Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory

Neil W. Netanel

The University of Texas School of Law

As published in 88 California Law Review 395 (2000).

Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory

Neil Weinstock Netanel†

TABLE OF CONTENTS

† Arnold, White & Durkee Centennial Professor of Law, University of Texas School of Law. Please send comments to: nnetanel@mail.law.utexas.edu. My thanks to the following persons, whose comments on earlier drafts of this Article and related subject matter greatly contributed to its development: Lynn Baker, Niva Elkin-Koren, Mark Lemley, Eben Moglen, David Post, Ilan Saban, Eli Salzberger, Paul Schwartz, Steve Ratner, Charlie Silver, Eugene Volokh, and Jonathan Weinberg. My thanks also to Alisa Ullian for her research assistance, and to participants at the University of Haifa and Hebrew University law faculty colloquia and the Tel-Aviv University Faculty of Law Conference on Law, Technology, and Information, at which I presented parts of this Article.

Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory

Neil Weinstock Netanel

The idea that cyberspace should be presumptively self-governing has resounded in thoughtful scholarship and has colored federal rhetoric and policy regarding electronic commerce. In this Article, Professor Netanel critiques a central prong of the argument for cyberspace self-governance: The claim that a self-governing cyberspace, which its advocates see as a shining example of "bottom-up private ordering," would more fully realize liberal democratic ideals than does nation-state representative democracy. Although granting that this claim poses an intriguing challenge to traditional liberal democratic theory, Professor Netanel argues that it ultimately fails. He contends, indeed, that an untrammeled cyberspace would ultimately prove inimical to the ideals of liberal democracy. It would free majorities to trample upon minorities and serve as a breeding ground for invidious status discrimination, narrowcasting and mainstreaming content selection, systematic invasions of privacy, and gross inequalities in the distribution of basic requisites for citizenship in the information age. Accordingly, Professor Netanel concludes, selective government regulation of cyberspace is warranted to protect and promote liberal democratic ideals.

> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.
>
> —John Perry Barlow, *A Declaration of the Independence of Cyberspace*[1]

1. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (visited Dec. 25, 1999) <http://www.eff.org/~barlow/Declaration-Final.html>.

INTRODUCTION

John Perry Barlow's impassioned call for cyberspace independence cannot be dismissed as the mere theatrical whimsy of a former lyricist for the Grateful Dead. The idea that cyberspace should be presumptively self-governing has resounded in thoughtful scholarship.[2] It has also colored federal policy regarding electronic commerce. A 1997 Presidential Directive, which heralded the dramatic withdrawal of the United States government from significant portions of Internet administration,[3] instructs federal agencies to "recognize the unique qualities of the Internet, including its decentralized nature and its tradition of bottom-up governance."[4]

---

2. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) [hereinafter Johnson & Post, *Law and Borders*]; David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3 (visited Sept. 10, 1998) <http://www.wm.edu/law/publications/jol/post.html> [hereinafter Post, *Anarchy*]; David Post & David R. Johnson, *The New 'Civic Virtue' of the Internet*, *in* THE EMERGING INTERNET 23 (Institute for Information Studies 1998), *available at* (visited Sept. 28, 1998) <http://www.cli.org/paper4.htm> [hereinafter Post & Johnson, *Civic Virtue*]. Commentators who have made similar arguments include 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); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994) (contending that in the absence of some compelling social reason to the contrary, rules of conduct in cyberspace should be governed by self-help, custom, and contract of cyberspace participants); Henry H. Perritt, Jr., *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?*, 12 BERKELEY TECH. L.J. 413, 419-20 (1997) (contending that as a general rule "self-governance is desirable for electronic communities"); Edward J. Valauskas, *Lex Networkia: Understanding the Internet Community*, FIRST MONDAY (Oct. 7, 1996) <http://www.firstmonday.dk/issues/issue4/valauskas/index.html> (calling for formalization of Internet self-governance).

