is, however, a third aspect that may differentiate cyberlaw from more traditional legal subjects. This aspect transcends substantive legal issues in cyberspace as much as it permeates them. It revolves around

17. *See* Rohan Samarajiva's quip that "cyberspace is no neutral container." MAYER-SCHÖNBERGER, *supra* note 16, at 41.

18. WILLIAM MITCHELL, CITY OF BITS 111 (1996); *see also* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors,* 66 U. CIN. L. REV. 177 (1997); Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U. CHI. LEGAL F. 335, 338.

19. LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999).

20. Lessig, *Horse*, *supra* note 14.

21. *Id.* at 503-06.

22. Mayer-Schönberger & Holzleithner, *supra* note 15, at 32.

23. Easterbrook, *supra* note 9, at 208.

24. Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92. For a similar view, see Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1 (1992); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996). For a "license rights" view, see Pamela Samuelson, *Privacy As Intellectual Property?,* 52 STAN. L. REV. 1125 (2000).

the question of who should govern and thus regulate cyberspace.[25] This article examines this cyber-governance dimension of cyberlaw. In part I, three typical cyber-governance debates are described. Part II analyzes the relationship between these three debates, usually seen as hierarchical layers. In part III,—and only partly tongue-in-cheek—a different analytical metaphor, the regulatory triangle, providing a basis for a much richer regulatory mix, is suggested and applied to a number of cyber-regulations. In part IV, other governance options based on regulatory extremes are examined and their weaknesses identified. Part V extends the regulatory *mix* to an even richer regulatory *blend*, based on the triangle metaphor. Finally, part VI adds a few cautious remarks on evaluating the regulatory shape.

This article does not argue that disconnecting the substantive legal issues from the structural dimension of governance is desirable or feasible. Rather, it suggests that viewing these issues as distinct yet connected discursive strands may help us not only to better analyze the many cyberlaw debates, but also to point to more innovative regulatory solutions.

I. THREE TYPES OF CYBERLAW DISCOURSES

Most cyberlaw debates combine arguments addressing substantive legal issues with arguments about regulatory governance. For example, debates about Internet content regulation reexamine important First Amendment questions.[26] At the same time, such debates also look at

25. *See, e.g.,* Froomkin, *Empire*, *supra* note 12; Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace,* 6 CORNELL J. L. & PUB. POL'Y 475 (1997); Viktor Mayer-Schönberger, *The Authority of Law in Times of Cyberspace*, 2001 J. L. TECH & POL. 1 (2001) (contrasting four scenarios of cyber-governance); Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory,* 88 CAL. L. REV. 395 (2000) (analyzing the normative implications of self-governance); David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155 (1996); Joel Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism,* 5 IND. J. GLOBAL LEG. STUD. 561 (1998) (suggesting that self-regulation and international regulation may not be exclusive modes of governance); Philip J. Weiser, *Internet Governance, Standard Setting, and Self Regulation,* 28 N. KY. L. REV. 822 (2001) (advocating a mixed governance approach that includes standard setting and other forms of self-regulation); Timothy S. Wu, *Cyberspace Sovereignty? The Internet and the International System,* 10 HARV. J. L. & TECH. 647 (1997) (suggesting that as national Internet regulation is feasible, nations will exercise their power of governance); *see also* EREZ KALIR AND ELLIOT E. MAXWELL, RETHINKING BOUNDARIES IN CYBERSPACE - BEREPORT OF THE ASPEN INSTITUTE INTERNET POLICY PROJECT (2002).

26. *See*, *e.g.*, John F. McGuire, *When Speech is Heard Around the World: Internet Content Regulation in the United States and Germany*, 74 N.Y.U. L. REV. 750 (1999); Mark S. Nadel, *The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Librarians Exclude?,* 78 TEX. L. REV. 1117 (2000); Walter Pincus,

who can and should regulate Internet content.[27] Whereas the substantive parts of such debates are issue-specific, focusing for example on free speech, the parts of the debates concerning who should regulate are more abstract, and transcend concrete substantive issues. Hence, similar statements about who should regulate can be found in any substantive debate concerning cyberlaw, from content regulation to domain name and trademark protection disputes.

Arguments about the appropriate agency of governance for cyberspace surface particularly when the obvious and accepted jurisdictional reach of the agency being suggested is incongruent with the space to be regulated.[28] Because of the plentitude of such partial overlaps between accepted regulatory reach and regulatory space in cyberspace, arguments about governance have become commonplace in cyberlaw debates. Opponents of proposed cyber-rules in particular rarely fail to point out governance deficiencies caused by such overlaps, thereby introducing the governance dimension into the discourse.[29]

In order to analyze the discourses concerning governance of cyberspace, one has to first separate them from substantive arguments. Once these substantive issues are filtered out of the discourse, what remains are comparatively abstract discourses on who should govern cyberspace. In a second step, these abstract debates can be categorized in groups, or - perhaps - clusters of discourses on the appropriate

The Internet Paradox: Libel, Slander & the First Amendment in Cyberspace, 2 GREEN BAG 2D 279 (1999); Cass R. Sunstein, *The First Amendment in Cyberspace,* 104 YALE L.J. 1757 (1995); Eugene Volokh, *Freedom of Speech, Cyberspace, and Harassment Law,* 2001 STAN. TECH. L. REV. 3; Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex,* 1996 U. CHI. LEGAL F. 377; Kim L. 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); Junichi P. Senitsu, Note, *Burning Cyberbooks in Public Libraries: Internet Filtering Software vs. the First Amendment*, 52 STAN. L. REV. 509 (2000).

27. *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage, in* BORDERS IN CYBERSPACE 129, 140-50 (Brian Kahin & Charles Nesson eds., 1997) [hereinafter Froomkin, *Arbitrage*]; William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community,* 30 WAKE FOREST L. REV. 197 (1995); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 13-25 (1996) [hereinafter Perritt, *Jurisdiction*]; John S. Zanghi, *"Community Standards" in Cyberspace,* 21 DAYTON L. REV. 95 (1995).

28. *See also* Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?,* 12 BERKELEY TECH. L. J. 413, 422-423 (1997) [hereinafter Perritt, *Self-Government*] (stating that impracticalities with existing governance structures in cyberspace arise "when the boundaries of electronic communities cross the geographic boundaries of traditional sovereigns").

29. *See, e.g.,* Froomkin, *Arbitrage*, *supra* note 27, at 150; Post, *supra* note 25, at 159-63; Sean Selin, Comment, *Governing Cyberspace: The Need for an International Solution,* 32 GONZ. L. REV. 365, 380 (1996) (arguing that "the Internet tends to ignore national boundaries").

governance agency for cyberspace. Three such clusters can be easily identified and provide blueprints for "traditionalist", "cyber-separatist", and "internationalist" discourses on the most appropriate agency to govern cyberspace.[30]

1. The State-Based Traditionalist Discourse

Traditionalists begin by stating that the preeminent existing governance agency, the state, is the appropriate regulator of cyberspace.[31] After all, the state has the democratic legitimization, the procedural setup, and the institutional enforcement to make regulations, including ones pertaining to cyberspace, work.

The opponents of national laws regulating cyberspace contest this assumption that the state is the best agency to regulate cyberspace. They point out that any national law applied to cyberspace will lack the necessary democratic legitimacy on a global network. Why, they ask, should anyone operating in cyberspace be subject to a cyber-regulation in whose enactment she did not partake even in the most indirect way? Isn't democratic legitimization all about taking part in the political process?[32] Further, if each and every national law on the face of the earth is applied to conduct in cyberspace, then people interacting on the Net would potentially have to obey hundreds of different, potentially even contradictory regulations at the same time.[33] In the words of *The*

30. This taxonomy is one focused simply on governance. Others have attempted to identify a general taxonomy of cyberlaw discourse and cyberlaw regulations. For a recent example, see Bradford L. Smith, *The Third Industrial Revolution: Policymaking for the Internet,* 3 COLUM. SCI. & TECH. L. REV. 1 (2001).

31. *See, e.g.,* Terrence Berg, *www.wildwest.gov: The Impact of the Internet on State Power to Enforce the Law*, 2000 B.Y.U. L. REV. 1305, 1307 (2000) (advocating numerous proposals to "enhance the state's ability to continue its traditional role of protecting its citizens in the online world"); Fried, *supra* note 11, at 626 ("After all, the publisher who tries to enforce a clickwrap contract invokes the state's help, and he must expect that the state will impose its conditions and policies in granting it.").

32. Aron Mefford, *Lex Informatica: Foundations of Law on the Internet,* 5 IND. J. GLOBAL LEGAL STUD. 211, 217 (1997) ("States wishing to control activity on the Internet suffer from two legitimacy problems.").

33. This is often referred to as a "negative spillover effect." *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV 1199, 1200 (1998) [hereinafter Goldsmith, *Against Cyberanarchy*]; Sanjay S. Mody, Note, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365, 382 (2001). For warning against such spillover effects, see Johnson & Post, *Law and Borders*, *supra* note 3, at 1374 (stating that if the state-based governance model is taken seriously, web content "must be subject simultaneously to the laws of all territorial sovereigns"). For analysis of the potential conflicting exercise by multiple authorities of prescriptive jurisdiction over Internet transmissions, see Jane C. Ginsburg, *Copyright Without Borders? Choice of Forum and Choice of Law for Copyright Infringement in Cyberspace*, 15 CARDOZO ARTS & ENT. L.J. 153 (1997) [hereinafter Ginsburg, *Copyright Without Borders?*]; Jane C. Ginsburg, *Extraterritoriality and Multiterritoriality in Copyright*

Economist, reporting on an American online service provider's decision to bar its customers from accessing parts of the Internet because of a Bavarian prosecution alleging a violation of German law, "when Bavaria wrinkles its nose, must the whole world catch a cold?"[34]

Traditionalists do not respond to this extreme portrayal of unfettered regulatory overlap in cyberspace by denying the theoretical problem of regulatory spillover effects.[35] Instead, they emphasize that this problem is not unique to cyberspace:[36] It has accompanied any cross-jurisdictional activity since the beginning of lawmaking. An extensive body of legal doctrine, conflict of laws, has been developed to address this problem successfully.[37] As a result, even though some cases of regulatory spillover might be of profound complexity, the problem is hardly as perplexing and irresolvable, according to traditionalists, as their opponents portray it. Furthermore, traditionalists add that the democratic state currently offers the best and most comprehensive system of governance legitimization around.[38] Why brandish imperfections if one cannot offer a better alternative? Finally, Internet users fearing subjection to foreign rules can easily employ technology to

Infringement, 37 VA. J. INT'L L. 587 (1997); Allan Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998). For a Canadian view, see Pierre Trudel, *Jurisdiction over the Internet: A Canadian Perspective*, 32 INT'L LAW. 1027 (1998).

34. *Sex On the Internet: When Bavaria Wrinkles its Nose, Must the Whole World Catch a Cold?*, THE ECONOMIST, Jan. 6, 1996, at 18.

35. *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEG. STUD. 475, 487 (1998) [hereinafter Goldsmith, *Territorial Sovereignty*]; Mody, *supra* note 33, at 382; Amy Lynne Bomse, Note, *The Dependence of Cyberspace*, 50 DUKE L.J. 1717, 1740 (2001).

36. Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1201, 1208; Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 481; Mody, *supra* note 33, at 389.

37. Because of significant changes in the world, as well as the rise of legal realism and legal positivism, conflict-of-laws doctrine has evolved from an overly simplistic "hermetic territorialism," which Jack L. Goldsmith argues is what skeptics of national cyber-governance have in mind when they argue that national governance leads to unsolvable jurisdictional problems. Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1205-12; *see also* Ginsburg, *Copyright Without Borders?*, *supra* note 33, at 154, 168-75; Andreas P. Reindl, *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks*, 19 MICH. J. INT'L L. 799, 803 (1998) ("Territorial views have traditionally dominated copyright choice of law analysis . . . ."); Jennifer M. Driscoll, Comment, *It's A Small World After All: Conflict Of Laws And Copyright Infringement On The Information Superhighway,* 20 U. PA. J. INT'L ECON. L. 939 (1999).

38. *See generally* Steven R. Ratner, *New Democracies, Old Atrocities: An Inquiry in International Law*, 87 GEO. L.J. 707, 740 (1999) ("If, as appears to be the case, democracy—fairly elected governments combined with the rule of law—is increasingly accepted as the sole or most legitimate form of government. . ."); Guy-Uriel E. Charles, Note, *Fourth Amendment Accommodations: (Un)compelling Public Needs, Balancing Acts, and the Fiction of Consent*, 2 MICH. J. RACE & L. 461, 509-10 ("The idea of consent is an important concept in a democracy because governance through consent is the most efficient and the most legitimate method of governance.").

restrict the interaction they have with foreign actors that might subject them to the jurisdiction of a foreign state.

Conflict of laws, the opponents may counter, is a field of such inherent complexity[39] (even for lawyers) that average netizens cannot be subjected to it without risking a profound "chilling effect" on their behavior online, thus stifling the free flow of information.[40] It is even worse to tell netizens on a global network to use technology to minimize information flows to others, as it makes them "internalize the chill" and thereby undermines the very foundation of freedom of expression, a paramount principle in any society based on information and its free exchange.[41] In addition to this grave problem of constitutional legitimacy, opponents point out that any state-based enforcement system is bound to fail when attempting to police a global network like the Internet. National enforcement, they contend, will never be perfect in a global network.[42]

But the traditionalists have a rebuttal. They say that perfect enforcement is not necessary for cyberlaw to work.[43] Take, they say, the

39. Mefford, *supra* note 32, at 221, calls choice of law "too clumsy to deal with Internet transactions." As Jack Goldsmith has reminded us, the skeptics' views about territorialism and choice of law are remarkably similar to Story's and Beale's. JOSEPH HENRY BEALE, A TREATISE ON THE CONFLICT OF LAWS OR PRIVATE INTERNATIONAL LAW 118 (1916); JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS 7 (Little, Brown 2d ed 1841); Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1205 n.24; *see also* Alfred Hill, *The Judicial Function in Choice of Law*, 85 COLUM. L. REV. 1585, 1619-36 (1985). The classic criticisms of the traditional view are BRAINERD CURRIE, SELECTED ESSAYS ON THE CONFLICT OF LAWS (1963), and WALTER WHEELER COOK, THE LOGICAL AND LEGAL BASES OF THE CONFLICT OF LAWS (1949). *See also* ERNEST G. LORENZEN, SELECTED ARTICLES ON THE CONFLICT OF LAWS 305-21 (1947); Walter Wheeler Cook, *The Jurisdiction of Sovereign States and the Conflict of Laws*, 31 COLUM. L. REV. 368, 372-80 (1931).

40. Dan L. Burk, *Federalism in Cyberspace,* 28 CONN. L. REV. 1095 (1996) [hereinafter Burk, *Federalism*] (cautioning against negative spillover effects that may chill free speech); Thomas W. Hazlett & David W. Sosa, *"Chilling" the Internet? Lessons from FCC Regulation of Radio Broadcasting*, 4 MICH. TELECOMM. TECH. L. REV. 35 (1997); Perritt, *Self-Government*, *supra* note 28, at 422 (calling the use of conflicts of laws "impractical").

41. *Cf.* David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems,* 73 CHI.-KENT. L. REV. 1055 (1998) (employing a "complex systems" model to demonstrate that spillover effects are better attuned to self-regulation than traditional state-based regulation).

42. *See, e.g.,* Mefford, *supra* note 32, at 214 ("States wishing to impose law on or in Cyberspace will find that they simply do not have the physical control over the Net necessary for lawmaking authority."); Perritt, *Self-Government*, *supra* note 28, at 423 (suggesting that national laws may "lack the means of enforcing its decision, because the actor is somewhere beyond its reach").

43. *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996) [hereinafter Lessig, *Zones*], noting:

> A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially. If regulation increases the cost of access to this kind of information, it will

case of speeding on the highway. Not everyone who speeds gets a ticket. But the chances of getting caught, combined with the burdens of punishment, are in general a strong enough incentive for most drivers to keep in check their desire to speed.[44] In fact, few of us would speed even if there were hardly any legal controls on speeding at all. We have internalized the speed limit, as we have internalized regulation in many other areas of our daily lives. We keep ourselves in check without even the necessity of outside enforcement.[45]

But even if we do not need *perfect* enforcement, the opponents argue back, we will still require *sufficient* enforcement to discourage the few among us who will not adhere to a rule on their own; and even sufficient enforcement is unlikely in global cyberspace.[46] Whenever, for example, an information provider is threatened by a regulation in one state, it just needs to relocate the potentially violating information to another jurisdiction with a more favorable regulation. Given the market forces in a global network, over time certain states will turn their liberal regulatory regimes into a competitive advantage, in essence offering to providers of questionable content flags of convenience in the sea of information called the Internet.[47] As Frances Cairncross put it, cyberspace causes the "death of distance."[48] It ridicules traditional

> reduce access to this information, even if it doesn't reduce it to zero. . . . If government regulation had to show that it was perfect before it was justified, then indeed there would be little regulation of cyberspace, or of real space either. But regulation, whether for the good or the bad, has a lower burden to meet.

See also Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies,* 73 CHI.-KENT. L. REV. 1119, 1126 (1998) [hereinafter Goldsmith, *Fallacies*] ("But regulation is rarely if ever perfect in this sense, and it need not be perfect to be effective.")

44. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1229 (citing further examples).

45. A recent study has shown that a substantial number of people (about 30 percent) obey rules even with no sanctions and that size of this group doubles with minimal sanctions and endogenous rule making. JEAN-ROBERT TYRAN & LARS P. FELD, WHY PEOPLE OBEY THE LAW—EXPERIMENTAL EVIDENCE FROM THE PROVISION OF PUBLIC GOODS (CESifo Working Paper No. 651(2), 2002). *See generally* R. D. COOTER, DO GOOD LAWS MAKE GOOD CITIZENS? AN ECONOMIC ANALYSIS OF INTERNALIZING VALUES (Berkeley Olin Program in Law & Economics, Working Paper Series, Paper No. 39, 2000); THOMAS TYLER, WHY PEOPLE OBEY THE LAW (1990); Eric A. Posner, *Law and Social Norms: The Case of Tax Compliance,* 86 VA. L. REV. 1781 (2000).

46. *See* Goldsmith, *Fallacies*, *supra* note 43, at 1126 (conceding that "[t]he relevant question is whether these regulatory strategies will heighten the cost of transmitting, obtaining, copying, and using digital goods *sufficiently* to achieve acceptable control over them" (emphasis added)).

47. Selin, *supra* note 29, at 382. *See* Viktor Mayer-Schönberger & Teree E. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, 3 MICH. TELECOMM. & TECH. L. REV. 45, 56 (1997) [hereinafter Mayer-Schönberger & Foster, *Regulatory Web*]. *Contra* Dan L. Burk, *Virtual Exit in the Global Information Economy*, 73 CHI.-KENT. L. REV. 943, 961-972 (1998) [hereinafter Burk, *Virtual Exit*].

48. FRANCES CAIRNCROSS, THE DEATH OF DISTANCE (1997); Goldsmith, *Against*

national borders and boundaries.[49]

Even worse for national laws, content can be transferred almost without cost and instantaneously across the globe, enabling regulatory arbitrage.[50] Consumers, too, seeking information that is illegal in their own jurisdiction, can go out on the Internet, disguise themselves, take on another identity - and thus simulate their presence in another jurisdiction - and obtain the information they desire.

Well, the traditionalists respond, national regulation may still be possible, it just may involve higher costs.[51] If nations cannot regulate the flow of information at its source, they can certainly attempt to regulate the flow of information into their jurisdictions and within it.[52] Singapore,[53] Vietnam[54] and China[55] have done and continue to do just that, for example, through elaborate filtering systems. Such regulation might be costly and less than perfect, but it is nevertheless an option.[56] Moreover, even if regulatory arbitrage might work in theory, it is not certain it will work in practice. The Internet is not a perfect network, all of the links of which are equally strong. In fact, the United States holds

Cyberanarchy, *supra* note 33, at 1203 (describing this phenomenon as the "boundary-destroying" view of cyberspace).

49. Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, *in* BORDERS IN CYBERSPACE 84, 85, 89 (Brian Kahin & Charles Nesson eds., 1997) [hereinafter Reidenberg, *Rule-Making*].

50. *See* Froomkin, *Arbitrage*, *supra* note 27; Selin, *supra* note 29, at 381-82 (speaking of the "lowest common denominator" that would result in such a regulatory arbitrage); David G. Post, *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3, ¶¶ 39-41, *at* http://www.warthog.cc.wm.edu/law/publications/jol/articles/post.shtml (last visited Nov. 15, 2002); *see also* Trachtman, *supra* note 25, at 577 ("One dark side of cyberspace is its facilitation of private sector jurisdictional evasion and, at least in some contexts, its facilitation of regulatory arbitrage").

51. Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1222 (stating that "[i]n cyberspace as in real space, offshore regulation evasion does not prevent a nation from regulating the extraterritorial activity"); Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 488 (noting that "the question is the cost of modification and the degree of effectiveness"); *see also* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1229 ("What is not well-founded, however, is the belief that imperfect regulation means ineffective regulation."); Wu, *supra* note 25.

52. Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1223-24.

53. Froomkin, *Arbitrage*, *supra* note 27, at 144; Joshua Gordon, *East Asian Censors Want to Net the Internet*, CHRISTIAN SCI. MONITOR, Nov. 12, 1996, at 19.

54. Froomkin, *Arbitrage*, *supra* note 27, at 144; Mayer-Schönberger & Foster, *Regulatory Web*, *supra* note 47, at 48.

55. Graham Hutchings, *Beijing Builds Barriers Against an Electronic Democracy Wall*, DAILY TELEGRAPH, Mar. 15, 1996, at 38; Sheila Tefft, *China Attempts to Have Its Net and Censor It Too*, CHRISTIAN SCI. MONITOR, Aug. 5, 1996, at 1; *see also* Froomkin, *Arbitrage*, *supra* note 27, at 145.

56. Froomkin, *Arbitrage*, *supra* note 27, at 148 (stating that "a country that wishes to ban electronic mail to or from foreign anonymous remailers will find violations hard to detect unless it expends great resources on monitoring all national traffic"); Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1224.

a commanding lead over the other nations of the world in available communications bandwidth. About two thirds of the global Net traffic is within the United States.[57] Consequently, Internet resources are very unequally distributed across the globe, such that some parts of the network are orders of magnitude faster than others. Being forced to move one's information site from North America to somewhere else will not make reaching the relocated information impossible, but it will hamper access through problems generated by small bandwidth, low reliability and substantial waiting times. Given the short attention spans of users in Internet time, these impediments, although not fatal in theory, may render such information inaccessible in practice. Moreover, a suitable regulatory regime may not be the only factor in the decision of where to locate a business. In addition, recent studies have shown that "race-to-the-bottom" effects might be less prevalent than originally thought.[58] Hence, regulation of Internet conduct and enforcement would remain sufficiently effective at the national level, at least for the dominant nations in the global information economy.

The opponents of national regulations may concede this point – for now. But this situation is bound to change, they may add. Even where these network inefficiencies exist, the market will make sure that they soon disappear. If Caribbean islands turn into well-paid hosts of elsewhere-illegal information providers, they will waste no time expanding their infrastructures to permit even more such providers to flock to them. In the Internet economy, the market incentives are tilted against the states and their enforcement efforts.

This imagined debate between the regulatory traditionalist and the cyber-opponent ends, like many such arguments, with the regulatory skeptic smelling rhetorical victory. Of course, not all debates on state-based cyber-regulation closely resemble this archetype. Some cover only parts, others might continue with lesser arguments or speculations about the practical effects and possible efficiencies of nation-driven policies. But in almost all such debates, one can identify parts of the debate just described: the perfect-enforcement assumption, the sufficient-enforcement rebuttal, the "death of distance" reasoning, the argument about regulation cost and unequal network topology, and the rejoinder of invisible and merciless market forces.

57. Chris Jones, *New Net Hub Will Speed Data to Latin America*, Wired News, *at* http://www.wired.com/news/technology/0,1282,3863,00.html (May 14, 1997) (stating that "the two major North American Network Access Points, which are located in San Francisco and Washington, DC . . . handle about 75 percent of Net traffic worldwide").

58. Burk, *Virtual Exit*, *supra* note 47, at 964-69.

Sometimes, opponents of national regulations for cyberspace "enrich" their arguments by introducing into the debate a different model, one based on "self-regulation," and juxtaposing it with the one based on national laws. In so doing, they muddy the discursive waters, mixing arguments against governance through national lawmaking with arguments for self-governance based on their conception of cyberspace. Filtering out the critique of state governance, one discovers a second debate, this one time about the perceived virtues (and vices) of self-regulation.

2. The Cyber-Separatist Discourse

Cyber-separatists look at cyberspace as a social space separate and apart from the real world.[59] Consequently, they argue that existing national norms should not be or are not applicable to cyberspace, the "new frontier."[60] Some of them, like John Perry Barlow, want cyberspace to remain devoid of any rules, free from any form of governance.[61] Having a choice, they argue, one should abstain from regulating cyberspace altogether.[62]

59. *See* Johnson & Post, *Law and Borders*, *supra* note 3, at 1402 (arguing that cyberspace is a distinct "place"). *But see* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1201; Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 476. For more general discussions of this point, see Katsh, *supra* note 18; Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 895-99 (1996); Reidenberg, *Lex Informatica*, *supra* note 16.

60. *See* Boyle, *supra* note 18, at 179 ("If the king's writ reaches only as far as the king's sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular sovereign."); Johnson & Post, *Law and Borders*, *supra* note 3, at 1378 ("[T]rying to tie the laws of any particular territorial sovereign to transactions on the Net, or even trying to analyze the legal consequences of Net-based commerce as if each transaction occurred geographically somewhere in particular, is most unsatisfying.").

61. *See*, *e.g.*, John Perry Barlow, *A Cyberspace Independence Declaration*, *at* http://www.eff.org/barlow (last visited Nov. 15, 2002) ("Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.").

62. *Cf.* Burk, *Federalism*, *supra* note 40; John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207 (1997); Reidenberg, *Rule-Making*, supra note 49; *see also* Boyle, *supra* note 18, at 178 ("For a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation."). Among the most frequently cited regulation skeptics are David Post and David Johnson. *See* Johnson & Post, *Law and Borders*, *supra* note 3; Post, *supra* note 25; David G. Post & David R. Johnson, *The New "Civic Virtue" of the Internet*, *in* THE EMERGING INTERNET (Annual Review of the Institute for Information Studies, Feb. 1998), *available at* http://www.cli.org/paper4.htm (last visited Nov. 15, 2002). Courts have made similar arguments. *See*, *e.g.*, ACLU v. Reno, 929 F. Supp. 824, 832 (E.D. Pa. 1995), *aff'd*, 521 U.S. 844 (1997) ("[I]t would not be technically feasible for a single entity to control all of the information conveyed on the Internet."); Digital Equip. Corp. v Altavista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997) ("To impose traditional territorial concepts on the commercial uses of the Internet has dramatic implications, opening the Web user up to inconsistent regulations throughout fifty states, indeed, throughout the globe. It also raises the

Like their counterparts in the debate over the role of state-based regulation, opponents of the cyber-separatist's approach have no difficulty in identifying severe flaws in the cyber-separatist argument. They remind the cyber-separatists that even if cyberspace is conceived as a separate space in which people interact with each other, it is still a social space, full of social interaction. Wherever there are social interactions, they go on, conflicts will arise and will have to be resolved.[63] One very familiar way to limit the potential for conflict within a society is to develop a societal system of rules – a framework of accepted behavior – and enforce it. Indeed, it is precisely such a system of rules that differentiates even the most primitive societies from the lone savage.[64] Therefore, if, as Barlow seems to advocate, no governance structures whatsoever should be instituted in cyberspace, then he is aiming not so much for cyber-separatism as cyber-anarchy.[65]

Moreover, even if one succeeds in keeping formal governance structures out of cyberspace, one might still be unable to abolish rules governing conduct in cyberspace altogether. Social spaces devoid of formal rules will develop informal rules of accepted behavior.

possibility of dramatically chilling what may well be 'the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen.'") (quoting *ACLU v. Reno*, 929 F. Supp. at 881); Am. Library Assoc. v Pataki, 969 F. Supp. 160, 183 (S.D.N.Y. 1997) ("Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace.").

63. *See, e.g.,* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F Supp 1119, 1121 (W.D. Pa. 1997) (plaintiff manufacturer of "Zippo" tobacco lighters alleging trademark dilution, infringement, and false designation against online computer news service for use of domain names "zippo.com," "zippo.net," and "zipponews.com"); Naxos Res. (U.S.A.) Ltd. v. Southam, Inc, 1996 U.S. Dist. LEXIS 21757, *12-15 (C.D. Cal.) (plaintiff asserting defamation by defendant through publication of article in LEXIS); Panavision Int'l v. Toeppen, 938 F. Supp. 616, 619 (C.D. Cal. 1996) (plaintiff alleging interference with economic advantage on account of defendant's registration of domain name with view to compelling plaintiff and trademark holder to purchase that domain name); Religious Tech. Ctr. v F.A.C.T.NET, Inc., 901 F. Supp. 1519, 1521-22 (D. Colo. 1995) (plaintiff alleging copyright infringement by nonprofit corporation, that maintained library of materials concerning plaintiff and allegedly posted unpublished, copyrighted documents to international computer network); *see also* Sally Greenberg, *Threats, Harassment, and Hate On-line: Recent Developments*, 6 B.U. Pub. Int'l L.J. 673, 673-75, 680-84 (1997) (discussing harassment and threats on the Internet); *Anatomy of a Cyber Break-in*, NEWSWEEK, Feb. 27, 1995, at 63 (discussing data theft).

64. *See generally* Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action*, 63 U. CHI. L. REV. 133, 165-97 (1996) (applying economic theory of solidarity to explain how informal trade associations, religious groups, and families may be used to regulate behavior).

65. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33. Francois Dessemontet calls cyber-anarchy an American concept. Francois Dessemontet, *The European Approach to E-Commerce and Licensing,* 26 BROOK. J. INT'L L. 59 (2000); Weiser, *supra* note 25, at 822. For a broader use of the word "cyber-anarchy" to denote competing and overlapping jurisdictions in cyberspace, see Neil Weinstock Netanel, *supra* note 25, at 443-46 (2000).

Netiquette,[66] the Internet etiquette developed over time in newsgroups and email lists, is a perfect example. Netiquette is a quite participatory and inclusionary set of rules that have evolved slowly over time and largely by consensus among netizens.[67] It is also a set of rules originating during a time of limited participation in cyberspace, when netizens, regardless of their geographic location, shared many of the early ideals of the Net. This idyllic infancy of cyberspace has disappeared as the Net has become an international mass phenomenon. More and more, the original netiquette has been replaced by a mixture of commercial rules and crude forms of social Darwinism. Whoever shouts loudest will be noticed first. Surely this cannot be the optimal model for regulatory governance.[68]

But there is a second flavor of cyber-separatism, quite apart from Barlow's extreme approach. Its proponents do not argue for the formal regulatory void of the cyber-anarchists. Instead they aim for self-regulation of cyberspace.[69] They point out that any free society must be governed only by its own rules. In their arguments, they recall the plight

66. *Netiquette—Webopedia Definition and Links*, internet.com, *at* http://webopedia.internet.com/TERM/n/netiquette.html (last visited Nov. 15, 2002) (defining "netiquette" as a "[c]ontraction of *Internet etiquette,* the etiquette guidelines for posting messages to online services, and particularly Internet newsgroups").

> Netiquette covers not only rules to maintain civility in discussions (i.e., avoiding flames), but also special guidelines unique to the electronic nature of forum messages. For example, netiquette advises users to use simple formats because complex formatting may not appear correctly for all readers. In most cases, netiquette is enforced by fellow users who will vociferously object if you break a rule of netiquette.

Id.

67. *Cf.* Arlene H. Rinaldi, *Questions/Answers: Will Netiquette Evolve Much?*, The Net: User Guidelines and Netiquette, *at* http://www.fau.edu/netiquette/net/netlife.txt (last visited Nov. 15, 2002) ("'Old timers' . . . generally are very patient with newbies and tend to guide them to understanding the established long time 'rules' which have evolved.").

68. *See* Mark A. Lemley, *The Law and Economics of Internet Norms,* 73 CHI.-KENT. L. REV. 1257, 1268 (1998) (suggesting that "[t]here is no evidence these values [embodied in netiquette] are shared by the overwhelming majority of those now on the Net.")

69. What is referred to here as self-governance or self-regulation in cyberspace is to be understood in the broadest sense, encompassing all the different modes of "private ordering," which some commentators have preferred over self-regulation. *See, e.g.,* Niva Elkin-Koren, *Copyrights in Cyberspace - Rights Without Laws?,* 73 CHI.-KENT. L. REV. 1155 (1998); Lemley, *supra* note 68; Bomse, *supra* note 35; *see also* Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998); Wiliam W. Fisher, *Property and Contract on the Internet,* 73 CHI.-KENT. L. REV. 1203 (1998); Lawrence Lessig, *Social Meaning and Social Norms,* 144 U. PA. L. REV. 2181 (1996); Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace,* 73 CHI.-KENT. L. REV. 1295 (1998) (suggesting that as all law is public, it depends on a legal framework, even in cyberspace). On "private ordering," see generally ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Avery Katz, *Taking Private Ordering Seriously,* 144 U. PA. L. REV. 1745 (1996).

of the Founding Fathers and their fight for independence and self-rule.[70] They reason that subjecting people in cyberspace to rules conceived outside of it necessarily involves the enforcement of rules devised by one society against members of another, thus contradicting the fundamental principle of self-government. Cyberspace, it is argued, needs to be governed, but not by some distant, unaffected national legislature (again evoking powerful historical metaphors of American suffering under the British Crown); rather, it should be governed by the people who are actually affected, the people interacting in cyberspace: the netizens themselves. Self-regulation, they argue, is the single best way to ensure the legitimacy of governance.[71]

Self-rule and self-regulation have very strong, positive ideological undercurrents. They sound very American and thus resonate with many of the largely American, suburban, middle-class people on the Net today.[72] But the call for self-regulation of cyberspace has its limits. Opponents point out that, regardless of whether cyberspace is a separate place from the physical world or not, the human beings who interact in it are real, living in that physical world.[73] They might utilize technologies to interact with each other, but these are interactions nevertheless among real people living in the real world. Nobody resides in cyberspace without a real-life presence. Why, then, should people's behavior not be subject to existing rules simply because they use

70. David Post links self-regulation of cyberspace with Thomas Jefferson's idea of decentralized lawmaking. Post, *supra* note 25, at 163-65. National governance of cyberspace, to him, is acting in the vein of Alexander Hamilton, abandoning Jeffersonian ideas. *Id*.

71. *But cf.* Netanel, *supra* note 25 (questioning whether self-regulation advances liberal democratic ideals).

72. As of the first quarter of 2001, over forty percent of people with internet access live in the United States or Canada. Michael Pastore, *429 Million Online Worldwide*, *at* http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_782281,00.html (June 11, 2001). Further statistical data allow us to picture a typical U.S. Internet user as White or Asian American/Pacific Islander, of workforce age (25-49), with at least some college education, and earning more than $50,000 a year. See DEPARTMENT OF COMMERCE, FALLING THROUGH THE NET: TOWARD DIGITAL INCLUSION 33-60 (2000), *at* http://www.ntia.doc.gov/ntiahome/fttn00/Falling.htm#33 (last visited Jan. 8, 2003).

73. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1215-16 (arguing that "[c]yberspace is not, as the skeptics often assume, a self-enclosed regime"); Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 476 (stating that "[t]he Internet is not, as many suggest, a separate place removed from our world"); Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code,* 8 SETON HALL CONST. L. J. 703, 709 (1998) (stating that the notion of cyberspace as a separate space is "cyber-romanticism at its worst"); *see also* Fried, *supra* note 11, at 618 (describing Lessig's use of the "cyberspace metaphor" as "hyperbolic, if not somewhat fatuous"). Despite Fried's criticism, Lessig has been quite forthright about cyberspace *not* being a separate space. LESSIG, *supra* note 19, at 21 ("You are never *just* in cyberspace; you never just *go* there. You are always both in real space and in cyberspace at the same time." (emphasis in original)).

technologies to communicate their actions?

In essence, whereas the cyber-separatists contend that one should not extend the regulation of apples to oranges and thus confuse the two, their opponents counter that in cyberspace every orange is also an apple, every netizen is also a citizen in a physical community. The first battleground of arguments is about the nature of the cyber-community (or cyber-communities) and its (their) members. The second discursive thread, concerning the legitimacy dimension of cyberspace self-regulation, focuses more on the principal shortcomings of self-regulation.

Less radical cyber-separatists concede that people interacting in cyberspace also have a physical presence. But, they argue, that should not preclude them from setting up a system of self-governance. In the physical world, there are numerous examples of groups forming communities and creating self-regulating regimes: from corporations to nonprofit organizations, from business associations to sports clubs. We are all members of various overlapping and/or nested real-world communities; being a member of one of them, and thus subject to its system of governance, does not preclude us from being a member of (and thus subject to) another. For a system of self-governance to work, therefore, one needs only to understand that the assessment of one's actions depends on the community involved.

Opponents of this modest form of cyber-separatism may openly accept such a premise and still object to it. How, they ask rhetorically, does a system of self-regulation deal with the problem of illegal information, such as child pornography? Does self-regulation imply that the networked pedophiles of the world can come together in cyberspace and govern themselves? Is "self-regulation" code for the prisoners guarding the prison?[74]

Such an example is charged, emotional, and perhaps may sound simplistic. But the underlying question is a valid one. How far is self-regulation to go? What is the appropriate community level in cyberspace for purposes of self-regulation? All netizens, or only a subset of them? And in which regulatory areas? In the physical world we have found ways to define the ability and competence of communities to govern themselves. But as many disputes over competency and appropriateness in self-governance attest, how to define these borders is not always clear.[75] Moreover, the intricacies of

74. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1216, 1242 (pointing out that some activities in cyberspace may not be suitable for self-regulation).

75. *See* Jonathan I. Edelstein, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 231, 284-86 (1996); Lemley, *supra* note 68 at

cyberspace and its plentitude of community overlap may not only exacerbate this ambiguity but also threaten to reopen the Pandora's box of governance and delegation.[76] In the end, self-regulation may pose as many fresh questions about the legitimacy of such an enterprise as it intends to answer.[77]

Cyber-separatists might be undeterred by such problems, which they perceive as minor. After all, their claim that self-regulation implies legitimate governance is strong, and the need to delineate borders of competence is not unique to cyberspace. Furthermore, some cyber-separatists may move away from a normative discourse—that is, one focused on what kind of governance there ought to be—and toward a more descriptive one—that is, one focused on what kind of governance there is—, arguing that even though self-governance in cyberspace is not without problems and pitfalls, it is nevertheless more practicable than state-based governance.[78] Opponents may not have to counter such descriptive and often anecdotal claims of legitimized cyberspace self-governance. Instead, they may just point at another important dimension of the discourse: enforcement. How, they ask, can a cyber-community enforce its rules with no physical police force at hand?[79]

Cyber-separatists respond by drawing on another historical parallel.

1268-69.

76. *See* Lemley, *supra* note 68, at 1270. This problem, of course it not unique to cyberspace. The European Union, itself a complex governance institution, has been struggling with the issue of delegation for decades. *See* ANDREAS FØLLESDAL, SUBSIDIARITY AND DEMOCRATIC DELIBERATION (ARENA Working Paper No. 99-21, 1999); THEODOR SCHILLING, SUBSIDIARITY AS A RULE AND A PRINCIPLE, OR: TAKING SUBSIDIARITY SERIOUSLY (Jean Monnet Center Working Paper, 1995), *available at* http://www.jeanmonnetprogram.org/papers/95/9510ind.html.

77. Recent research has shown that self-regulation is much more complex and multi-faceted that any of the more deterministic legal or economic explanations. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990).

78. Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1200 (1998) (untangling such normative and descriptive claims).

79. *See* Mefford, *supra* note 32, at 213 ("Methods of social self-regulation such as excluding offending users from the community and communicating their behavior to others are losing impact as the size of the Internet now allows a user who has violated social rules in one area of the Net to move to another area . . . . It is clear, therefore, that the Internet must have law and order if it is to become a stable marketplace and if it is our belief that people ought to be protected from disreputable conduct. What is unclear, however, is what this law will be, who will have the opportunity to write it, and who will enforce it.")

> In contract law, self-regulation on the Net does not give us much in terms of power over territory [. . .] at least as far as contracts are concerned**,** enforcement power still rests with those who can seize property and garnish wages to satisfy judgments. That is to say, states must still play a role in this new regime because they monopolize the exercise of police power.

Id. at 235.

They liken self-regulating cyber-communities to those of medieval merchants, which would subject themselves to a common regulatory framework.[80] Violators of these rules could be expelled from the community of merchants. Similarly, medieval cities, in addition to the traditional enforcement methods of physical punishment, possessed an even stronger weapon: They could also expel a member from the city and thus from the protection of its outer walls.[81] Expulsion from the "free" city back into the system of feudalism acted as the ultimate deterrence, in turn strengthening enforcement. Cyber-communities possess a similarly effective tool of deterrence.[82] They, too, can expel members who continue to violate community rules.[83] Members will obey the rules, particularly if the total costs—physical, financial and emotional—incurred when one is expelled are high. Lawrence Lessig has made a similar argument.[84] If such an argument is valid, self-regulation in cyberspace would have at its disposal a powerful means of enforcement.