3. Since its inception, the Internet domain name system has been administered by the United States government through contract. In June 1998, the Clinton Administration announced that, as part of its overall policy of promoting Internet self-regulation, it would turn over responsibility for such administration to a new nonprofit corporation. *See* National Telecomms. and Info. Admin., U.S. Dep't of Commerce, Statement of Policy on Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (1998). The government subsequently retained the right to reassert its authority over domain name administration. *See infra* note 377.

4. *Presidential Directive on Electronic Commerce* (July 1997) <http://www.ecommerce.gov/presiden.htm>. The Clinton Administration has been highly inconsistent in following its own Internet self-governance rhetoric. On one hand, in addition to its announced withdrawal from Internet domain name registration, the Administration has supported a three-year moratorium on imposing taxes on Internet sales and has steadfastly insisted that industry self-regulation is the preferred alternative for protecting Internet user privacy. *See* Internet Tax Freedom Act, Pub. L. No. 105-277, 112 Stat. 2681 (1998), *available at* <http://www.house.gov/cox/nettax/law.html> (tax moratorium); *Clinton Administration Support* (last modified Jan. 15, 1999) <http://www.house.gov/cox/nettax/Web-clinton.html> (detailing Clinton Administration support for the Act); FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (1999) [hereinafter FTC PRIVACY REPORT] (advocating industry self-regulation of online data practices). But on the other hand, the Administration has forbidden the export of digital encryption technology, backed legislation (since stricken down as an unconstitutional burden on free speech) prohibiting the Internet transmission of indecent material to minors, and sponsored legislation prohibiting the circumvention of technological measures designed to control online access to and uses of copyrighted works. *See* Digital Millennium Copyright Act, Act of Oct. 28, 1998, Pub. L. No. 105-304, § 1, 112 Stat. 2860 (short title: "Prohibiting Circumvention"); Reno v. ACLU, 521 U.S. 897 (1997) (striking down Communications Decency

Cyberspace is a burgeoning realm of communication taking place over a global web of linked computers.[5] John Perry Barlow notwithstanding, that realm is firmly embedded in a foundation of state institutions, subsidies, and law.[6] But within the interstices of state intervention and support, cyberspace also offers a rich field for private ordering. Rule making within cyberspace reflects the highly decentralized character of cyberspace's communicative matrix. It finds expression in myriad forms and settings, including web site terms of use; behavioral norms of virtual chat rooms and discussion groups; network administration guidelines; listserv moderator filtering; Internet service provider contracts; Usenet voting procedures;[7] local area network acceptable use policies;[8] newsgroup

---

Act of 1996); Jeri Clausing, *Internet Tax Debate Returns to the Hill*, N.Y. TIMES ON THE WEB (Sept. 28, 1999) <http://www.nytimes.com/library/tech/99/09/cyber/capital/28capital.html> (reporting the Administration's recent plan to lift encryption technology export controls after years of resisting calls to do so).

5. Cyberspace includes the physical infrastructure, software, expressive content, and human activity that make up the Internet, Usenet, World Wide Web, and other interconnected digital networks. I use the now-conventional term *cyberspace* with some hesitancy. To some, the term suggests that communication over packet-based digital networks constitutes a world unto itself, fundamentally separate from "offline" life. In contrast I join with other commentators in insisting that such digital communication is simply another activity, one increasingly integrated with offline commerce, communication, politics, and community. *See, e.g.*, Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703 (1998); Philip E. Agre, *Life After Cyberspace*, 18 EASST REV. (Sept. 1999) <http://www.chem.uva.nl/easst/easst993.html>. On the other hand, digital communication over a decentralized, multi-hub global network of linked computers is, in many respects, qualitatively different from offline communication and does present unprecedented challenges to a wide variety of offline institutions. For that reason, it does make sense to refer to cyberspace as a distinct communicative realm, just as one might speak metaphorically of the "world" of academia or law practice. Although none would seriously contend that either world is a freestanding physical or social domain, each—like cyberspace—has its own peculiar rules, institutions, bodies of knowledge, and social practice.