Opponents, however, see flaws in this line of reasoning, too. Enforcement based on the threat of expulsion rests entirely on the costs of punishment outweighing the benefits of breaking the rules. But

80. Johnson & Post, *Law and Borders*, *supra* note 3, at 1389-90 (suggesting that "the most apt analogy to the rise of a separate law of Cyberspace is the origin of the Law Merchant"); Mefford, *supra* note 32, at 223-26 (suggesting that the "similarities between the needs for a Lex Mercatoria and the needs of dispute resolution and law in Cyberspace are remarkable"); Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance,* 5 IND. J. GLOBAL LEG. STUD. 423, 427 (1998) [hereinafter Perritt, *Sovereignty*] ("Cybernauts most closely resemble medieval merchants who developed substantive rules and practices to regulate transnational trade - the lex mercatoria - outside traditional polictical institutions."); Reidenberg, *Lex Informatica*, *supra* note 16, at 553-54; Trachtman, *supra* note 25, at 579-80; *see also* Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1051-53 (1994); David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law, in* COORDINATING THE INTERNET 81-90 (Brian Kahin & James H. Keller eds., 1997) [hereinafter Johnson & Post, *Governed*].

81. *See* MARY C. MANSFIELD, THE HUMILIATION OF SINNERS: PUBLIC PENANCE IN THIRTEENTH-CENTURY FRANCE 266-67, 276 (1995) (discussing public display of punishment); *cf*. Gerald R. Miller, *Banishment—A Medieval Tactic in Modern Criminal Law*, 5 UTAH L. REV. 365, 365-67 (1957) (discussing banishment); William Garth Snider, *Banishment: The History of Its Use and a Proposal for Its Abolition Under the First Amendment*, 24 NEW ENG. J. ON CRIM. AND CIV. CONFINEMENT 455, 459 (1998) (discussing banishment).

82. However, the leading cyber-separatists have avoided making that point, perhaps because linking virtual communities with medieval cities (and their pronounced, fortified geographic borders) is less suitable for arguing for an "un-territorial" system than suggesting a connection to merchants.

83. *See* Gibbons, *supra* note 25, at 523 n.331; Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1214 (conceding that cyber-communities can "establish private enforcement regimes"); Mefford, *supra* note 32, at 235 ("[S]ysops wield a very effective punishment in banishment.").

84. Lessig, *Zones*, *supra* note 43, at 1405.

expelling someone from a virtual community hardly carries with it the badge of life-threatening danger that expulsion from the physical protection afforded by the enclosed city did in medieval times. In cyberspace, much more so than in real life, people belong to many different communities at once. Being expelled from one of them might be an inconvenience, but little else. In fact, if a person is expelled from one virtual community, cyberspace offers dozens of others for her to join; and in cases where this is not feasible, cyberspace permits the cyber-exile to form a *new* virtual community at almost no cost. As a result, the cost of being expelled from most cyber-communities is minimal, leaving members with little incentive to obey the rules. Thus, what has heretofore been an argument for self-regulation on the legitimacy dimension—the fact that many (sometimes even overlapping) groups can legitimately and effectively govern themselves—is now turned against self-regulation in the enforcement area as concurrent membership in virtual communities decreases the ability of the community to police through threatened expulsion. And without strong enforcement mechanisms, self-regulation is severely crippled.[85]

Cyber-separatists may try to improve this bleak picture by adding some rays of light. Some cyber-communities may have unique qualities that make membership and participation in them sufficiently desirable that being expelled from them creates the deterrent effect required for their self-governance.[86] Being expelled from one of the many online communities debating the intricacies of fly-fishing may hardly deter – one could just join another such community, or (dare I suggest?) switch sports. But expulsion from America Online (AOL) may be a fairly strong threat, implying that one would not only lose access to content, and a known virtual space interface, but through the loss of one's email address and instant messaging "handle" encounter the difficulty of maintaining one's social network in cyberspace. And if one takes the cyber-community as a whole, expulsion not just from any single virtual community but from cyberspace itself in a global information society may, indeed, for some end up feeling just as catastrophic as being

85. *See* Lemley, *supra* note 68, at 1272 (stating that "most mini-communities are generally easy to enter and exit - even more so than the Net itself").

86. The deterrent effect of expulsion is dependent upon the uniqueness of the community, as well as its ability to enforce an expulsion. For a gripping tale of expulsion and the difficulties of enforcement, see Julian Dibbell, *A Rape in Cyberspace; or, How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society, in* FLAME WARS 237-61 (Mark Dery ed., 1994).

expelled from a medieval city.[87]

The desire to create a system of self-regulation for all of cyberspace, the critics will interject, is nothing less than asking for a global regime of governance for everyone online. Such "self"-regulation is a far cry from the cyber-separatists' ideal of small-scale, community-based self-governance. In the end, it aspires to govern communication among all users of the Internet. If this is what cyber-separatists are arguing for, they are arguing for world cyber-governance, with all the difficult legitimacy issues that self-regulation originally proposed to cure. At this point, the self-regulatory discourse might blur into another, third discourse on cyber-governance.

3. The Cyber-Internationalist Discourse

Cyber-internationalists see cyberspace as an already globalized world community. If the Net is linking the citizens of the world, they argue, one must transcend the idea that specific areas of governance can be geographically delimited. The appropriate level of governance for cyberspace, therefore, is international, and the correct means of governance international law.[88]

Opponents of such an internationalist approach to cyberspace governance quickly point out the lack of legitimacy involved in such an approach, the very problem that limits the use of international law in other areas.[89] Given the vastly different views on culture and values

87. Of course, such expulsion from cyberspace is currently difficult to institute, but that could change if it is deemed politically and economically desirable, as the technology exists. *See* Gibbons, *supra* note 25, at 523 (differentiating between "removal from the relevant Cyberian community" and being "ultimately disconnected from the system").

88. *See* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 521 (1998) ("Most laws were conceived in and for a world of atoms, not bits . . . national law has no place in cyberlaw.") (quoting NICHOLAS NEGROPONTE, BEING DIGITAL 237 (Vintage Books 1995)); Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 491 (1998) (stating that "international harmonization [of cyberlaw] is a solution"); Michael H. Spencer, *Anonymous Internet Communication and the First Amendment: A Crack in the Dam of National Sovereignty*, 3 VA. J.L. & TECH. 1, 36 (1998) (maintaining that the global nature of cyberspace communication "foreshadow[s] the growth of international law at the expense of national sovereignty"); Selin, *supra* note 29, at 385 ("The creation of an international convention, comparable to one like the Convention on the Law of the Sea, is the answer to the problems inherent to the Internet and the lack of adequate law covering it."); *see also* Susan Thomas Johnson, *Internet Domain Name and Trademark Disputes: Shifting Paradigms in Intellectual Property,* 43 ARIZ. L. REV. 465, 488-89 (2001); Henry H. Perritt, Jr., *The Internet is Changing International Law,* 73 CHI.-KENT. L. REV. 997, 998 (1998) [hereinafter Perritt, *Changing*]. A more cautious version is proposed by Burk, *Virtual Exit*, *supra* note 47, at 985-89 (suggesting as an alternative to international cooperation a supranational regime setting minimal standards or implementing public property rights).

89. For such a critical view of international law, and especially international customary law, see Curtis A. Bradley & Jack L. Goldsmith, *Customary International Law as Federal Common*

across nations, how can one reasonably assume that a consensus would exist among them on how to govern cyberspace?[90]

Cyber-internationalists reply that the size of the international legal framework has constantly increased over the last decades. An ever-increasing stream of economic, political and legal issues have become subject to international codification and formal cooperation, from the establishment of the World Trade Organization[91] to the convention on the ban of landmines.[92] Furthermore, international law is no longer restricted to simple cross-border issues; like it or not, it has extended deep into policymaking at the national level.[93] In times of globality, the argument goes, the momentum is clearly on the side of international governance.[94]

But opponents quickly respond that cyberspace is a communicative space, linked deeply to freedoms of speech and information, as well as cultural values in nation-states. Any attempt to harmonize cyber-regulation on a global scale and by consensus would have to overcome supreme hurdles, as nations would have to give up part of their fundamental power, particularly the power to control societal communication, and would likely be reluctant to do so. One might find agreement among the participants on business issues, based on pragmatic consideration among them that the sum is more than its individual parts. But giving away control of communication is different,

Law: A Critique of the Modern Position, 110 HARV. L. REV. 815 (1997).

90. Perritt, *Sovereignty*, *supra* note 80, at 430 ("The range of important interests and values that the Internet affects makes the prospects for such harmonization or universal choice-of-law approach unlikely. International governance of Internet issues, thus, appears to be a chimera.").

91. Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Apr. 15, 1994, RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS—LEGAL TEXTS (1994), 33 I.L.M. 1125 (1994) (agreement establishing the World Trade Organization); General Agreement on Tariffs and Trade, Oct. 30, 1947, 55 U.N.T.S. 194 (original GATT).

92. *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction*, Sept. 18, 1997, 36 I.L.M. 1507 (1997).

93. *See, e.g.*, Aryeh Neier, *The Military Tribunals on Trial*, N.Y. REVIEW OF BOOKS, Feb. 14, 2002 (addressing the domestic debate on the categorization (and thus treatment) of Al-Quaeda fighters in relation to the Geneva Convention); Ronald Dworkin, *The Trouble with Tribunals*, N.Y. REVIEW OF BOOKS, April 25, 2002. For an earlier controversy, see Filartiga v. Pena-Irala, 630 F.2d 876 (2d Cir. 1980) (using international customary law - the prohibition of torture - in a domestic civil action). *See also* Trachtman, *supra* note 25, at 570 ("There have never been many issues that one country can completely deal with on its own; cyberspace simply accelerates the realization of this fact.").

94. Perritt, *Changing*, *supra* note 88, at 999 (arguing for "[h]armonization, greater transparency, more democracy, and greater influence by entities and groups of both supernational and subnational scope"); Trachtman, *supra* note 25, at 571 ("Finally, I see moration [sic] among states to establish rules of prescriptive jurisdiction, harmonized laws, and international organizations to apply these rules.").

and international consensus on that issue difficult to imagine.[95]

Cautious cyber-internationalists agree with this contention. They argue, however, that some international consensus is bound to arise, if it is not already there. Liberal democracies especially, they contend, have to gain from the free flow of information brought about by the Internet. This positive spillover will create incentives for other nations to change and join the group of liberal democracies, and through alignment create more homogeneity internationally.[96] Other developments in international law similarly may indicate a movement towards consensus. For instance, *jus cogens*, embodying peremptory norms of international law, already provides a small, yet valuable, set of universally held norms. International cyber-governance could start by building on them.[97]

But such an argument will not placate the opponents. They juxtapose the ideal of liberal democracies spreading like wildfire and thus enabling international law with a realist view of nations fighting for their competitive advantage, and conclude that peremptory norms of international law will provide too little too late—at best.[98] Switching to the issue of enforcement and mirroring arguments against state-based cyber-governance, opponents then argue that international cyber-governance will work only if it is truly global, if all the states whose citizens partake in the global Net adhere to its rules. Merely one rogue nation unwilling to play its part in the global orchestration of cyber-governance could severely undermine the system by permitting illegal information to be introduced into cyberspace through its network. Hence, enforcement of cyberlaws, they conclude, must be truly global to be effective.

At this point in the debate, cyber-internationalists might use a line of argument the traditionalists employed in their defense: Resources in

95. Perritt, *Jurisdiction*, *supra* note 27, at 108 (conceding that the proponents of "new laws to restrict indecent material are likely to oppose the loss of sovereignty they perceive to be associated with international machinery and are most likely to focus their efforts to enact new legislation and to enlist the national prosecutors at the local, state or (at most) national levels").

96. Perritt, *Changing*, *supra* note 88, at 998 (stating that the Internet reinforces international transparency, democracy, and harmonization); Perritt, *Jurisdiction*, *supra* note 27, at 128 (concluding that the Internet "presents a potent opportunity in the evolution of the international legal system"); Perritt, *Sovereignty*, *supra* note 80.

97. The author himself has fallen victim to the temptation of such an argument. *See* Mayer-Schönberger & Foster, *Regulatory Web*, *supra* note 47; *see also* Viktor Mayer-Schönberger & Teree E. Foster, *More Speech, Less Noise: Amplifying Content-Based Speech Regulations Through Binding International Law*, 18 B.C. INT'L. & COMP. L. REV. 59 (1995).

98. *See* Goldsmith, *Fallacies*, *supra* note 43, at 1127-31 (suggesting a realist approach); Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 491 (arguing that international approaches may be "hard to achieve").

cyberspace are unevenly distributed, and getting the major players to agree may allow for sufficient levels of enforcement.[99] To this the skeptics might point, as did the skeptics of national governance, to market forces at work in cyberspace that will eliminate network bottlenecks, particularly if there is demand for better access.

Another, potentially more powerful line of argument the opponents might pursue would be to link the necessity of (nearly) universal enforcement back to the question of legitimacy. If a global consensus cannot be reached, but a few nations decide plurilaterally to enact and enforce their own cyber-rules, what legitimacy do they possess to implicitly govern the citizens of states who have not joined the group?[100] If, as traditionalists maintain with some reason,[101] any enforcement on a global network by any group of nations will have implicit effects on all the others, from whence do the cyber-internationalists derive the legitimacy of their proposed regime?[102]

The situation becomes even worse when cyber-internationalists, in order to keep apace with rapid developments in cyber-technology, opt for informal international cooperation[103] rather than formal international

99. *See supra* notes 51-58 and accompanying text.

100. Froomkin, *Empire*, *supra* note 12, at 1114 ("Once the OECD nations agree to a policy among themselves, there are few other nations which would choose to stand up to such pressure.").

101. *See*, *e.g.*, Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1222; Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 488; Wu, *supra* note 25, at 651 ("[W]here widespread usage of the Internet depends on physical components, a government that controls these components can regulate cyberspace."); *see also* discussion *supra* note 58 and accompanying text.

102. *See* Froomkin, *Empire*, *supra* note 12, at 1114 (raising the concern that "[s]upra-national bodies . . . tend to have a 'democratic deficit'").

103. *See, e.g.*, the agreement among the G-8 to battle cybercrimes and cyberterrorism. *Final Communiqué*, G-8 Summit 2001 (Genoa, July 22, 2001), *at* http://www.g7.utoronto.ca/g7/summit/2001genoa/finalcommunique.html ("We encourage further progress in the field of judicial co-operation and law enforcement, and in fighting corruption, cyber-crime, online child pornography, as well as trafficking in human beings."); *Communiqué*, Conference of the G8 Ministers of Justice and the Interior (Milan, February 26-27, 2001), *at* http://www.g7.utoronto.ca/g7/adhoc/justice2001.htm ("encouraging the Group of Anti-terrorism Experts rapidly to achieve further results, with particular enphasis [sic] on the operational problems connected with cyber-terrorism and on the analysis of potentially high-risk international developments" and "[a]ction against high-tech crime, including use of the Internet in child pornography"); *Final Communiqué*, G-8 Summit 2000 (Okinawa, July 23, 2000), *at* http://www.g7.utoronto.ca/g7/summit/2000okinawa/finalcom.htm ("We must take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society."). The Okinawa Charter on Global Information Society sets out the G-8 approach.

> International efforts to develop a global information society must be accompanied by co-ordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures [. . .] are put in place to fight cyber-crime. G8 co-operation within the framework

law as a foundation for governance. In that case, the legitimacy of their system—legitimacy in the democratic, participatory sense of the governed having a say in their government—is stretched so thin that it is all but lost. Enforcement may be a problem for cyber-internationalism, but it pales in comparison to the problem of legitimacy. Representative democracy, the tried and true creator of legitimacy, is nowhere in sight for unilateral action by a plurality of states, particularly when those states are attempting to govern a global network.[104] And so, once again, the skeptics seem to gain the upper hand.

At the end of this overview of three discourses on cyber-governance, a few words of caution are in order. First, the debates recounted here are not meant to cover every possible governance argument. They are nothing more than discursive structures, chains of some of the most common arguments for and against certain types of governance proposed for cyberspace. Actual debates about specific regulatory issues in cyberspace neither contain all the arguments described here, nor contain them in the order presented. What these three debates represent, however, is what one could call ideal type discourses of cyber-governance.

II. THREE LAYERS OF GOVERNANCE

The three types of Internet governance outlined above can be easily identified as state-centered (the traditionalists), self-regulation or community-based (the cyber-separatists), and trans/supranational[105] (the

> of the Lyon Group on Transnational Organised Crime will be enhanced. We will further promote dialogue with industry, building on the success of the recent G8 Paris Conference "A Government/Industry Dialogue on Safety and Confidence in Cyberspace." Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures.

Okinawa Charter on Global Information Society, (Okinawa, July 22, 2000), *at* http://www.g7.utoronto.ca/g7/summit/2000okinawa/gis.htm. International standardization organizations provide another example. On their role, see Stanley M. Besen & Joseph Farrell, *The Role of the ITU in Standardization: Pre-eminence, Impotence or Rubber Stamp,* 15 TELECOMMUNICATIONS POL'Y 311 (1991); Krishna Jayakar, *Globalization and the Legitimacy of International Telecommunications Standard-Setting Organizations,* 5 IND. J. GLOBAL LEG. STUD. 711 (1998); Weiser, *supra* note 25.

104. Goldsmith, *Territorial Sovereignty*, *supra* note 35, at 491 ("International harmonization is a solution to both problems. But harmonization is not a perfect solution because it is sometimes hard to achieve and, more broadly, because it defeats the benefits of decentralized national lawmaking.").

105. There is, of course, an important distinction between a transnational and a supranational approach; yet they have in common that they look beyond the state. *See, e.g.,* William C. Bradford, *International Legal Regimes and the Incidence of Interstate War in the Twentieth Century: A Cursory Quantitative Assessment of the Associative Relationship*, 16 AM. U. INT'L L.

cyber-internationalists).

A deficiency of the debates over these types of governance, as they have been portrayed above, is their implicit "binarity."[106] Viewed structurally, they pit all-or-nothing propositions against each other. Either national laws will be able to govern cyberspace completely or they will not at all. Either self-regulation will provide the one and only answer or it is no answer at all. Either cyberspace is comprehensively regulated internationally or it is not at all. Such a binary choice between two extreme positions, between black and white, does not allow for more nuanced solutions, thereby impoverishing the debates artificially (and without good reason).[107]

There is another more subtle, more complex and perhaps more realistic way to describe these three types of governance for cyberspace. One can conceive them as separate layers in a larger structure of governance, with national regulation sandwiched between self-regulation by communities at the bottom and international regulation at the top (or vice versa).[108] To be sure, this stacking of the various modes of governance does not simply imply a crude ranking based on the complexity of the governance type or on the level of abstraction involved. Neither is it just an ordering based on some notion of geographic proximity, a modified version of the metaphor of concentric circles of closer and wider communities, with the individual at its core.

REV. 647, 664 n.57 (2001) (noting that "although subnational actors (ethnic and indigenous groups), transnational actors (multinational corporations), and supranational actors (the UN) are becoming increasingly important determinations of international relations"); Jeffery A. Hart, *Globalization in Question: The International Economy and the Possibilities of Governance By Paul Hirst and Grahame Thompson*, 4 IND. J. GLOBAL LEG. STUD. 571, 572 (1997) (book review) ("It is meant to represent activities carried out not just by governments of nationstates, but also by supranational organizations like the European Union, transnational actors like the multinational corporations . . ."); *see also* RICHARD FALK, HUMAN RIGHTS AND SOVEREIGNTY 45-51 (1981) (providing a more in-depth discussion of the "supranational logic" and "transnational logic").

106. *See* Niklas Luhmann, *Law as a Social System*, 83 NW. U. L. REV. 136, 140 (suggesting that legal systems—and, by extension, legality—must always have some form of binarity); *see also* Gunter Frankenberg, *Down by Law: Irony, Seriousness, and Reason*, 83 NW. U. L. REV. 360 (1989); Robert J. Lukens, *Discoursing on Democracy and the Law - A Deconstructive Analysis,* 70 TEMPLE L. REV. 587 (1997) (linking binarity to Habermas's theory).

107. To be sure, a number of cyberlaw commentators have been explicit about the need to identify shades of gray. *See* Perritt, *Sovereignty*, *supra* note 80; Henry H. Perritt. Jr., *Economic and Other Barriers to Electronic Commerce,* 21 U. PA. J. INT'L ECON. L. 563, 563 (2000) [hereinafter Perritt, *Barriers*] (suggesting "hybrid forms of international regulation"); Trachtman, *supra* note 25, at 580 ("The rise of cyberspace will not destroy the state. In fact, as Perritt points out, cyberspace may strengthen the powers of the state as well as demean them.").

108. *See* Graeme B. Dinwoodie, *(National) Trademark Laws and the (Non-National) Domain Name System,* 21 U. PA. J. INT'L ECON. L. 495, 521 (2000) (suggesting that a multi-tiered approach is most likely to emerge).

A somewhat crude – much of the early libertarian understanding of cyber-democracy is a bit crude – "anti-federalist" notion of cyber-democracy would see this stacking of layers as the reflection of a certain ordering, based on two fundamental qualities of governance: democratic legitimacy and enforceability.[109] Examining these two qualities, the anti-federalist cyber-theorist will perceive an inverse relationship between them.