6. The Internet began as a U.S. Department of Defense initiative. *See* Steve Bickerstaff, *Shackles on the Giant: How the Federal Government Created Microsoft, Personal Computers, and the Internet*, 78 TEX. L. REV. 1, 38 (1999). Its use remains heavily subsidized by the public fisc and by telecommunications regulations maintaining cross-subsidies from telephone and other non-Internet services. *See id.* at 45-55, 82-83; Jonathan Weinberg, *The Internet and "Telecommunications Services": Access Charges, Universal Service Mechanisms and Other Flotsam of the Regulatory System*, 16 YALE J. ON REG. 211 (1999). Moreover, ownership and possession of the Internet's physical infrastructure of computers and telecommunications cables is secured by property law, and Internet users live and work (and garner the material resources needed for Internet access) in the real world outside cyberspace, governed by the law of territorial states. *See* Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI-KENT L. REV. 1295 (1998) (contending that Internet ordering depends upon a background of state created and enforced property and contract law); *see also* A. M. Rutkowski, *Factors Shaping Internet Self-Governance*, *in* COORDINATING THE INTERNET 92 (Brian Kahin & James H. Keller eds., 1997) [hereinafter COORDINATING THE INTERNET] (describing U.S. government and intergovernmental involvement in Internet administration and development).

7. The Usenet is a network of discussion groups called *newsgroups*, each of which is established for a specific topic, ranging from topics you can imagine to those you could never imagine. Newsgroup messages are stored on a computer for a specified period of time, usually a couple of weeks. When a newsgroup member signs on, she typically reads a list of messages, which contain hypertext links to the messages themselves. She may then choose to read some messages and may or

frequently-asked question files; decisions of virtual magistrates;[9] help manners and programmers' manuals for multi-user dimensions;[10] the code embedded in browsers, servers, and digital content;[11] and the technical protocols that enable intra- and inter-network communication. All such norms shape and delimit the possibilities for human interaction and commerce in cyberspace. In that sense, they have much the same effect as formal state-promulgated law.[12]

As cyberspace grows to encompass ever-increasing areas of human thought, interaction, and commerce, it regularly co-mingles with the sorts of "real world" activity, ranging from product sales to criminal conspiracy, commonly subject to state regulation. As a result, courts and legislators have increasingly applied real world, state-promulgated law to cyberspace activity, steadily constricting the domain of semi-autonomous cyberspace rule making.[13] But despite these incursions, supporters of cyberspace

---

may not reply by posting her own message on the newsgroup bulletin board. The Usenet used to be a completely independent communications network. It is now functionally interconnected with the Internet. *See* Charles D. Siegal, *Rule Formation in Non-Hierarchical Systems*, 16 TEMP. ENVTL. L. & TECH. J. 173, 181-84, 186-91 (1998). New newsgroups are typically established through an Internet-wide voting procedure. *See infra* note 48.

8. *See* Gibbons, *supra* note 2, at 493.

9. On arbitration in cyberspace, see George H. Friedman, *Alternative Dispute Resolution and Emerging Online Technologies: Challenges and Opportunities*, 19 HASTINGS COMM. & ENT. L.J. 695 (1997); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 94-100 (1996) (discussing possibilities for arbitration to resolve disputes arising from Internet use).

10. The Internet contains numerous virtual spaces called multi-user dimensions ("MUDs"). A MUD is a computer program that creates a virtual environment that can be accessed by remote users, who assume the persona of characters in that world. Many MUDs are games. Others are organized for social or educational purposes. MUD participants can typically determine the characteristics of the persona they assume and can determine with which other characters they will interact. In some MUDs, participants can create and program robots and other objects for use by their character. Such MUDs are often called "MOOs," for MUD-object-oriented. MUDs and MOOs typically follow a set of rules regarding participant interaction and the characteristics of various virtual objects and surroundings in which interaction takes place. *See* Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMOO*, 2 J. COMPUTER-MEDIATED COMM. (June 1996) <http://www.ascusc.org/jcmc/vol2/issue1/lambda.html> (describing MOO rules); Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1197 n.86 (1999) (describing MUDs).