1. Legitimacy: According to this anti-federalist conception, communities regulating their own affairs create rules more directly than national or international communities, rules that are—at least to some extent—legitimized by their members.[110] Therefore, one may argue that community rules have the edge over other forms of governance in terms of legitimacy. In nations based on democratic governance, lawmakers derive their legitimacy from popular mandate. Unlike members of a small community, national legislators may be connected neither intimately nor on a daily basis to the citizens they represent.[111] Yet in most cases, they will at least to some extent strive to represent their constituents, even if only to get reelected.[112] Thus nation-states enjoy a certain measure of legitimacy. International governance, however, is further removed from direct legitimacy. To be sure, even on the international level, representatives of elected national governments negotiate international agreements, and national legislatures ultimately decide on them.[113] But the legitimacy of a process whose members are at

109. *See* Niva Elkin-Koren, *Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace*, 14 CARDOZO ARTS & ENT. L.J. 215, 238-40 (1996); Peter P. Swire, *Symposium on Jurisdiction and the Internet: Of Elephants, Mice, And Privacy: International Choice Of Law And The Internet*, 32 INT'L LAW. 991 (1998).

110. The term "legitimacy" is used here in a substantive, not restrictively formal sense; a legitimate norm in a liberal democracy requires transparency, procedural due process, and equity, as well as accountability. *See, e.g.,* F. C. DeCoste, *Introduction*, 38 ALTA. L. REV. 607, 615 (2000) ("For, whatever the particulars of institutional design, the judiciary, as a branch of the liberal democratic state, must be subject to the norms of liberal democratic governance; chief among these, according to any account worth the name, are accountability and transparency."); Richard B. Lillich, *Kant and the Current Debate Over Humanitarian Intervention*, 6 J. TRANSNAT'L L. & POL'Y 397, 402 (1997) ("Kant meant what today we would call a liberal democracy, a society that provides full respect for human rights, including freedom, due process, and equality."); Steven R. Salbu, *Information Technology in the War Against International Bribery and Corruption: The Next Frontier of Institutional Reform*, 38 HARV. J. ON LEGIS. 67, 93 (2001) ("Like technology, transparency supports the continued maintenance of a liberal democracy. Democracy's liberties and freedom then continue to bolster openness and transparency. In an independent, mutually reinforcing manner, technology-driven openness and transparency help to cement democratic institutions. Enhanced free flow of information creates checks and balances, and therefore accountability.").

111. *See supra* notes 86-87 and accompanying text.

112. *See* DENNIS C. MUELLER, PUBLIC CHOICE 1-8 (1979).

113. U.S. CONST. art. VI, § 1, cl. 2 ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under

best legitimized only through one (or more) layers of delegation quite obviously involves less transparency and accountability, and resultantly less legitimacy, than a process whereby the members of a community make the rules for themselves.[114]

2. Enforceability: Whereas one may see legitimacy decrease from the bottom to the top layer of our stacked hierarchy of modes of governance, the ability to enforce rules on a global structure like the Internet arguably increases, as options for regulatory arbitrage diminish. Communities, as has been mentioned, in general have limited enforcement mechanisms. Their strongest method of enforcement is expulsion. Although costs incurred when one is expelled from a virtual community vary widely and can be quite high in real life, being expelled from any cyber-community today is a comparatively limited threat, especially compared with what is often used as an example for the ability of communities to enforce: the ultimate cost of expulsion from a medieval city.[115]

The state has a stronger enforcement mechanism. It can take a citizen's liberty and in some nations even his life. The only possible escape from such enforcement is—analogous to exit from smaller communities—exile.[116] International governance closes this possibility. In a world of truly global governance, there is no longer any place to run to anymore, in which case enforcement, at least in theory, has attained its outer limit. Jurisdictional reach equals the world itself, the very scope and extent of the Net.[117]

---

the Authority of the United States, shall be the supreme Law of the Land . . . ."); U.S. CONST. art. II, § 2, cl. 2 ("[The President] shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur . . . ."). The most recent debate on the scope of the U.S. treaty-making power concerns the implementation of NAFTA and the WTO Agreement. *Compare* Laurence H. Tribe, *Taking Text and Structure Seriously: Reflections On Free-Form Method In Constitutional Interpretation*, 108 HARV. L. REV. 1221 (1995) (arguing that both agreements constitute "Treaties" under Art. VI and need to be ratified by Congress) *with* Bruce Ackerman & David Golove, *Is NAFTA Constitutional?*, 108 HARV. L. REV. 799 (1995) (arguing that such agreements have the character of executive agreements).

114. *See* Froomkin, *Empire*, *supra* note 12, at 1114. For a list of disputes in Lambda Moo's "Object orientated multi user dialogue," see College of Computer Science, *Index of /MOO/lambda/disputes*, *at* http://mirrors.ccs.neu.edu/MOO/lambda/disputes (last visited Nov. 24, 2002). *See also* Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMOO*, J. COMPUTER-MEDIATED COMM., June 1996, *at* http://www.ascusc.org/jcmc/vol2/issue1/lambda.html (last visited Nov. 24, 2002) (providing a general discussion of legislation in LambdaMoo and an introduction to the world of MUDs and MOOs).

115. *See supra* note 87 and accompanying text.

116. *See supra* notes 86-87 and accompanying text.

117. To be sure, I am overstating here the case favoring such a stacked hierarchy of

In essence, if one subscribes to this "anti-federalist" conception of democracy, one is presented with a three-layered hierarchy of cyberspace governance with two fundamental (and desirable) qualities of it—legitimacy and enforceability—pitted against each other. Choosing the "right" layer of governance for cyberspace will, it seems, always involve a *trade-off* between the very values one attempts to maintain; the more attractive any regulatory framework chosen for cyberspace begins to look in terms of legitimacy, the less attractive it is on account of enforceability. In fact, one could argue that some of the raging debates about the appropriate regulatory mechanism for cyberspace exist precisely because of this underlying tension, this "tragic choice".[118]

[CHART HERE]

A superficial look at the discourses described above strengthens this view. Both values are strongly present in all three of them. In fact, the arguments brought forward by the disputants seem to conform to the hierarchy of layers suggested. Traditionalists face claims of lack of both legitimacy and enforceability of national norms in a global network. Cyber-separatists grapple mainly with the hurdle of limited enforceability, whereas cyber-internationalists wrestle mostly with the question of legitimacy. Given this structural trade-off, the quest for the best solution to governing cyberspace—enacting a regulatory framework that is both legitimate and enforceable—seems futile, leading almost by definition to suboptimal results. Is cyber-regulation really nothing but a continuous zero-sum game of trade-offs among equally important values?

A closer look at the arguments made in the discourses above reveals a more complex picture. The cyber-separatists' problem is not limited to enforcement. In fact, for some cyber-communities the deterrence of exclusion may be a workable enforcement mechanism.[119] But, as we have seen, cyber-communities may surprisingly face legitimacy problems as well. To keep the edge in the race against traditional nation-based lawmaking (and its legitimizing processes), a community-based private ordering must be deeply legitimizing. Intertwined with the

governance. For more nuanced discussions, see FRITZ SCHARPF, GOVERNING IN EUROPE: EFFECTIVE AND DEMOCRATIC? (1999). On the foundation of enforcement authority, see generally JOSEPH RAZ, THE MORALITY OF FREEDOM (1988).

118. *See generally* GUIDO CALABRESI & PHILIP BOBBITT, TRAGIC CHOICES: THE CONFLICTS SOCIETY CONFRONTS IN THE ALLOCATION OF TRAGICALLY SCARCE RESOURCES (1978).

119. *See supra* notes 86-87 and accompanying text.

issue of legitimacy is the question of the appropriate cyber-community to regulate itself.[120] Are, for instance, some governance issues reserved for higher levels of cyber-communities, even for the Net community as a whole, thus implying a switch to cyber-internationalism?

Similarly, the cyber-internationalists' model of governance may not be as illegitimate as its critics portray. To be sure, negotiators of international treaties in general are quite removed from direct democratic control. Yet, on a more general level, the international community is made up of mostly—at least in principle—legitimate representatives of well-established nation-states and thus may enjoy an overall edge in legitimacy over small, self-selected cyber-communities, which enact cyberspace standards affecting and restricting many nonmembers of their communities as well.[121] On the other hand, enforcement of an international regulatory framework—the perceived forte of international governance in cyberspace—might be limited if it does not include all (or at least the vast majority of) nations, as market forces make exploitation of the enforcement gaps generated by nonparticipating nations highly profitable.

The analysis of the three models of governance hierarchically stacked and structurally linked to the legitimacy/enforceability trade-off does not render a simple and obvious "winner" in the quest for optimal cyber-governance. International governance has the advantage of enforceability, as it is global in scope, but may lack legitimacy. Self-regulation within virtual communities may be the most legitimate solution, as the governed have a direct say in the creation of the rules that will govern them, but may be difficult to enforce. The traditional nation-state—a structural compromise of legitimacy and enforceability—offers a bit of both, but provides neither at a higher level than the other two models of governance. This lack of a clear winner, however, is less a consequence of the "unregulability" of cyberspace and more one of the intrinsic limitations of the structural metaphor employed.

To be sure, the hierarchical stacking of the governance models atop each other is less constrained than the binary model, as one can—using the metaphor of stacked layers—envision a governance model in which the borders between layers become less absolute and pronounced. For example, any cyber-governance based on the hierarchical model may

120. For a recent critical analysis of the legitimacy of private ordering, see Steven L. Schwarcz, PRIVATE ORDERING (SSRN Working Paper No. 298409) (2002).

121. Cyber-communities, like states, face the problem of negative spillover effects, because of the incongruence of their scope and reach. *See supra* notes 51-58 and accompanying text.

combine two layers of governance, as long as they are adjacent to each other. International governance may be combined with national, or national with community governance. Based on this stacked approach, however, it is conceptually difficult to envision, for example, a mix of international regulation and community self-regulation.[122] In essence, the hierarchical model incorporates a combination of international and national modes of governance, or national and community governance, but never international and community governance. It is still restrictively one-dimensional. Worse, the two qualities any regulation must strive to attain—legitimacy and enforceability—seem to be inversely proportional to one another in the hierarchical model, leaving us with an inescapable trade-off between them. This leaves one with a hierarchical model of governance that will not be able to escape the legitimacy/enforceability trade-off—another "tragic choice," this time on a meta-level in which one is doomed to allocate limited resources among competing values, only to achieve suboptimal outcomes. Is this a useful or even accurate depiction of our choices in developing a model for effective regulation in cyberspace?

III. AN ALTERNATIVE SHAPE OF GOVERNANCE: THE TRIANGLE OF CYBER-GOVERNANCE

The hierarchical stacking of layers of governance, from community to state to international, implicitly takes for granted that communities can be linked to a specific geographic area and thus subjected to the regulatory framework of a particular physical territory.

Cyberspace arguably escapes at least some limitations of geography. Cairncross may have overstated her hand when she announced the "death of distance,"[123] but the global nature of the Net is a fact. Moreover, Internet users do not pay by the distance their data travels on the global network. Economics thus encourages global reach and the overcoming of territorial borders.[124] Netizens can organize in cyberspace on a global scale, at least as long as national governments are either

122. *But see infra* Section III. 4. Community-based Standards: A Mix of Community-based Self-regulatory and International Governance.

123. *See* CAIRNCROSS, *supra* note 48.

124. Global reach is also not discouraged by Internet connection, as the prevalent pricing models for Internet connection are either time-based or, more importantly, flat fees. Notably, neither model—unlike that of telephone connections—factors in distance traveled. *See* Loretta Anania & Richard Jay Solomon, *Flat–The Minimalist Price, in* INTERNET ECONOMICS (Lee W. McKnight & Joseph P. Bailey eds., 1997), 91, 114-16 (suggesting that, economically speaking, for the Internet and similar networks, a "flat" fee is the best option).

incapable or unwilling to intervene.[125]

Conceiving of cyber-governance as a stacked hierarchy or "multiple layers of nested enterprises"[126] does not square well with the reality that cyberspace has this virtual dimension. Whereas the individual members of a cyber-community reside at specific geographic locations, the community itself does not need to be incorporated in their (or *any*, for that matter) physical world to exist.[127] Consequently, it may be difficult to place some cyber-communities within a hierarchy of modes of governance beneath a specific national one. To be sure, self-regulation is not taking place in a complete governance vacuum either. Private ordering recedes from areas for which alternative national or international norms are created and in fact enforced.[128] But self-regulation in cyberspace, like the lex mercatoria, does not originate within a specific (or specifiable) nation, and may be enforced (at least to a certain extent) independent of a particular nation's acquiescence. In this very real, and very practical sense, self-regulation overlaps with the other two modes of governance.

The use of a stacked-layers metaphor to conceptualize governance in cyberspace thus suffers from a fundamental shortcoming. In its place, one may envision an alternative, more accurate rendition of the linkage and interdependency among the three models of governance: the triangle. One has to envision the "triangle of cyber-governance" as an ordinary, plain triangle, neither right-angled nor equilateral, but sides and angles of unequal size. Each of its corners represents one institution, structure, or mode of cyber-governance: self-regulation within cyber-communities, the state governing cyberspace through the application of national laws, and international cyber-regulation. Conceiving these three forms of governance as corners of a triangle (and the relationships among them as the sides of the triangle) frees our imagination from the restrictive mono-dimensionality implicit in the stacked-layers view.[129] There is no structural hierarchy among the three

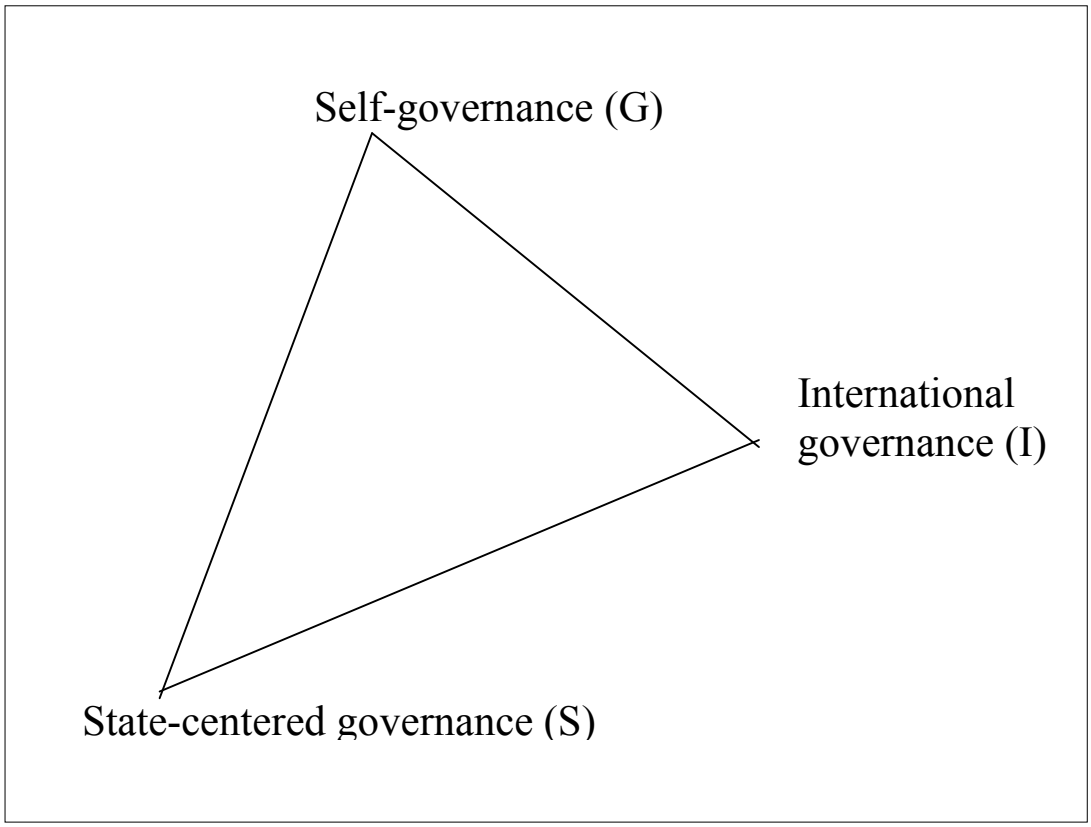
125. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1203 (discussing the oft-promulgated characterization of cyberspace as a "boundary-destroying" means of communication).

126. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 101 (1990) (viewing this structural feature of governance as a basic criterion for successful self-regulation in common property regimes).

127. LESSIG, *supra* note 19, at 9-14.

128. Even national enforcement is not impossible, it may just be very costly. *See* Froomkin, *Arbitrage*, *supra* note 27, at 148.

129. *See* Trachtman, *supra* note 25, at 570 ("[S]ome things are bound to remain for the state, while some things are for the market, and other things are for international governance. This is the true meaning of subsidiarity, and it leaves us in the existential position of having to analyze



corners of a triangle, just as there is no implicit hierarchy among the three models of Internet governance.

Figure 2: The Regulatory Triangle

The suggested switch from binary thinking about governance of cyberspace and conceptualizing such governance as a layered hierarchy to a conception of a nonpre-determined order of governance, which the triangle exemplifies, may sound simple, even simplistic and naïve. The triangle of cyber-governance is not intended to render a precise solution,

and choose, rather than being able to conclude debates by simple epithets.")

or to solve the cyber-governance puzzle generally. It is simply a metaphor to free our mind from thinking too restrictively and too abstractly about who should make the rules (and enforce them) in cyberspace.[130]

Instead of limiting our conception of what modes of governance to choose from, the triangle of cyber-governance allows us to think past the three simple modes of the hierarchical conception, and to envision regulatory *mixes* to govern cyberspace even beyond what might be produced through the interaction of two adjacent layers in a hierarchical setup. The triangular shape enables us to visualize regulatory mixes as any point on a side between two corners of our triangle. Unlike the pure black and white of binarity, the triangle helps us conceptualize governance as any imaginable mix of two modes, creating a vast spectrum of different options, of shades of gray. Such governance mixes may sound unfamiliar at first. But the world is full of them, and not just in cyberspace. In the following discussion five such mixes are described briefly, and - with the help of the triangular metaphor - their governance components untangled.

1. Obscenity Laws: A Mix of Self-Governance and State-Governance

The first example of a governance mix, the law of obscenity in the United States may look like an unlikely candidate for investigating cyberspace governance. To be sure, although much older than cyberspace, U.S. obscenity laws have helped the Internet gain much notoriety—and given rise to a famous Supreme Court decision.[131] But here it is of interest not because of what it does, but how it does it.

State and federal obscenity laws have restricted obscene speech for many decades. In the 1950s, tracking a broadening interpretation of speech protected by the First Amendment, cases came before the Supreme Court challenging these obscenity laws on the grounds that

130. Others have similarly suggested more innovative forms of mixed governance. *See* Marcelo Halpern & Ajay K. Mehrota, *From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age,* 21 U. PA. J. INT'L ECON. L. 523 (2000) (arguing for an "Internet Common Law," a mix of self-regulation and international law); Thomas B. Nachbar, *Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character,* 85 MINN. L. REV. 215 (2000) (suggesting a division-of-labor approach that combines national governance and voluntary self-regulation); Perritt, *Barriers*, *supra* note 107 (advocating hybrid forms of governance). For a mixed governance proposal outside the context of cyberspace, see Kenneth W. Abbott & Duncan Snidal, *International "Standards" and International Governance*, 8 J. EUR. PUB. POL'Y 345 (2001).

131. Reno v. ACLU, 521 U.S. 844 (1997) (invalidating indecency provisions of the Communication Decency Act but reaffirming the right of legislatures to restrict obscene speech).

they violate the right to free speech. Many of these challenges focused on the definition of what constitutes obscene speech. In Roth v. United States,[132] the Supreme Court linked the definition of obscenity to "contemporary community standards." This is an intriguing link: traditional state (and federal) governance - obscenity statutes - is thus connected to the opinions and assessment of a particular community. Although not a governance mix in the strictest term—the task of the community is not to set the obscenity norm, but to make determinations of fact as to whether something is obscene according to the law—on a practical level the Supreme Court's decision in Roth does combine state and community views. But what exactly is the appropriate "community" to make the determinations the Court's ruling requires?

Rejecting calls and earlier decisions to opt for "national scope,"[133] in *Miller v. California*,[134] the Supreme Court emphatically reiterated the need, in obscenity cases, for assessment by communities well below the national threshold: "These are essentially questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists."[135] Why is the Supreme Court so adamantly advocating a mix of state laws and community assessment? Frederick Schauer suggested that this provides for a measurable standard, one that—although creating some negative spillover effects[136]—emphasizes geographic aspects over temporal ones.[137] If in fact communities need to be protected from the harm created by obscene material entering them, as most obscenity laws purport to do, involving the community itself in determining the appropriate standard provides such an emphasis on geography. Guided by the principles developed by the Supreme Court for the nation as a whole,[138] the jurors in an obscenity trial decide among themselves

132. 354 U.S. 476, 489 (1957).

133. In *Jacobellis v. Ohio*, 378 U.S. 184, 195 (1964), Justice Brennan suggested that the community needs to be national in scope, but he did not speak for the majority of the court.

134. 413 U.S. 15 (1973). *Miller* has, according to Westlaw, been cited more than 3,500 times in case law and academic literature. For academic reviews of *Miller*, see Amy M. Adler, *Post-Modern Art and the Death Of Obscenity Law*, 99 YALE L.J. 1359 (1990), and J. Todd Metcalf, *Obscenity Prosecutions In Cyberspace: The Miller Test Cannot "Go Where No Porn Has Gone Before,"* 74 WASH. U. L.Q. 481 (1996). The Supreme Court has most recently upheld the *Miller* test in *Reno v. ACLU*, 521 U.S. at 872 (1997).

135. *Id.* at 30.

136. *See* Zanghi, *supra* note 27, at 113 (suggesting that this spillover is "massive" in cyberspace).

137. FREDERICK F. SCHAUER, THE LAW OF OBSCENITY 121 (1976).

138. *See Miller,* 413 U.S. at 24 (stating that a work could be considered obscene for First Amendment purposes if "'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest," "the work depicts or

applying their community's standard if they would call the speech in question obscene. This is, in effect at least, a governance mix by another name.

The Supreme Court's combination of positive law and community standards has been frequently criticized. But looking at it closely, it undeniably has its advantages. As noted above, restrictions of obscenity aim at protecting the moral well-being of the community.[139] Emphasizing geography has the benefit of enabling communities with less restrictive standards to permit the distribution of material that other, more conservative communities would want to prohibit. A homogenous national standard (or even a state standard) would be too restrictive for some communities and too tolerant for others. In *Miller*, the Supreme Court explicitly noted this difficulty: "It is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City."[140] A more local standard, on the other hand, can be better tailored to the differing views and moral values of various localities in a heterogeneous nation.

Problems may arise, of course, when the sender of obscene material and the recipient of it reside in two different communities, with differing community standards. As Schauer stated, this is essentially a conflict-of-laws problem.[141] What at first sight sounds like a vexing problem, however, can be solved comparatively easy by recourse to what obscenity laws attempt to do: protect communities from outside "harm." It is the recipient's community that is to be protected, and hence that community's standards are particularly useful in assessing the claim of obscenity with respect to material received by a resident of that community. Imagine if one were to install a microphone at somebody's house and link it to loudspeakers in a village one hundred miles away. Any resulting danger from the speech transmitted would be almost nonexistent for the speaker's community but substantial for the recipient's. Asking the unaffected community on the sender's side to judge the speech would effectively thwart the very purpose of obscenity

describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law," and "the work, taken as a whole, lacks serious literary, artistic, political, or scientific value") (quoting Roth v. United States, 354 U.S. 476, 489 (1957)) (citations omitted); *id.* at 24-25 (rejecting the constitutional test for obscenity as that which is "utterly without redeeming social value") (quoting Memoirs v. Massachusetts, 383 U.S. 413, 419 (1966)).

139. SCHAUER, *supra* note 137, at 129.

140. 413 U.S. at 32.

141. SCHAUER, *supra* note 137, at 127-30.

laws, namely, to protect local communities' moral standards.[142] This all works nicely in a system in which the recipient's community is grounded in geographic proximity. Assessing material received by someone in Boston may involve the Massachusetts or the Suffolk County community, but it is based on a locational propinquity. What to do, however, where this is not so clear? Governance mixes are not perfect solutions just because they combine two modes of governance. Only the right mix, the most suitable one for a specific governance problem, may unleash the power of combining governance modes, as the following case will help us to understand.

Robert and Carleen Thomas, a couple residing in Milpitas, California, operated an electronic bulletin board (BBS) from which members could, with the aid of a modem and a computer, download files containing pornographic images.[143] Access to the BBS was restricted to members.[144] Obtaining a membership (and thus password enabling members to gain access to the BBS) was no easy procedure: One had to fill in a form, identify oneself, and provide credit card information and a phone number.[145] Mr. Thomas would then call the applicant and conduct an interview to determine that he or she was of proper age.[146] Only then was membership granted, a username assigned, and a password issued.[147]

The Thomases had been investigated by the San Jose police for violating California's obscenity laws.[148] Formal charges were never brought, however, because investigators did not ultimately believe that the material they had seized from the Thomases violated local community standards.[149] The Thomases continued their business undeterred.[150] An undercover agent in conservative Memphis, Tennessee, then heard about the Thomases and applied for membership.[151] Once granted access to the BBS by the Thomases, he downloaded pictures onto his computer.[152] Subsequently, the couple was

142. This, of course, does not imply that the concrete impact of speech needs to be factored in. The Supreme Court has never permitted the restriction of speech based on subjective impact. Instead of the impact the message has on specific individuals, its content is to be assessed based on shared community values.

143. United States v. Thomas, 74 F.3d 701, 705 (6th Cir. 1996).

144. *Id.*

145. *Id.*

146. JONATHAN WALLACE & MARK MANGAN, SEX, LAWS, AND CYBERSPACE 2 (1996).

147. *Id.*

148. *Id.* at 6-7.

149. *Id.* at 7.

150. *Id.* at 7-12.

151. United States v. Thomas, 74 F.3d 701, 705 (6th Cir. 1996).

152. *Id.*

brought before a court for violating Tennessee obscenity laws.[153] A jury of Tennesseeans was selected and found the material received clearly to be obscene.[154] The Thomases were convicted and sentenced to multiple-year prison terms,[155] a verdict ultimately upheld on appeal.

Obscenity laws represent a remarkable regulatory mix of state and federal law combined with community assessment. The Thomases' case does not contradict this. But during the appeal, counsel for the Thomases argued that the court should consider as the appropriate local community the cyber-community in which the Thomases were operating.[156] "The cyberspace community," he suggested, "is as much a community as traditional geographic divisions. This community should have the right to articulate its standards on the issue of obscenity."[157]

This is a variation of the conflict-of-laws argument. Unlike others who have used such an argument, however, counsel for the Thomases did not argue for the sender's community to be used, or for the community to become "national." Instead, he took the Miller court at its word and argued that cyberspace was the "appropriate community" that would be subjected to the "harm" of the obscene material. Unimpressed, the appeals court rejected the argument. It feared that such a cyber-community was hard to define, and thus—practically speaking—jurors that would correctly apply such a standard hard to get.

But the appeals court also feared the slippery slope of an ever-expanding community. Echoing the Supreme Court's rejection two decades earlier of a national standard, which would not only be hard to define, but also invalidate the very idea of a proximity-based standard, the appeals court in *Thomas* stated:

> The reality is that if the court "examined the community created by computer technology," it would find that computers essentially create a world community. Computers unite citizens of small midwestern towns with denizens of New York City. For that matter, they unite Memphis residents with computer users in London, Tokyo, Bombay. It would be unrealistic to attempt to define the accepted standards of a 'community' that includes Iowa farmers, Las Vegas casino owners, Icelandic fishermen, and Tibetan monks.[158]

And the court has a point. The Thomases did know the geographic

153. *Id.*
154. *Id.* at 706.
155. *Id.*
156. *See Thomas*, 74 F.3d at 711.
157. WALLACE & MANGAN, *supra* note 146, at 32.
158. *Id. But cf.* Zanghi, *supra* note 27 (advocating a federal standard in light of cyberspace).

community to which they were sending their material. They knew about obscenity laws and that obscenity is assessed by employing community standards. By accepting a member whom they knew to be living in Tennessee, they explicitly permitted their message to be received there.[159]

But what happens if messages are sent or published in such a way that they can unintentionally be received in a completely untargeted community, violating its local standards. The Thomases still had control over whom they gave access. They were aware of the local communities to which they were sending their obscene information. The Internet shifts this level of control. In cyberspace it is more difficult than it was for the Thomases to locate the recipient of information. Does everyone maintaining a webpage on the Internet have to consider the various standards of all the possible communities whose members might access the material on the page? Information providers have to go by proxy (credit cards, user choice) to determine the geographic communities to which their users belong, and Congress has permitted them to do so.[160] But this, too, is a slippery slope, as it enables recipients potentially to self-select the community in which they tell others in cyberspace they are residing. The conventional concept of geographically proximate communities may not work well in this context.[161] Perhaps, the Thomases' counsel had a point after all. The more the world moves toward a society in which it is natural for people to form communities in cyberspace as well as in the physical world where they reside, the more pressure will mount to accept one's cyber-peers as one's appropriate jury. Perhaps.

The laws of obscenity provide an intriguing mix of governance, in the broad sense of the word, combining national (and state) laws with the

159. In that sense, they were doing much more than just broadcasting to the world or serving a webpage. It is this difference that makes the *Thomas* precedent of so little utility in analyzing obscenity laws in cyberspace.

160.

> No provider or user of an interactive computer service shall be held liable on account of—(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Communication Decency Act, 47 U.S.C. § 230 (2002) (safe harbor clause). *See also* Children's Online Privacy Protection Act, 15 U.S.C. § 6503 (1998) (safe harbor provision); Children's Online Privacy Protection Rule, 16 C.F.R. § 312.10 (1999) (safe harbors).

161. *See, e.g.,* Salbu, *supra* note 2, at 440 (suggesting that the "disjunction between community and geographic proximity . . . reduces the legitimacy of state authority").

values of the community, expressed by its members. From a structural viewpoint, this may be the right approach, that of wedding a national (or state) law with local values and thus making it fit a nation of heterogeneous communities. Identifying the right community to partake in this kind of self-control has until recently been mostly easy.[162] In the case of cyberspace, however, it turns into a significantly tougher task. This must not come as a surprise. The challenge of delineating a community, as has been described in the discursive analysis above, is germane to all forms of self-regulation. It is not necessary to solve this puzzle here, either. For present purposes, it is sufficient to note that this is, indeed, an example of a regulatory mix between state and self-governance, transcending the binary choice inherent in entrusting regulation exclusively to one set of controls or the other.

2. European Union Directives: A Mix of International and State Governance

The European Union (EU) has implemented a different regulatory mix: the directive. The directive is a legal document enacted by the EU and addressed to its member states.[163] It requires member states to "transpose" the substance of the directive into national laws, which involves implementing the substance of the directive within a specified period of time.[164] According to this arrangement, regulatory governance is shared between the EU and national legislatures. The EU sets the principles but leaves the details of implementation to the member states.[165] The amount of flexibility available in transposing the directive into national law depends largely on the text of the directive itself. In most cases, directives set only minimum standards (viz., prescribe a "floor") or the maximum permissible deviation from the directive (viz.,

162. *But cf.* Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 124-26 (1989) (discussing the problem of locating the caller of "dial-a-porn" services).

163. *See* TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Nov. 10, 1997, art. 249, O.J. (C 340) 3 (1997) [hereinafter EC TREATY] ("A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."); *see also* ENCYCLOPEDIA OF THE EUROPEAN UNION 324 (Desmond Dinan ed., updated ed. 2000).

164. Not all directives get transposed within the time limit set by the directive, but the overall transposal rate has been increasing steadily over the last few years, from below 90 percent in 1991 to 94 percent in 1998. *See* Better Lawmaking: Commission Report to the European Council (1998), *available at* http://europa.eu.int/comm/off/rep/lawmaking/1998/en.pdf (last visited Jan. 13, 2003).

165. EC TREATY, *supra* note 163, art. 249 (the directive "shall leave to the national authorities the choice of form and methods").

create a "ceiling").[166] National laws implementing the directive have to stay within this "bandwidth". Sometimes directives allow member states to choose among a number of options for implementation.[167] Directives may also detail the implementation of a specific rule – thus restricting flexibility in the wording of the implementation – but leave it to the member states to decide whether to transpose that part of the directive at all.[168]

The directive is *the* legal instrument of choice in the EU. The overwhelming majority of EU measures are adopted in the form of directives.[169] This approach has been particularly successful in the area of telecommunication deregulation and the establishment of a legal framework for the information society.[170]

It is not difficult to understand the inherent advantages of the

166. For example, Council Directive 90/270 of 29 May 1990 on the Minimum Safety and Health Requirements for Work with Display Screen Equipment, 1990 O.J. (L 156) 14, sets a floor for health and safety standards; member states may exceed that floor. See, e.g., Council Directive 90/270, art. 9, para. 5, 1990 O.J. (L 156) 14 ("Protection of workers' eyes and eyesight may be provided as part of a national health system."). In contrast, the Parliament and Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data sets both a floor and a ceiling for the level of protection afforded to personal data. Council Directive 95/46, art. 3, 1995 O.J. (L 281) 31 [hereinafter Privacy Directive].

167. For example, the Parliament and Council Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector permits member states to regulate unsolicited calls for direct marketing purposes on either an "opt-in" or an "opt-out" basis. Council Directive 97/66, art. 12, 1997 O.J. (L 24) 1 [hereinafter Telecom Privacy Directive].

168. For example, Privacy Directive permits member states to exempt certain public registers from privacy restrictions. Privacy Directive, *supra* note 166, art. 21.

169. *See The Community's Range of Tools, at* http://www.europa.eu.int/eur-lex/en/about/abc/abc_20.html (explaining the EU's legal instruments and focusing on regulations/decisions and directives as the two most important primary sources. In 2001, there were more directives adopted than any other legislative instrument. This is remarkable because the EU has already adopted a great number of directives in the early 1990s to harmonize the common market, and since the late 1990s, the emphasis has been on police and justice coordination, which is less a field of directives. *See Annual General Report of the EU Commission*, *at* http://www.europa.eu.int/abc/doc/off/rg/en/2001/pg1287.htm (providing a detailed overview of the action items taken during 2001). 1,566 directives have passed that are still applicable of which the average EU member nation has transposed 1,496. Compare this to the number of regulations adopted in the last couple of years (between five and six) and the difference is obvious: even forty years of an annual load of five regulations would result only in 200 regulations; yet the EU counts almost eight times as many directives still to be applicable. *See Annual Progress Reports of the European Commission, at* http://www.europa.eu.int/comm/secretariat_general/sgb/droit_com/pdf/mne-country_20021231.en.pdf.

170. For direct comparisons between this EU approach and the U.S. manner of regulatory usurpation by the federal level, see David Lazer & Viktor Mayer-Schönberger, *Governing Networks: Telecommunication Deregulation in Europe and the United States,* 27 BROOK.J. INT'L L. 819 (2002); Viktor Mayer-Schönberger & Mathias Strasser, *A Closer Look at Telecom Deregulation: The European Advantage,* 12 HARV. J.L. & TECH. 561 (1999).

directive approach. It permits the Union-wide implementation of a common policy in a particular area, while leaving enough flexibility for national, societal, economic and cultural differences among the nations that make up the Union. In this way the directive is capable of creating a regulatory umbrella across a fairly extensive spectrum of different values and approaches. This is particularly useful in contentious areas of regulation and in areas of fast, dynamic development in which no overall consensus about the regulatory details has emerged.

In addition, this mix of supranational directives (promoting homogeneity among regulatory ends) and national implementation (ensuring flexibility with regard to regulatory means) provides for the creation of strong regulatory interdependence.[171] Rulemaking never takes place in a regulatory vacuum.[172] Whoever governs is also part of a larger process of competition, coordination, and learning.[173] Nations see how other nations govern, and examine what policies worked well and why.[174] In the EU context, the flexibility of directive implementation provides a modicum of regulatory competition—establishing in essence a market for different regulatory frameworks. It is augmented by the directives' shared common objectives, providing a strong current of central coordination. Regulatory competition promotes experimentation and learning from others, and thus is particularly helpful in highly innovative areas, in which no tried regulatory blueprints exist. Yet, central coordination is equally important. Such coordination ensures that through shared goals and values, the EU achieves a level of regulatory homogeneity that decreases the costs of transactions that cross the borders of member countries.

Recent studies have shown that regulatory competition does not necessarily lead to a mono-dimensional "race to the bottom" among regulatory regimes, but may result instead in the pragmatic selection of a "suitable" framework given many external factors of restraint.[175] But

171. *See* David Lazer, *Regulatory Interdependence and International Governance,* 8 J. EUR. PUB. POL'Y 474 (2001).

172. *Id.* at 481.

173. *Id.* at 475, 480.

174. *Id.* at 480.

175. *See* Simon Deakin, *Two Types of Regulatory Competition: Competitive Federalism vs. Reflexive Harmonisation. A Law and Economics Perspective on* Centros, *in* 2 Cambridge Yearbook of European Legal Studies 231 (Alan Dashwood & Angela Ward eds., 1999); Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race to the Bottom" Rationale for Federal Environmental Regulation,* 67 N.Y.U. L. REV. 1210 (1992). Deakin differentiates between two types of regulatory competition: "competitive federalism," which leads to regulatory mono-cultures based on the regulatory framework of the dominant player(s), and "reflexive harmonization," the "evolutionary selection of rules through mutual learning between national-

the EU approach of combining regulatory competition and coordination through its innovative directive-based governance mix provides a more immediate (and thus effective) protection against detrimental "races to the bottom," and fosters transnational regulatory homogeneity, providing the foundation for beneficial economies of scale.[176] And it seems to work. The tremendous success of the EU in liberalizing European telecommunication markets,[177] establishing a competitive cellular phone market (and the leading global standard, GSM[178]) provides significant evidence that the directive approach of mixed governance works, especially in the fast-paced field of high-tech.

There is no reason to believe that the directive approach will yield a perfect result in all possible areas of cyber-regulation. But it does provide another example of a mix of two different modes of governance, international and national, being successfully employed, in this case in the European Union.

3. Transnational Networks: A Mix of Informal Transnational and National Governance

The EU directive process represents a formal means of sharing governance responsibilities between a supranational and various national entities. The sharing of governance and rulemaking need not, however, be so formalized. Anne-Marie Slaughter has examined what she calls "transgovernmental networks" as informal settings for cooperation and coordination in rulemaking and enforcement.[179] Somewhat overlooked by researchers,[180] these networks have flourished

level systems." Deakin, *supra*, at 232.

176. *See* David Vogel, *Trading Up and Governing Across: Transnational Governance and Environmental Protection*, 4 J. EUR. PUB. POL'Y 556, 562 (1997) (arguing that larger and more developed economies can push for stricter environmental standards because, even though such standards seemingly put those jurisdictions at a competitive disadvantage as compared to jurisdictions with lower standards, their size and importance compel producers to meet such higher standards in order to participate in those markets).

177. *See* Mayer-Schönberger & Lazer, *supra* note 170, at 842-43.

178. *See* Jacques Pelkmans, *The GSM Standard: Explaining a Success Story*, 8 J. EUR. PUB. POL'Y 432 (2001).

179. Anne-Marie Slaughter, *The Real World Order*, FOREIGN AFF., Sept./Oct. 1997, at 183, 194 [hereinafter Slaughter, *The Real World Order*]; *see also* Anne-Marie Slaughter, *Agencies on the Loose? Holding Government Networks Accountable, in* TRANSATLANTIC REGULATORY COOPERATION: LEGAL PROBLEMS AND POLITICAL PROSPECTS 521 (George A. Bermann, Matthias Herdegen & Peter L. Lindseth eds., 2000); Anne-Marie Slaughter, *Governing the Global Economy through Government Networks*, *in* THE ROLE OF LAW IN INTERNATIONAL POLITICS 177 (Michael Byers ed., 2000); Anne-Marie Slaughter, *Government Networks: The Heart of the Liberal Democratic Order*, *in* DEMOCRATIC GOVERNANCE AND INTERNATIONAL LAW 199 (Gregory H. Fox & Brad R. Roth eds., 2000).

180. *But see* Perritt, *Changing*, *supra* note 88, at 1009 (stating that "[g]overnment institutions

in practice. Slaughter details numerous examples, ranging from the highly informal international meetings of supreme court justices to the much more formalized Basle Committee on Banking Supervision.[181] Despite their informal character, these networks wield substantial power and have permitted international coordination without the formal devolution of regulatory responsibility from national institutions to some supranational entity.

Transgovernmental networks do not aspire to become international superstructures. Remaining closely linked to the mode of national governance, they arguably offer advantages over a purely national or international governance. In some contexts, they may even have the edge over a more formalized setup like the EU directive process. For example, they do not take (formal) legitimacy away from elected national decision makers and transfer it to a possibly nonelected, less legitimate international body. The formal decision-making power is clearly retained by national policymakers, making such arrangements potentially more acceptable to constituencies suspicious of new international regimes.

However, keeping the formal governance authority where it has been (i.e., at the national level) and setting up informal networks not only offers advantages over purely national or international governance, but also may offer an even bigger advantage, particularly when regulating a fast-changing field like cyberspace: It does not take a long time to set up. Today, negotiating an international treaty takes years at best, and perhaps much longer if negotiating states are expected to relinquish some important parts of their power in favor of the nascent international regime. Even in a highly formalized, supranational structure like the EU, negotiating a directive may span years of protracted bargaining.[182] Transgovernmental networks, on the other hand, can be set up comparatively quickly, taking on different informal structural shapes in a matter of months if the task should require it. At the same time, such networks permit cooperation and coordination across national regulatory frameworks, which is an absolute necessity when regulating cyberspace.

Transgovernmental networks have recently been extended to address

have formed networks of their own"); Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet,* 32 INT'L LAW. 991, 1015 (1998).

181. Slaughter, *The Real World Order*, *supra* note 179, at 186-91.

182. For example, the EU's Privacy Directive, *supra* note 166, was adopted five years after the first Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3.

cyber-regulation issues.[183] For example, at the OECD Council meeting in Paris in May 1997, leading economic powers identified areas in which international co-operation is warranted, including efforts to combat dissemination of child pornography on the Internet.[184] Similar international coordination has been announced for the prevention of cyberterrorism.[185] Of course, transgovernmental networks do not come into being easily. Whether, for instance, such one-time calls for cooperation and coordination lead to a working transgovernmental network or whether they end up being transformed into more traditional (and thus much slower) international treaty negotiations that result in general inertia depends on many individual factors.[186]

The informal but regular meetings of the national data protection and privacy commissioners of the major postindustrialized nations provide

183. International organizations such as the United Nations Commission on International Trade Law (UNCITRAL) and the Organization for Economic Co-operation and Development (OECD) also offer a layer of cooperation by providing a forum for informal talks on harmonization in addition to the formal competencies of their charters. For example, in February 1997, UNCITRAL began to draft model international digital signature legislation. *See* UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW, *Report of the Working Group on Electronic Commerce*, 31st Sess., U.N. Doc. A/CN.9/437 (1997). *See also* UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW, *Working Group on Electronic Commerce*, Planning Of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues, 31st Sess., U.N. Doc. A/CN.9/WG.IV/WP.71 (1996). Similarly, in November 1997, the International Chamber of Commerce issued the General Usage for International Digitally Ensured Commerce (GUIDEC), a set of guidelines for ensuring trustworthy digital transactions over the Internet. INTERNATIONAL CHAMBER OF COMMERCE, General Usage for International Digitally Ensured Commerce, *available at* www.iccwbo.org/home/guidec/guidec_one/guidec.asp (last visited Nov. 15, 2002). And the OECD recently adopted principles to guide countries in formulating their own policies and legislation relating to the use of cryptography. *See* Organization for Economic Co-operation and Development, Cryptography Policy: The Guidelines and the Issues (1997), *available at* www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10242-29,FF.html (last visited Nov. 15, 2002).

184. Communiqué, Organization for Economic Co-operation and Development, Meeting Of The Council At Ministerial Level (May 26-27, 1997), *available at* http://www.g7.utoronto.ca/g7/oecd/oecd97.htm. *See generally* Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society - COMCRIME Study* (1998), *available at* http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (last visited Nov. 15, 2002).

185. *See* G8, Ministerial Conference on Terrorism: Agreement on 25 Measures (July 30, 1996), *available at* http://www.g7.utoronto.ca/g7/terrorism/terror25.htm (last visited Nov. 15, 2002). *See generally* W. Michael Reisman, *International Legal Responses to Terrorism*, 22 HOUS. J. INT'L L. 3 (1999) (describing international efforts to develop appropriate responses to terrorism). In Europe, this transgovernmental coordination has led to a formal international instrument, the Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Nov. 15, 2002).

186. For a discussion of some of these factors in the context of cybercrimes and cyberterrorism, see Michael A. Sussmann, *The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451 476-89 (1999).

an example of an informal transnational governmental network already in existence in which regulatory frameworks and their interpretations are discussed and coordinated.[187] Just being able to discuss and exchange ideas on privacy and data protection regularly has arguably helped not only to overcome problems associated with the European Union Privacy Directive,[188] for the nations participating in these meetings,[189] but also to shape and advance privacy legislation globally.[190] The lack of a privacy commissioner in the United States precluded U.S. involvement in coordination efforts and may have exacerbated a sharp exchange—some have even termed it an information economy "trade war"—between the United States and Europe.[191]

It is probably too early to assess the impact and success of these transnational governmental networks. But they, too, represent a unique mix of national and international governance, although the national-governance component is much stronger than in the more formalized approach embodied in the use of EU directives. Yet, contrasting the two—the EU Directive and transnational governmental networks—exemplifies the wide spectrum of options possible when mixing two

187. These meetings are both informal (for example, in conjunction with OECD meetings) and formalized (for example, through International Conference of Privacy and Data Protection Commissioners); there are also sectoral conferences such as the International Working Group on Data Protection in Telecommunications. *See, e.g.,* Press Release, Privacy Commissioner of Canada, 18th International Conference of Privacy and Data Protection Commissioners (Sept. 18, 1996), *available at* http://www.privcom.gc.ca/speech/archive/02_05_a_960918_e.asp (last visited Nov. 15, 2002).

188. Privacy Directive, *supra* note 166; *see also* Telecom Privacy Directive, *supra* note 167.

189. *See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 467 (1995).

190. Lazer & Mayer-Schönberger, *supra* note 170, at 847-49.

191. *See* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT 18 (1998) (critiquing the EU's "broad, centralized, top-down approach to privacy protection" that could disrupt "the free flow of information"); KEVIN FEATHERSTONE & ROY H. GINSBERG, THE UNITED STATES AND THE EUROPEAN UNION IN THE 1990S: PARTNERS IN TRANSITION 137, 149 (2d ed. 1996); Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 438 (1995); Gregory Shaffer, *Globalization And Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000). The tension was finally diffused with the "safe-harbor agreement" between the United States and the European Union. Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7; *see also* Corrigendum to Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2001 O.J. (L 115) 14.

governance modes.

4. Community-based Standards: A Mix of Community-based Self-regulatory and International Governance

There is no reason why regulatory mixes should be limited to community/national or national/international combinations. Internet standardization may provide a case in point.

Traditionally, standardization has been a prerogative of the state. The National Institute of Standards and Technology (NIST)[192] in the United States and the Deutsches Institut für Normung (DIN)[193] in Germany are well-known national standardization institutions. Only over the last couple of decades have some standardization processes been transferred to newly created international institutions such as the International Organization for Standardziation (ISO)[194] and the International Telecommunication Union (ITU).[195] National standardization bodies

192. The National Institute of Standards and Technology is an agency of the Department of Commerce. Established in 1901 as the National Bureau of Standards, it employs about 3,000 people and has a yearly budget of over 800 million dollars. In 1988, its name was changed to NIST. National Institute of Standards and Technology, General Information, *at* http://www.nist.gov/public_affairs/general2.htm (last updated Dec. 19, 2002).

193. The DIN is not a governmental agency but a private nonprofit organization, permitting private business and individuals to become members. About 26,000 external experts work for the DIN. *See* Deutsches Institut für Normung, About DIN, *at* http://www2.din.de/index.php?lang=en (last visited Nov. 22, 2002).

194. The International Organization for Standardization acronym "ISO" is derived from the Greek word for "equal" (or "standardized"). ISO is a federation of about 140 national standardization bodies, established in 1947. ISO is organized in about 850 expert committees with roughly 30,000 experts who meet regularly. The central Secretariat is located in Geneva, Switzerland. International Organization for Standardization, Introduction: What is ISO?, *at* http://www.iso.ch./iso/en/aboutiso/introduction/whatisISO.html (last modified July 17, 2002).

International standardization dates back to 1906 when the International Electrotechnical Commission (IEC) was founded. In 1946, when international organizations became modern in many areas, 25 countries started ISO, "the object of which would be to facilitate the international coordination and unification of industrial standards." Business started officially on February 23, 1947. International Organization for Standardization, Introduction: How It All Started, *at* http://www.iso.ch./iso/en/aboutiso/introduction/howstarted/howstarted.html (last modified July 17, 2002).

195. The background of the ITU goes back to the last century. On May 17, 1865, twenty countries signed the first International Telegraph Convention. Following the invention of the telephone, the Telegraph Union began, in 1885, to draw up international legislation governing telephony, and, in 1906, the first International Radiotelegraph Convention was signed. Ultimately the Union's regulatory conferences governed international agreements on all forms of communication by wire, radio, optical systems or other electromagnetic systems. The International Frequency Registration Board (IFRB) allocates specific frequency bands with a view to avoiding interference. In 1932, the International Telegraph Convention of 1865 and the International Radiotelegraph Convention of 1906 were combined to form the International Telecommunication Convention, and the name of the organization was changed on January 1, 1934 to the International Telecommunication Union. In 1947, it became a specialized agency of

have not become powerless, but they have become member organizations of these international bodies. An interesting example is provided by the European standardization processes. National standardization bodies today are closely connected to three Europe-wide standardization organizations.[196] The European Committee for Standardization (CEN) provides voluntary harmonization of standards among European countries[197] and thus might be seen as another example of a transgovernmental network. Yet by the same token, the EU in its legislative acts sometimes refers explicitly to European standards, thus replicating the national/international governance mode of the EU directive.[198] Additionally, CEN has forged an agreement with ISO, mandating (at least in principle) automatic recognition of ISO standards as European standards,[199] creating another interesting, and innovative governance mix based on automatic recognition. These are just a few examples of different types of governance mixes used in the area of standardization.

Yet, despite this variety of mixes, self-regulatory standardization processes have played a minor role in setting the Internet protocol and similar standards. They have remained largely outside the established national and international standardization organizations.[200] The first Internet standards were set by a handful of engineers working on the early equipment.[201] Later an Internet Configuration Control Board was

the United Nations, and, in 1948, the headquarters were transferred from Bern to Geneva. New developments such as space radio communication and space communications have since been included in the agenda of the ITU. *See generally* International Telecommunication Union, ITU History – Overview, *at* http://www.itu.int/aboutitu/overview/history.html (last updated Feb. 13, 2002).

196. CEN, the European Committee for Standardization (http://www.cenorm.be), works in partnership with CENELEC, the European Committee for Electrotechnical Standardization (http://www.cenelec.org), and ETSI, the European Telecommunications Standards Institute (http://www.etsi.org). European Committee for Standardization, Objectives and Principles, at http://www.cenorm.be/aboutcen/whatis/objectives.htm (last updated June 28, 2001).

197. *See id.* ("CEN's mission is to promote voluntary technical harmonization in Europe in conjunction with worldwide bodies and its partners in Europe.").

198. *See, e.g.,* Directive 98/91/EC of the European Parliament and of the Council of 14 December 1998 Relating to Motor Vehicles and Their Trailers Intended for the Transport of Dangerous Goods by Road and Amending Directive 70/156/EEC Relating to the Type Approval of Motor Vehicles and Their Trailers, art. 3, 1999 O.J. (L 11) 25.

199. The coordination of CEN and ISO standards was formalized in the Vienna Agreement, signed in 1991. *See* International Organization for Standardization (ISO) & European Committee for Standardization (CEN), Agreement on Technical Cooperation Between ISO and CEN (Vienna Agreement), *available at* http://www.cenorm.be/BOSS/supmat/refdoc/ms002V2.htm (last updated Feb. 1, 2002); *see also* Council Resolution of 28 October 1999 on the Role of Standardisation in Europe, 2000 O.J. (C 141) 1.

200. Froomkin, *Arbitrage, supra* note 27, at 131-32.

201. *See generally* M. MITCHELL WALDROP, THE DREAM MACHINE (2001).

formed to develop the protocols further. In 1983 it morphed into the Internet Activities Board, which turned over its work in 1986 to the Internet Engineering Task Force (IETF).[202] IETF is not an international organization, nor is it a governmental body. It is a self-regulatory organization with a very limited bureaucratic structure.[203] For a long time, standards were chosen in IETF by means of the "humming test." All in favor of a proposal would hum, and the group present would decide whether the hum was loud enough to signify broad acceptance. Similarly, the original "standard" for the World Wide Web was set by its inventor, Tim Berners-Lee.[204] Today another nonprofit, self-regulatory organization, the World Wide Web Consortium (W3C) is advancing these standards.[205] In contrast, ISO is an organization comprising 143 national standards bodies and 2,885 technical committees and working groups. ISO employs over 500 staff and has an annual budget of US$90 million.[206] And ITU,[207] another international standardization body relevant for cyberspace, is even more bureaucratic.[208] Quite obviously, these are two very different types of entities. Although they might benefit from working together and forming a governance mix of their own, they have not done so yet.

The reasons for this are complex, but two are worth mentioning here. First, the Internet self-regulatory bodies and the international bodies operate at very different speeds. The existing international standardization processes are slow. The typical ISO process for promulgating a standard takes five years from the first steps to the final document.[209] Internet standards evolve much faster—and they have to, given Moore's Law[210] and Gilder's Law.[211] Second, Internet "standards"

202. TIMOTHY PARKER, TEACH YOURSELF TCP/IP IN 14 DAYS 19-21 (1994).

203. Froomkin, *Arbitrage, supra* note 27, at 132.

204. *See* TIM BERNERS-LEE, WEAVING THE WEB (1999).

205. Information about the W3C may be obtained at http://www.w3c.org.

206. See International Organization for Standardization, ISO In Figures, *at* http://www.iso.ch/iso/en/aboutiso/isoinfigures/January2002-p1.html (last visited Jan. 13, 2002).

207. *See* George A. Codding, *The International Telecommunication Union: 130 Years of Telecommunication Regulation*, 23 DENV. J. INT'L L. & POL'Y 501 (1995).

208. On the role of the ITU, see William J. Drake*, The Transformation of International Telecommunication Standardization: European and Global Dimensions*, *in* TELECOMMUNICATIONS IN TRANSITION 71 (Charles Steinfeld et al., eds, 1994); Besen & Farrell, *supra* note 103; Jayakar, *supra* note 103.

209. Roy Rada, *Corporate Shortcut to Standardization*, COMM. ACM, Jan. 1998, at 11 [hereinafter Roda, *Shortcut*].

210. Gordon Moore, *Cramming More Components Onto Integrated Circuits*, ELECTRONICS, Apr. 19, 1965, at 114 (suggesting that the development of computer chips will result in a doubling of processing speed every eighteen months); *see also* Gordon Moore, *Moore's Law*, *in* VISIONS OF TECHNOLOGY 243 (Richard Rhodes ed., 1999).

211. George Gilder, *Fiber Keeps Its Promise*, FORBES ASAP, Apr. 7, 1997, at 90-94 (stating that the development of networks will result in a tripling of network bandwidth every twelve

are never complete; they are never "done." Internet standards are published in the form of Requests for Comment (RFCs)[212] and are seen as continuous works in progress. In the Internet community, it is taken for granted that the various protocols need to be regularly revised. The Internet Protocol (IP), one of the most fundamental Internet standards, is currently in its sixth major version, or incarnation, with many minor revisions and add-ons made in between each major overhaul.[213] ISO has recently added a "fast-track" process for the development of standards, as well as a "shortcut" that promises to cut the total time it takes for a standard to be adopted by up to 80 percent.[214] But this is not nearly enough to catch up given the rapidity of the changes.

Perhaps the Internet self-regulatory standardziation bodies and ISO should think about a possible alternative governance mix, joining forces, which would enable ISO to play at least some role in a game in which, as of late, it has had no role at all. Conversely, bringing ISO into the picture would help to legitimize what so far has been a fairly U.S. and Western nation-centric process vis-à-vis nations that have not yet been represented in these *ad hoc* processes. It might go quite a ways to counter the claim that standards for cyberspace are made without taking into account the needs of currently marginalized societies and countries.[215] At the same time, keeping the general RFC structure in place, the actual process itself could remain speedy (at least relative to the standard ISO processes) as well as evolutionary.

Of course, a governance mix such as this, which combines international and community-grown institutions, has its disadvantages as well. However marginally, it will still slow down the process. There is a danger of prolonged culture clash between the fast-paced, informal,

months); *see also* GEORGE GILDER, TELECOSM: HOW INFINITE BANDWIDTH WILL REVOLUTIONIZE OUR WORLD (2000).

212. *See* The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force, *at* http://www.ietf.org/tao.html (Aug. 2001); Parker, *supra* note 202, at 20-21.

213. Guy Basque, *Introduction to the Internet*, in THE ELECTRONIC SUPERHIGHWAY 7, 8-15 (Ejan Mackaay et al. eds., 1995); David H. Crocker, *Making Standards the IETF Way*, 1 STANDARDVIEW 46, 51 (1993). For an introduction to IP tools, see Gary C. Kessler & Steven D. Shepard, *A Primer On Internet and TCP/IP Tools* (Network Working Group, Request for Comments No. 2151, June 1997), *available at* http://rfc.sunsite.dk/rfc/rfc2151.html (last visited Jan. 13, 2003).

214. For information regarding the "fast-track" process, see *Standardization Activities*, 16 COMPUTER STANDARDS & INTERFACES 375 (1994); Roy Roda, *Consensus Versus Speed*, COMM. ACM, Oct. 1995, at 21 [hereinafter Roda, *Consensus*]. For information regarding the "shortcut," see Roy Roda, *Shortcut*, *supra* note 209, at 11; Roy Roda, *The PAS Process*, 5 STANDARDVIEW 136, 136-39.

215. *See* Roda, *Consensus*, *supra* note 214, at 23 (arguing that standardization cannot just be fast, but must also be consensual for the many stakeholders and of high quality).

nuts-and-bolts Internet community and the international, culture-sensitive, deliberative standards community. Yet, given the challenges ahead for Internet standardization, it might still be useful to consider governance modes beyond the traditional, overly simplistic binary thinking of national, international or community-based categories and even beyond the already existing national/international mixes described above. In the end, combining two completely distinct governance models may add up to more than just the sum of the parts.

5. ICANN: Blending All Three Modes of Governance

The recent history of cyberspace offers an even more intriguing example of an unusual, unexpectedly innovative combination of modes of governance.

As many have pointed out before, the Internet is a decentralized network of networks.[216] It may have no central control, but its addressing and naming structure, although decentralized, is built as a multilayered, tree-like structure, whose branches share a common root. The root of the Internet address tree resides on a set of computers called the root servers.[217] In somewhat simplified terms the system works like this: Whenever a computer deep down in one network needs to contact another computer on a different but connected network, it will ask this root server how to reach the address directory of the destination computer's network.[218]

The list of address directories the root server keeps is fairly short but extremely important. Without it, computers would have difficulty communicating with each other. Metaphorically speaking, it would be like losing the essential part of a long distance directory. One might still be able to communicate with someone on one's network, but one would be unable to communicate much beyond it. In addition to this root server, keeping the Internet address system functioning and interoperable across the many different networks connected to it

216. *See, e.g.,* Robert Kline, *Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet*, 6 CORNELL J.L. & PUB. POL'Y 23, 24-25 (1996). *But see* Joseph P. Liu, *Legitimacy And Authority In Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 595-96 (1999) (arguing that the decentralized structure of the Internet gives power to central knots in the Internet organization).

217. *See, e.g.,* Cisco Systems, *DNS FAQ Answers*, *at* http://www.cisco.com/public/sw-center/sw_download_guide/dnsfaq.shtml (last visited Nov. 22, 2002); Ing. Abraham Gebrehiwot & Eberhard W. Lisse, *Introduction to the DNS 1.0*, *at* http://www.na-nic.com.na/dnsintro.html (last visited Nov. 22, 2002); The Linux Documentation Project, *How does the Internet work?*, *at* http://tldp.org/HOWTO/Unix-and-Internet-Fundamentals-HOWTO/internet.html (last updated Jan. 12, 2003).

218. *See supra* note 217.

requires universal addressing protocols and standards.

Related to the allocation and maintenance of Internet addresses is the issue of Internet domain names,[219] which make it easier for humans to memorize where in cyberspace a particular piece of information is located or how a particular communication partner can be reached. In essence, a domain name is mnemonic shorthand for the hard-to-remember numerical Internet address.[220] To use an Internet domain name, one has to register it with a domain registrar, so that the name can be added to Internet domain name directories, which others in turn may query to establish communication.[221]

For most of the life of the Internet the majority of these functions have been performed by the Internet Assigned Numbers Authority (IANA), which basically was a small group of dedicated experts around Jon Postel.[222] The domain name registration process was delegated to others. For example, although the U.S. Department of Commerce claimed formal power over the global domain name space, in practice, domains with the now well-known ".com" ending were registered and managed under agreement with the Commerce Department by a for-profit corporation called Network Solutions, Inc.[223] Domain names in other countries were mostly managed by IANA-designated registrars in those countries.[224]

With the booming of the New Economy, domain names gained currency. A string of domain name disputes and accusations that Network Solutions was handling the process intransparently and with limited efficiency, as well as a rising international awareness of the

219. For a technical explanation of the domain name system, see Jon Postel, *Domain Name System Structure and Delegation* (Information Science Institute, Request for Comments No. 1591, 1994), *available at* http://www.ieft.org/rfc/rfc1591.txt (last visited Nov. 22, 2002).

220. Johnson & Post, *Governed*, *supra* note 80, at 62, 68-69.

221. For a description of this system, see also Thomas v. Network Solutions, Inc., 176 F.3d 500, 504 (D.C. Cir. 1999).

222. *See generally* http://www.iana.com. IANA was not a legal person, it was not incorporated, and at its core was Jon Postel. Postel himself had once (jokingly) called himself the "czar" of the addressing system. Jon Postel, *Proposed Standard Socket Numbers* (Network Working Group, Request for Comments No. 349, 1972), *available at* http://www.ietf.org/rfc/rfc349.txt (last visited Nov. 22, 2002); *see also* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L. J. 17, 54-55 (2000) [hereinafter Froomkin, *Wrong Turn*] (providing a history of the domain name system); Jonathan Zittrain, *ICANN: Between The Public and the Private, Comments Before Congress*, 14 BERKELEY TECH. L.J. 1071 (1999); Scott Bradner, *The Internet Standards Process—Revision 3* (Network Working Group, Request for Comments No. 2026, 1996), *available at* http://www.ietf.org/rfc/rfc2026.txt (last visited Nov. 22, 2002).

223. *See generally* http://www.networksolutions.com.

224. One exception is RIPE, to which IANA delegated management of all Western European domain registrars, and which, in turn, delegated such management to national registrars.

importance of Internet naming and addressing, led the Department of Commerce to search for a new governance model.[225]

After intense debate, the government contracted with a newly founded entity, the Internet Corporation for Assigned Names and Numbers (ICANN).[226] ICANN was entrusted with (i) maintaining and advancing the fundamental Internet protocols related to naming and addressing, (ii) maintaining the central Internet root server, and (iii) accrediting and overseeing independent Internet domain name registrars who would create a market for domain name registrations.

There was substantial discussion as to the nature of ICANN. Should it be a government agency, a self-governing body, or an international organization? As this involved more than just a simple question of organization, the ensuing debate was waged about whether one of the very few central functions of the global Internet should be governed by U.S. (federal) law, community self-regulation or international agreement.[227] Internet players lobbied for community self-regulation, foreign nations (and users) fearing the structural entrenchment of US domination advocated an international approach, and the U.S. government, conscious of what was at stake, was wary of completely losing control over the process.[228]

Given the governance triangle suggested earlier, it would seem sensible to establish a governance framework for Internet addresses and names as a combination of international and community-based approaches. This governance mix, similar to the mix for standardization bodies suggested in the previous section, would incorporate the global nature of the Net while permitting the important technical work involved to remain close to the community affected.

225. The National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce, issued such a proposal. Improvement of Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826 (Feb. 20, 1998) (to be codified at 15 C.F.R. pt. 23); *see also* United States Department of Commerce, NTIA/OIA, A Proposal to Improve Technical Management of Internet Names and Addresses, *available at* http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm (last visited Nov. 22, 2002) (discussion draft of Jan. 30, 1998).

226. Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, *available at* http://www.icann.org/general/icann-mou-25nov98.htm (last updated Dec. 31, 1996) [hereinafter ICANN Memorandum of Understanding]; *see also* Heather Mewes, *Memorandum of Understanding on the Generic Top-Level Domain Space of the Internet Domain Name System*, 13 BERKELEY TECH L.J. 235 (1998).

227. For a description of the debate, see Froomkin, *Wrong Turn*, *supra* note 222, at 99-125; Lawrence Lessig, *The Law of Cyberspace*, 112 HARV. L. REV. 1586, 1608-09 (1999).

228. Jeri Clausing, Democracy Tugs at Internet Agency, N.Y. TIMES, Aug. 30, 1999, at C1 (reporting contentious debate regarding ICANN's membership structure and interest group representation).

The U.S. government, however, decided against employing such an approach.[229] Instead, governance was contractually assigned to ICANN. ICANN itself was set up as a not-for-profit corporation incorporated in California and governed by U.S. law.[230] This represents a regulatory mix as well, but of a different flavor than expected. Instead of a combination of international and community-based governance, the ICANN structure is a mix of national and community-based control. The national element is represented not merely by the contractual relationship between ICANN and the Department of Commerce, which has entrusted ICANN with its addressing and naming mission.[231] It is also manifest in the fact that ICANN, as a California corporation, is subject to state and federal laws.[232] At the same time, ICANN enjoys great latitude in its internal decision-making processes, and government oversight (as spelled out in ICANN's agreement with the Department of Commerce) is relatively minimal.[233] Moreover, ICANN is empowered to create procedures to execute its role without having to ask the government for formal agreement to those procedures.[234] Because of the way ICANN may

229. The Department of Commerce has documented the decision-making process and the relevant arguments in the "White Paper," Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 10, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (last visited Nov. 22, 2002). The National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce, issued for comment the "Green Paper," A Proposal to Improve Technical Management of Internet Names and Addresses, *at* http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm (last visited Nov. 22, 2002) . The proposed rulemaking was later published in the Federal Register. Improvement of the Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826 (Feb. 20, 1998).

230. ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers, *at* http://www.icann.org/general/bylaws.htm (last amended Feb. 12, 2002) [hereinafter ICANN, Bylaws].

231. ICANN, Memorandum Of Understanding, *supra* note 226.

232. ICANN, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers, as Revised November 21, 1998, *at* http://www.icann.org/general/articles.htm (last visited Nov. 22, 2002).

233. *See* ICANN, Bylaws, *supra* note 230.

234. ICANN's authority over domain name holders is, in effect, derived from a chain of top-down contracts. ICANN enters into contracts with entities that wish to serve as registries for various top-level domain names (e.g. .com, .net, .rec). These contracts specify the terms of those entities' contracts with domain name registrars (firms that offer domain name registration services to users). The registry–registrar contracts will likely, in turn, specify key terms of registrar–domain name holder contracts. ICANN's power over domain name registration (and through it, possibly other aspects of Internet activity) ultimately derives from its ability to maintain the obedience of operators of top-level domain name root servers, which sit on top of a pyramid of servers that record and track Internet domain names. (A series of servers, with the root servers at the top, enable Internet users to find and get access to websites or to send email.) Conceivably, root server operators could defect, and Internet users could then turn to a variety of root servers to resolve their Internet address search inquiries. But given network effects, users

structure itself and define its procedures, the Internet community retains a very substantial amount of self-governance.[235]

One might argue that the governance mix used for ICANN was at least in part motivated by deeply felt suspicions among members of Congress about delegating governing authority to an international body.[236] ICANN officials maintain, however, that the main reason for the approach eventually adopted was the need for a flexible and timely solution.[237] Any regulatory mix that included a formal international component, the government feared, would have taken too long to finalize. Time was of essence in setting up ICANN because of the death in 1998 of Jon Postel, IANA's undisputed leader.[238] Had it taken too long to find somebody to manage the addressing and numbering tasks, the Internet's operation might have suffered. In comparison to an international organization, which would have required a multiyear international negotiation to set up, ICANN was quickly established and vested with the appropriate governing authority.

The genesis of ICANN did not suggest, however, the addition to the already existing governance mix of a third component. Once installed, ICANN's board of directors, which enjoys very substantial powers

would ultimately settle on a single set of compatible root servers, and whichever entity controlled those servers would effectively assume ICANN's power over domain name registration. *See* Jonathan Weinberg, *Backgrounder: ICANN and Internet Governance* (adapted from Jonathan Weinberg, *Internet Governance*, *in* TRANSNATIONAL CYBERSPACE LAW (Makoto Ibusuki ed., 2000)), *available at* http://www.law.wayne.edu/weinberg/mdrbackgrounder.pdf (last visited Dec. 15, 2002).

235. The Federal Communications Commission (FCC) very likely has statutory jurisdiction over Internet issues. *See* 47 U.S.C. §§ 151-152 (1994). However, the FCC has expressly disavowed any interest in getting involved in Internet governance issues. *See* Alexander Gigante, *Blackhole in Cyberspace: The Legal Void in the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 413, 416, 421-22 (1997); A Framework for Global Electronic Commerce: Executive Summary, July 1, 1997, *available at* http://www.nyls.edu/cmc/papers/whgiifra.htm (last visited Nov. 22, 2002) (setting forth the Administration's approach to Internet issues). Kanishka Jayasuriya has referred to this structural setup as regulated self-regulation. Kanishka Jayasuriya, *Globalization, Law, And the Transformation of Sovereignty: The Emergence of Global Regulatory Governance*, 6 IND. J. GLOBAL LEGAL STUDIES 425, 452 (1999).

236. International corporations and foreign governments have legitimately directed much criticism at the exclusively domestic focus of the proposals in the Green Paper and the White Paper. *See* Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,748 (June 10, 1998) ("White Paper"); Improvement of the Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826 (Feb. 20, 1998) ("Green Paper"); Douglas Hayward, *Europeans Disappointed by Net Names Plan*, *at* http://www.techweb.com/wire/story/domnam/TWB19980130S0009 (Jan. 30, 1998).

237. Interview with Michael Roberts, Former Director, ICANN.

238. *See* James Glave, *Net Mourns Passing of Giant*, *at* http://www.wired.com/news/culture/0,1284,15682,00.html (Oct. 18, 1998); PCEN: About Our Namesake, *at* http://www.postel.org/jonpostel.html (last updated Jan. 7, 2002) (tribute to Jon Postel).

under California law and ICANN's bylaws,[239] became very concerned about its geographic and cultural diversity.[240] It decided that of its nineteen members, only five should be from the United States.[241]

ICANN's next step was the election of nine board members by the Internet public at large. To this end, ICANN organized a global election of these board members, with—at least theoretically—every netizen being able to participate.[242] This radical approach to democratic self-governance on a global scale drew substantial criticism from various quarters.[243] U.S.-based Internet groups in particular expressed concern about the transparency and ultimate legitimacy of such broad elections in the absence of a regulatory framework to ensure election fairness.[244] As a consequence of this criticism, ICANN slowed its process of electing Board members by the public at large—five instead of the originally planned nine Board members were elected in 2000—and promised to monitor carefully the first election scheduled, which took

239. *See* Esther Dyson, Prepared Testimony for the U.S. House of Representatives, Subcommittee on Oversight and Investigation, July 22, 1999, *available at* http://www.icann.org/correspondence/dyson-testimony-22jul99.htm (last visited Dec. 19, 2002) (responding to House Subcommittee on Oversight and Investigation's questions regarding ICANN's formation, structure, and policies).

240. The Bylaws contain a provision designed to achieve international representation on the corporation's Board of Directors:

> In order to ensure broad international representation on the Board: (1) at least one citizen of a country located in each of the geographic regions listed in this Section 6 shall serve as an At Large Director on the Board (other than the Initial Board) at all times; and (2) no more than one-half (1/2) of the total number of At Large Directors serving at any given time shall be citizens of countries located in any one Geographic Region.

ICANN, Bylaws, *supra* note 230, art. V, § 6.

241. A complete list of the board members can be found at ICANN, About ICANN, http://www.icann.org/general/abouticann.htm (last visited Nov. 22, 2002).

242. The composition of the board is detailed in Art. VI of the bylaws. ICANN, Bylaws, *supra* note 230, art. VI.

243. In early September 1998, the Global Internet Project (GIP), a group of technology companies led by IBM and MCI, began a pledge drive to raise $500,000 of start-up money for ICANN**.** Members of GIP claim that they are not interested in influencing Internet policy, but only in advancing the launch of the new company. *See* John Borland, *Pledge Drive For New Domain System Kicks Off*, *at* http://www.techweb.com/wire/story/domnam/TWB19980909S0017 (Sept. 9, 1998); Paul Festa, *Raising Funds for Net Names Body*, CNET News, *at* http://news.com.com/2100-1023-215289.html?tag=mainstry (Sept. 9, 1998).

244. The Department of Commerce Green Paper itself recognizes that there are "substantial differences among Internet stakeholders on how the domain name system should evolve." Improvement of Technical Management of Internet Names and Addresses, 63 Fed. Reg. 8826, 8827 (1998); *cf.* Joseph P. Liu, *Legitimacy And Authority In Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 615 (1999); Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,745 ("Most of those who criticized the proposed allocation of Board seats called for increased representation of their particular interest group on the Board of Directors.").

place in the autumn of 2000. Because of technical problems caused by unexpectedly strong participation, especially from overseas, the election process itself was marred with problems and did not achieve the high standard of inclusiveness ICANN had set for itself. The elections took place, however, and—as a strong indication that ICANN had no hand in influencing the outcome—resulted predominantly in the election of board members vocally critical of ICANN.

One may or may not see these as teething problems of a novel governance setup. What is striking, however, is the actual structural and institutional setup. A U.S.-based nonprofit corporation contractually entrusted by the U.S. government with certain Internet-related tasks not only internationalizes its board of directors, so that members based in the United States are in a clear minority, but also decides to have its board members chosen by a global, all-inclusive election in which only members of the Internet community at large are allowed to partake.

The discussion here is not intended to analyze or critique ICANN and its work.[245] Rather, the focus is on a fascinating combination of national, international, and community-based governance at work with ICANN. In essence, ICANN attempted not just to mix two, but to blend together all three of the models of governance outlined in sections I.1–3 *supra*.

Whether the ICANN experiment will succeed remains to be seen.[246] The heavily-criticized move by ICANN management in 2002 to abolish the at-large membership signals a bit of a retreat from its bold governance innovation. However, it is only a limited retreat. ICANN still maintains its position as a governance organization authorized by the U.S. Department of Commerce, operating as a Californian non-profit, and largely self-regulatory with internal decision-making being done by a Board of Directors that remains fundamentally international, and represents many significant stakeholders.[247] To be sure, although incorporating all three different approaches into one does seem like an

245. For such critiques, see Froomkin, *Wrong Turn*, *supra* note 222; Weinberg, *ICANN and the Problem of Legitimacy,* 50 DUKE L. J. 187 (2000).

246. The main criticism of ICANN so far has been the lack of democratic oversight and due process. *See* Froomkin, *Wrong Turn*, *supra* note 222; Weinberg, *supra* note 245; Michael Geist, *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, at 6 (providing statistical summary through July 7, 2001), *available at* http://aix1.uottawa.ca/~geist/geistudrp.pdf (last visited Dec. 19, 2002). Yet, it is a bit unfair to hold ICANN to a standard of democratic legitimacy on par with that of U.S. federal governance. Although there is still room for substantial improvement compared with many other international regimes, ICANN has been trying hard to ensure legitimacy. *See* Viktor Mayer-Schönberger, *Namenlose Zukunft?, in* DAS RECHT DER DOMAIN NAMEN 189 (Viktor Mayer-Schönberger et al. eds., 2001).

247. *See* ICANN, Appendix A to Minutes of Board Meeting 31 October 2002 New Bylaws, *at* http://www.icann.org/minutes-appa-31oct02.htm (last visited Jan. 10, 2003).

innovative solution, it is no less a "silver bullet" than governance mixes.[248] Whether the blending of the different governance models in the ICANN setup will be workable in the long run, will depend on how well the chosen governance structure fits the governance challenges the organization faces.[249] Clearly, however, the possibility of blending all three governance modes has further broadened the spectrum of possible solutions.

Before analyzing in a bit more detailed way what "blending" entails, however, we need to take a look at another, alternative mode of governance suggested or employed in the enterprise of regulating cyberspace.

IV. GOVERNANCE MIXES VERSUS GOVERNANCE EXTREMES

Regulatory mixes offer some advantages over purely national, international, or community-based governance regimes in cyberspace. They may help enforcement or facilitate legitimacy. But these advantages come at a cost. International governance is time-consuming to set up. National governance provides a suboptimal compromise between legitimacy and enforceability. Community-based regulations suffer from limited enforcement capabilities. Combining governance modes requires skill. The aim is to find a mix that ameliorates the disadvantages of each mode, and to create a combination that is better than the sum of its parts.

Given the limited experience with such mixes, especially in the area of regulating cyberspace, it is quite understandable that there may be resistance to using them. Expanding on the single modes of governance reviewed in section I, one could envision another alternative, which I call "governance extremes." Such an approach would take a single mode of governance and deliberately extend it well beyond its traditional borders.

Some features of such an approach to cyber-governance can be found in recent cases regarding the use of trademarks for domain names. The general structure of these cases is as simple as it is comparable.

248. Moreover, it should not come as a surprise, even to commentators, that adding self-regulation to the governance mix may not solve the legitimacy issue. As discussed in Sections II and III, self-regulation may be more legitimate than other modes of governance, but that does not mean that every instance of self-governance is *automatically* more legitimate. *See supra* Sections II-III.

249. The changes in the Bylaws in 2002, the elimination of At-Large Directors, and the installation of an At-Large Advisory Committee point to the need for continuous adjustment of the governance components to find the optimal mix.

Corporation A has trademarked a name for a particular service in a state (S_A) where it conducts business, whereas corporation B has used—and possibly trademarked—that same name in another state (S_B). B creates a website for its business and goes online. As part of the Internet, the website is accessible from all over the world, including from S_A. A brings a lawsuit against B for trademark infringement based on the ability of potential customers in S_A to access the website.[250] This is a variation of the spillover effect discussed earlier, resulting from the indiscriminate global reach of cyberspace.[251]

Courts generally have been careful to limit their jurisdiction to cases in which B has actively attempted to solicit business from customers in S_A, thereby availing itself of the laws of S_A. A slightly more refined version, the "sliding scale" approach to jurisdiction,[252] appears to be a plausible way of delineating jurisdiction. The devil, however, is in the details. What exactly constitutes the conduct that would subject B to the jurisdiction of the S_A courts? Is it enough to offer online ordering to residents of S_A, or does B need to accept (or even directly solicit) orders from residents of S_A? Is it necessary to target one's website specifically to a particular community to fall within that community's jurisdiction, or is a simple website permitting online shopping sufficient to infringe upon someone else's trademark in any state in which the website can be accessed? The issue, in essence, is who should have to absorb the cost for spillover effects.

Taking the (realist) position that cyberspace conflict will occur regardless of the governance mix chosen, one could envision an extreme position attempting to externalize the effect of governance spillover. Such an approach would subject individuals from outside to one's jurisdiction but opt for strict territorial delineation should other jurisdictions attempt the same.

A somewhat comparable line of cases can be found in the area of Internet gambling.[253] Minnesota began civil proceedings to prevent a

250. *See, e.g.,* Minnesota Mining & Mfg. Co. v. Taylor, 21 F. Supp. 2d 1003, 1005 (D. Minn. 1998) (granting preliminary injunction against defendant's use of "post-it.com," "post-its.com," and "ipostit.com," reasoning that such use would likely dilute plaintiff's "Post-it" mark); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1121 (W.D. Pa. 1997) (plaintiff manufacturer of "Zippo" tobacco lighters alleging trademark dilution, infringement, and false designation against online computer news service for use of domain names "zippo.com," "zippo.net," and "zipponews.com."); Toys "R" Us, Inc. v. Akkaoui, 40 U.S.P.Q.2d (BNA) 1836, 1843 (N.D. Cal. 1996) (granting preliminary injunction against "adultsrus.com" or any other colorable imitation of plaintiff's mark for Internet sites and reasoning that use of such domain names tarnishes plaintiff's "Toys 'R' Us" and "Kids 'R' Us" trademarks).

251. *See supra* Section II., at [PAGE]; *supra* Section IV, at [PAGE].

252. *Zippo*, 952 F. Supp. at 1124.

253. Michael Anastasio, *The Enforceability of Internet Gambling Debts: Laws, Policies, and*

Nevada corporation from offering online gambling, although the company's activity was legal in Nevada.[254] Minnesota's attorney general asserted that he would even stop the company from operating its website in Central America, although the operation was perfectly legal there.[255] Recently, shareholders of a company that was legally operating a gambling website on the Caribbean island of Antigua were found liable by a New York court for the violation of a New York prohibition on gambling. Again, the courts effectively extended the jurisdictional reach of state law to cover the entire globe.[256]

Causes of Action, 6 VA. J.L. & TECH. 6 (2001); Jeffrey A. Dempsey, *Comment: Surfing for Wampum: Federal Regulation of Internet Gambling and Native American Sovereignty,* 25 AM. INDIAN L. REV. 133 (2000/2001); Joseph M. Kelly, *Internet Gambling Law*, 26 WM. MITCHELL L. REV. 117 (2000); Beau Thompson, *Internet Gambling*, 2 N.C. J.L. & TECH. 81 (2001). The U.S. government estimates that online sports betting garnered $600 million in gross revenues in 1997, up from $60 million in 1996. Nelson Rose, *Internet Gambling: Domestic and International Developments*, SC 91 A.L.I.-A.B.A. 131, 138 (1998); *see also* Cassandra Burrell, *Senate Targets Internet Gaming*, CHATTANOOGA TIMES, July 24, 1998, at A11; Greg Connors, *Government Efforts at Industry Regulation Show a House; Divided*, THE BUFFALO NEWS, July 12, 2000, at 1C; Tom Gorman, *Nevada Net Gaming May Be in Cards,* LOS ANGELES TIMES, June 5, 2001, at A1-14; Virtual Gaming Technologies Inc. Successfully Launched Credit Card Processing with Barclays Bank, BUS. WIRE, Aug. 26, 1998 ("Virtual Gaming Technologies (Antigua) Ltd. (a wholly-owned subsidiary of the company) conducts online gaming, over the Internet, exclusively targeting non-U.S. residents. Its online Virtual Casino at: http://www.virtcasino.com, has been accepting membership applications since November 1997."); Adam Creed, *Law Fails To Slow Online Gambling In Australia*, CasinoNews.Org, Feb. 6, 2002, *at* http://www.casinonews.org/archive/AA-AID=1201.html; James Ledbetter & Steve Viuker, *Net Gambling Craps Out in New York*, The Industry Standard, July 27, 1999, *at* http://www.thestandard.com/article/0,1902,5677,00.html; Gwendolyn Mariano, *Bill Set To Ban Net Gambling*, CNet News.com, *at* http://news.com.com/2110-1023-274370.html (Oct. 12, 2001); I. Nelson Rose, *100% Legal Gambling on the Internet?* (1999) ("Over the past six years, the number of web sites which will accept money bets has grown from zero to more than 250."), *at* http://www.gamblingandthelaw.com/legigamb.html (last visited Dec. 19, 2002); *see also* Written Question E-1190/98 - 99/C 31/025, 1999 O.J. (C 31) 21-22; Charles Keenan, *Web Wagering Firms Try to Entice Banks*, AM. BANKER, Mar. 2, 1999 ("Virtual Gaming Technologies Inc. of San Diego runs a service out of Antigua. . . . It does not allow gamblers with U.S. Internet addresses to place bets, said Bruce Merati, chief financial officer. The Web site, www.virtcasino.com, operates in six languages and clears credit card transactions in more than 60 countries . . . ."); *Online Gambling Comes to Region*, S. AM. REP., Mar. 1, 1999, *available at* 1999 WL 8887038; *see also* Arjan Van 'T Veer, *Internet Gaming in Europe: State of the Art*, 2 GAMING L. REV., 153, 153-54 (1998); Bruce Orwall, *Place Your Bets: Despite Lots of Obstacles, Gambling is Making Its Way Onto the Net*, ASIAN WALL ST. J., Apr. 3, 1996 (special report).

254. Johnson & Post, *Law & Borders*, *supra* note 3, at 1374 n.21 (citing Complaint, Minnesota v. Granite Gate Resorts, Inc., No. 9507227 (1995)).

255. *Id.*

256. *See*, *e.g.*, United States v. McDonough, 835 F.2d 1103, 1104-05 (5th Cir. 1988) (rejecting defendant's argument that the Wire Act did not apply to him because gambling information had been transmitted to him in Massachusetts, and there were apparently no laws in Massachusetts that explicitly forbade the transmission of wagers into the state, and instead holding that although § 1084(b) permits the transmission of gambling-related information when gambling is explicitly authorized in both the sending and receiving states, it was never intended to

The *reductio ad absurdum* of such a governance extremes approach to setting limits on the state's jurisdiction to adjudicate is that everybody in cyberspace would face the potential risk of being hauled into court by anyone, anywhere in the world.[257] To successfully employ such an extensive jurisdictional application of its laws, a country would have to possess enough power to enforce the decisions of its courts even extraterritorially. In a nutshell, governance extremes work best for a hegemon. The approach's utility diminishes the less powerful is the nation that employs it, as well as the more other nations use it.

Given its strong economic, political, and military position in the world, as well as its important trailblazing role in the development of cyberspace, the United States could be such a hegemon. The structural setup of ICANN exemplifies that it can effectively force the hand of the world. If a nation has the necessary enforcement power, choosing such a governance extreme must sound quite attractive.[258] Yet, should the

authorize gambling when only one of the two locales permits gambling); State v. Fiola, 576 A.2d 338, 340 (N.J. Super. Ct. App. Div. 1990) (holding that the defendants' business constituted gambling activity within the state of New Jersey and thus violated the state's gambling laws, since the New Jersey Constitution prohibits any type of gambling unless the constitution has been amended to explicitly permit the specific type of gambling); People v. Kim, 585 N.Y.S.2d 310, 312 (Crim. Ct. 1992) (holding that the use of a computer system to transmit orders for out-of-state lottery tickets was illegal since "[a]ll forms of gambling are illegal in New York except those expressly authorized by the New York Constitution"). *See also* Scherr v. Abrahams, 1998 WL 299678 (N.D. Ill.) (denying jurisdiction although the defendant's website allowed users to contact him via e-mail, and he sent his publication to users via e-mail).In essence, there are three points on this "sliding scale" spectrum. American Homecare Federation, Inc. v. Paragon Scientific Corp., 27 F. Supp. 2d 109, 113 (D. Conn. 1998). At one end of the scale is the passive website that contains only information and offers no interaction with the visitor. *Id.* At this end of the scale, the assertion of jurisdiction will likely be declined. *Id.* In the middle of the scale are websites where information is exchanged between the site operator and the visitors, including downloadable files or links to other websites. *Id.* It is in the middle of this scale where the circumstances that will lead a court to assert jurisdiction are most ambiguous. At the other end of the spectrum are the sites that engage in substantial activity within a forum state, such as: 1) sales; 2) solicitations; 3) acceptance of orders; 4) links to other sites; 5) product lists; or 6) the transmission of files. *Id.* at 113-14. These sites will most likely provide a court with ample reason to assert jurisdiction. Mieczkowski v. Masco Corp., 997 F. Supp. 782, 788 (E.D. Tex. 1998) (conferring general jurisdiction over the company, which, in addition to hosting an Internet website within the state, also conducted business there); *see also* People v. World Interactive Gaming Corp., 1999 WL 591995, at *2 (N.Y. Sup. Ct.). *See generally* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1208 (1998); Cynthia R. Janower, *Gambling on the Internet*, 2 J. COMPUTER-MEDIATED COMM. (1996), *available at* http://www.ascusc.org/jcmc/vol2/issue2/janower.html (last visited Nov. 25, 2002).

257. *But see* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1205-12 (suggesting that such spillovers are overstated).

258. S*ee, e.g.*, Deborah Bailey-Wells, *Internet Jurisdiction and Liability: Issues for Copyright & Trademark Cases*, *in* GLOBAL TRADEMARK AND COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY RIGHTS IN THE INTERNATIONAL MARKETPLACE (Practising Law Institute ed., 1997); James H. Aiken, *The Jurisdiction of Trademark and Copyright Infringement on the Internet*, 48 MERCER L. REV. 1331 (1997) (arguing for a broad scope of jurisdiction); Ian C. Ballon,

United States decide to proceed along that path in a more concerted effort, it would essentially open the floodgates for other nations to follow suit. But as international law experts including Lea Brilmayer have repeatedly pointed out, such an extreme approach might not be feasible in the long term, as over time cyberspace's center of gravity may move away from the United States.[259] Moreover, as it would impede cooperation and coordination, it might also have negative long-term consequences for the hegemon's role in the international society.[260]

A different regulatory extreme has already been briefly mentioned in section I: that of cyber-anarchism. This is John Perry Barlow's idea that the only way forward for cyberspace is not self-governance but no governance. Legal theorists, sociologists, and behavioral biologists agree that conflicts arise in any society.[261] If no formal, institutional conflict resolution system is in place, conflict will be resolved by power.[262] Hence, Barlow's cyber-anarchism will—absent of any form of governance—over time progress toward cyber-Darwinism, in which the most powerful will rule over the powerless. The question is whether our society (or any society for that matter) would prefer such a regime over its current conflict resolution setup. Again, as with the governance extreme of a vastly expansive jurisdiction, in the long run cyber-

Rethinking Cyberspace Jurisdiction in Intellectual Property Disputes, 21 U. PA. J. INT'L ECON. L. 481 (2000) (examining the very extensive jurisdictional reach of the Anticybersquatting Consumer Protection Act); Ginsburg*, Copyright without Borders?*, *supra* note 33 (suggesting that if a suitable link can be established, jurisdiction in the United States should be assumed, even if actual copyright infringement happens abroad); Lea Hall, *The Evolving Law of Personal Jurisdiction for Trademark Infringement on the Internet*, 66 MISS. L.J. 457 (1996).

259. *See, e.g.,* Lea Brilmayer, *What's the Matter with Selective Intervention?*, 37 ARIZ. L. REV. 955 (1995); *see also* Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217 (1992); Lea Brilmayer & Kathleen Paisley, *Personal Jurisdiction and Substantive Legal Relations: Corporations, Conspiracies, and Agency*, 74 CALIF. L. REV. 1 (1986).

260. *Cf.* JOSEPH S. NYE, THE PARADOX OF AMERICAN POWER: WHY THE WORLD'S ONLY SUPERPOWER CAN'T GO IT ALONE (2002).

261. *See* SIGMUND FREUD, CIVILIZATION AND ITS DISCONTENTS 144 (1962) ("As we already know, the problem before us is how to get rid of the greatest hindrance to civilization – namely, the constitutional inclination of human beings to be aggressive towards one another"); NICCOLÒ MACHIAVELLI, THE PRINCE 10 (1999 ed.) ("[T]here is no avoiding war; it can only be postponed to the advantage of others."); Suzy Hansen, *The Invention of Peace*, Salon.com Books (interview with Sir Michael Howard, "one of Britain's foremost military historians," who states that "Conflict is a natural state at every level of human life. [. . .] Conflict is what is endemic, and, if you like, is natural."), *at* http://www.salon.com/books/int/2001/04/12/howard/index.html (last visited Nov. 22, 2002).

262. *See* THOMAS HOBBES, LEVIATHAN 18-19 (1651) ("And therefore, as when there is a controversy in an account, the parties must by their own accord, set up for right Reason, the Reason of some Arbitrator, or Judge, to whose sentence they will both stand, or their controversie [sic] must either come to blowes [sic], or be undecided. . .").

Darwinism's costs are likely to be too high for anyone to seriously advocate it.

V. THE REGULATORY BLEND

Earlier I used a triangle as a metaphor of how the three different modes of regulating cyberspace might interact.[263] The vertices of the triangle represent the modes of governance – community-based, national and international – in their unadulterated forms. The sides signify possible governance mixes. The regulation of obscenity, as described at Section III.1 *supra*, would lie perhaps midway along the side connecting the two vertices of national and community-based modes of governance. Similarly, the regulatory approach of the EU directives could be positioned somewhere between the vertices signifying national and international modes. Transnational governmental networks would be somewhere along the same side, but because of their looser, more informal international structure, they would fall closer to the "national" vertex.

Depicting the available options of cyber-regulation in this way will permit a widening of the range of available regulatory options from just three – represented by the three vertices of the triangle – to whole spectrums of regulatory mixes, symbolized by the three line segments connecting the three corners.

The ICANN example is especially instructive because it offers an early glimpse into the possibility not merely of mixing two regulatory models, but of *blending* together all three of them. ICANN shows that any combination of the three modes of governance is possible. Any particular cyber-regulation made up of such a three-way blend may be represented by a point within the regulatory triangle depicted in Figure 2. This is of substantial significance, because it entails a drastic expansion of available regulatory options, whose scope it expands to include the area within the triangle's borders.

To be sure, this increase in theoretically available options comes at a price. Governance blends potentially are less transparent to people than existing governance regimes, which are founded to a much larger extent on more familiar territorial and physical concepts. Blends do not necessarily, but in some instances might lead to an increase in overlaps of governance regimes, which potentially could also increase the level of legal uncertainty. But such overlaps are not new. Transnational transactions routinely take place in a governance space that has some

263. *Cf.* Figure 1 *supra*.

governance overlaps and blends. Conflict-of-laws doctrine attempts to minimize these, but even these metarules for defining governance sometimes overlap, and transacting parties have learned to live with the remaining uncertainty.[264] It would be imprudent, therefore, to discard mixes and blends because they cannot guarantee certainty of regulatory governance.[265]

VI. PLACING THE SHAPE

The triangle has helped us to visualize the multiplicity of options available for cyber-regulation. But the triangle may be useful in yet another task: providing a metaphor of what evaluating the chosen mix or blend of governance is all about.

I have already mentioned two fundamental goals that regulatory frameworks strive to achieve: legitimacy and enforceability.[266] In the model of stacked modes of governance, these two values were represented as two inverse functions that resembled two parallel dimensions with an inescapable trade-off. The triangle helps us to extend our conceptual understanding of possible governance structures and dispel the illusion of a trade-off between legitimacy and enforceability. It also frees us to think—at least *prima facie*—of these two values not as intrinsically linked but as independent from each other. What therefore if, instead of positing an inescapable trade-off, we take these two values as two independent dimensions, spanning a plane

264. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 33, at 1209.

265. Moreover, governance overlaps may be less problematic than we think. Many have lived with multiple overlapping or even contradictory regulatory frameworks in societies of "legal pluralism." Legal pluralism argues that "the legal order of all societies is not an exclusive, systematic and unified hierarchical ordering of normative propositions depending from the state but has its sources in the self-regulatory activities of all the multifarious social fields present in society." John Griffith, *Legal Pluralism and the Theory of Legislation – With Special Reference to the Regulation of Euthanasia*, *in* LEGAL POLYCENTRICITY: CONSEQUENCES OF PLURALISM IN LAW 201, 201-02 (Hanne Petersen & Henrik Zahle eds., 1995). The concept of legal pluralism unites historical, sociological and legal theory lines of argument. Historically, the analysis centers around the blend of colonial power and formal legal systems with local tradition. A sociological approach points to the necessary overlap of formal and informal incentives on human behavior. Finally, legal theory has perceived the idea of legal polycentricity as a way to avoid the dichotomy between complete indeterminacy of critical legal studies and Dworkin's Hercules-judges. *See id.*; Gunther Teubner, "*Global Bukowina": Legal Pluralism in the World Society*, *in* GLOBAL LAW WITHOUT A STATE 3 (Gunther Teubner ed., 1997); *see also* MASAJI CHIBA, LEGAL PLURALISM: TOWARD A GENERAL THEORY THROUGH JAPANESE LEGAL CULTURE (1989); LEGAL PLURALISM AND THE COLONIAL LEGACY: INDIGENOUS EXPERIENCES OF JUSTICE IN CANADA, AUSTRALIA AND NEW ZEALAND (Kayleen M. Hazlehurst ed., 1995); SURYA PRAKASH SINHA, LEGAL POLYCENTRICITY AND INTERNATIONAL LAW (1996).

266. *See supra* Section II.

in which we could place the vertices of the triangle, and thereby set its shape? Evaluating governance frameworks would involve evaluating how they score on these two dimensions and placing them accordingly. Any governance regime would then be represented by a point within the triangular shape, and choosing the most appropriate governance blend is equivalent to selecting the point with the most suitable combination of legitimacy and enforceability (see figure 3).

Yet, it is important to understand that the triangle and the coordinate plane of legitimacy and enforceability are metaphors to help us envision a variety of governance options. They do not provide a mathematical model by which a governance "sweet spot," the ideal combination of governance modes given desired levels of legitimacy and enforceability, can be found. There is nothing magical, mythical, or mathematical about the triangle. To intentionally mix metaphors: the triangle is no "silver bullet" for selecting governance modes. But as a metaphor it may be a most useful visual tool for thinking about the possible universe of governance mixes and blends—and how they relate to legitimacy and enforceability—and may provide a vastly more open-ended view of options than mono-dimensional alternatives.

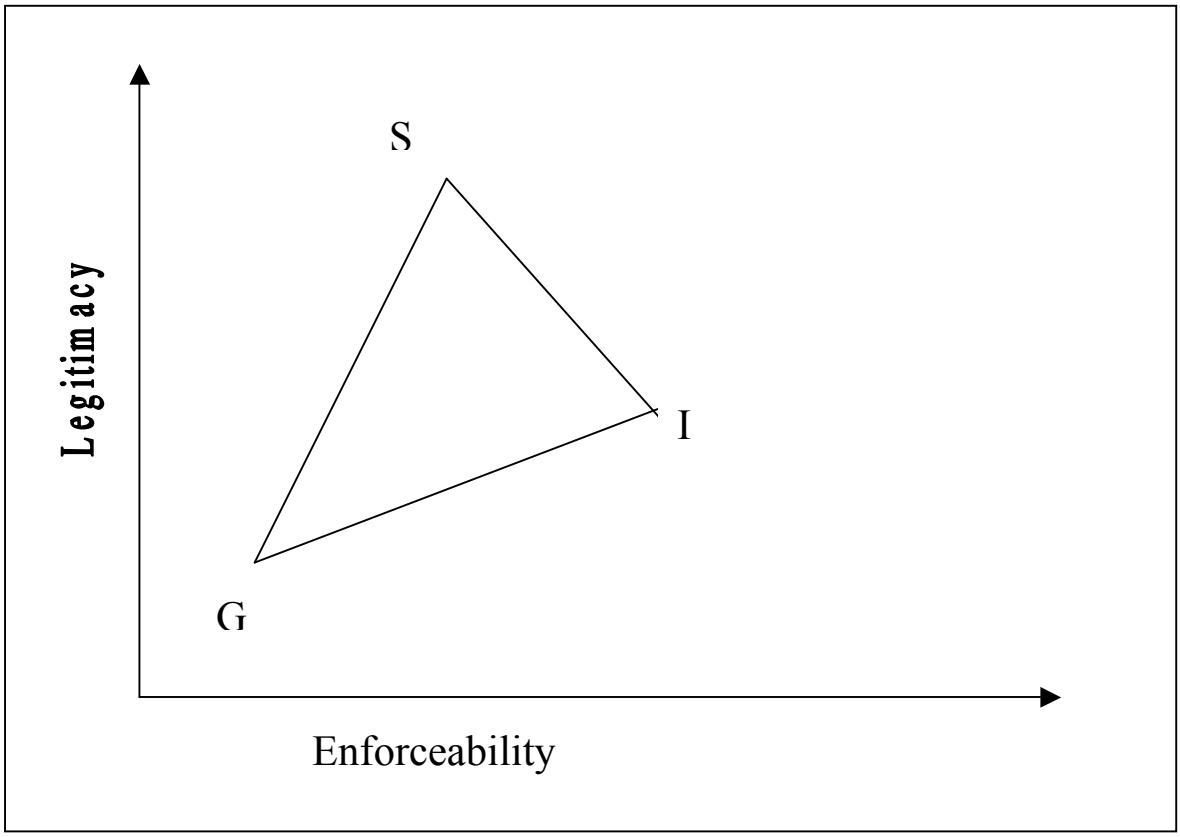


Figure 3: Placing the shape in the Legitimacy/Enforceability space

VII. CONCLUSION

Cyberlaw discourses ostensibly focus on substantive legal issues, like content control, intellectual property protection, and the preservation of privacy. Interwoven in these discourses are arguments about the appropriate mode of governance for cyberspace. Examining the governance strand of the cyberlaw discourses, this article has identified three strings of claims (and counterclaims) commentators have advanced for national, community/self-regulation, and international governance, engaging with each other in a binary, zero-sum debate. Others have advocated a somewhat different conception of governance modes, stacking them up as three layers, with community governance on the bottom and international governance on top. Coupled with this layered conception is the belief that these three distinct governance modes provide inversely proportional levels of legitimacy and enforceability. For example, international governance is generally seen

as having the highest enforceability but the lowest legitimacy, and community-based governance is seen as very legitimate but difficult to enforce on a global network. Implicit in these metaphorical understandings is the recognition that there is an inexplicable and inescapable tradeoff between legitimacy and enforceability.

To overcome the conceptual paucity of such mono-dimensional metaphors, I have suggested in this article that cyber-governance be envisioned instead as a triangle, with vertices representing the three traditional modes of governance. Breaking the restrictive mold of binary debates or layers, this shift in metaphors may help us understand that modes of governance can, and in fact are, quite frequently mixed together, ideally to offset each other's weaknesses. U.S. law regulating obscene speech, with its combination of national (or state) and community governance, the EU directives as international legal documents requiring national implementation, and transgovernmental networks provide sufficient examples of such mixed modes of governance even outside the confines of cyberspace. I have also argued that the triangle is useful in conceptualizing present and envisioning future standardization processes, especially as they pertain to the Internet, as well as explaining the unique setup of ICANN. The triangle's metaphorical usefulness does not, however, end there. It may also help us appreciate the potential not just to mix any two modes of governance, but also to blend together all three of them, as ICANN intriguingly demonstrates. The power of the triangular metaphor is the tremendous spectrum of possible governance solutions it helps us to conceptualize.

Moreover, moving away from binarity and stacked layers, the two-dimensionality of the triangle also facilitates our understanding of legitimacy and enforceability as two - at least *prima facie* - independent values used to measure good governance, overcoming the tragic choices embodied in simplistic views of inescapable trade-offs. Taking the metaphor a step further, we can even grasp the assessment of any particular governance regime by envisioning placing a triangle on a coordinate plane created by legitimacy and enforceability.

To be sure, placing the triangle is nothing but a metaphorical way of understanding how mixes and blends of governance are linked to legitimacy and enforceability. The triangle does not provide us with a "silver bullet" enabling us easily to devise an optimal governance solution. It is no recipe for success. In fact, it is little more than a simple metaphor. Yet, its remarkable power lies in its ability to help us break free of the all-too-restrictive conceptions of cyberspace governance of the past and to inform the debate about much-needed,

more innovative governance models of the future.