11. *See generally* Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181 (1997) [hereinafter Lessig, *Constitution of Code*]; Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996); Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

12. On norms as "law," see Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. PA. L. REV. 2181 (1996); Robert D. Cooter, *Against Legal Centrism*, 81 CALIF. L. REV. 417 (1993) (book review). A newly published, but already seminal work on cyberspace code and architecture as law is LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

13. Among numerous examples of judicial intervention are: Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999) (instructing district court to preliminarily enjoin defendant's use of plaintiff's trademark in defendant's web site domain name and metatags); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (E.D. Ohio 1997) (enjoining defendants unsolicited email advertisements as trespass to chattels). Legislation governing cyberspace

self-governance (I will call them "cyberians") insist that cyberspace rule making is far more than a set of isolated local arrangements. For them, cyberspace is partly a model and partly a metaphor for a fundamental restructuring of our political institutions. Cyberians view cyberspace as a realm in which "bottom-up private ordering" can and, indeed, should supplant rule by the distant, sluggish, and unresponsive bureaucratic state.[14] By its very architecture and global reach, they contend, cyberspace will ultimately elude the strictures of state-created law, challenging the efficacy and theoretical underpinnings of the territorial sovereign state.[15]

Cyberians raise three types of arguments in support of their broad vision of cyberspace self-governance. Their first argument is that cyberspace independence will maximize welfare. Cyberians assert that the multiple, decentralized, interconnected sites for digital communication that make up cyberspace create greatly enhanced possibilities for flexible decision making, transacting, and norm creation that more efficiently allocate resources than centralized, bureaucratic state regulation.[16] Second, cyberians claim that state regulation of cyberspace is essentially futile and thus the state should not attempt it. Given the decentralized character and global reach of digital network communication, any nation-state's effort to impose its stamp on that communication will simply be met by regulatory arbitrage and evasion.[17] Third, cyberians argue that cyberspace self-governance more fully realizes liberal democratic ideals than does

---

activity includes, among many other examples: Digital Millennium Copyright Act, Act of Oct. 28, 1998, Pub. L. No. 105-304, § 1, 112 Stat. 2860 (proscribing circumvention of technology controlling access to copyrighted works and regulating copyright infringement liability of Internet service providers); Child Online Protection Act, Pub. L. No. 105-277, tit. XVI, 112 Stat. 2681, 2736-41 (1998) (to be codified at 47 U.S.C. § 231) (forbidding according minors access to web sites containing indecent material); CAL. BUS. & PROF. CODE § 17538.45 (West Supp. 1999) (regulating dissemination of unsolicited email advertisements).

14. *See, e.g.*, Post & Johnson, *Civic Virtue*, *supra* note 2, at 25-26 (arguing that "bottom up" governance in cyberspace markets may be superior to "top down" rule by traditional democratic debate and legislative action); David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 170-71 (1996) (depicting local cyberspace rule making as a prime example of the possibilities for realizing a "Jeffersonian mode of law-making," a radically decentralized political order based on individual choice).

15. *See, e.g.*, JAMES DALE DAVIDSON & LORD WILLIAM REES-MOGG, THE SOVEREIGN INDIVIDUAL: HOW TO SURVIVE AND THRIVE DURING THE COLLAPSE OF THE WELFARE STATE 17-26 (1997) (predicting that territorial nation-states will give way to "merchant republics of cyberspace"); Post, *supra* note 14, at 163 (contending that cyberspace may herald the "final days of a governance system relying on individual sovereign states as primary law-making authority").

16. *See* Gibbons, *supra* note 2, at 509-10; David Post & David R. Johnson, *Chaos Prevailing on Every Continent: A New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. 1055 (1998).

17. *See* Gibbons, *supra* note 2, at 502; Johnson & Post, *Law and Borders*, *supra* note 2, at 1373-74; *cf.* Dan Burk, *Virtual Exit in the Global Information Economy*, 73 CHI.-KENT. L. REV. 943, 961-72 (1998) (predicting that, by providing a ready means of virtual mobility, the Internet will spur interjurisdictional competition to attract business revenue by offering desirable regulatory regimes); A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129 (Brian Kahin & Charles Nesson eds., 1997) (detailing the Internet's "resistance to control").

regulation by even a liberal democratic nation-state. They contend that in contrast to "top-down" state regulation, cyberspace rule making epitomizes a "Jeffersonian mode of law-making," a political order based in the primacy of local norms and individual choice.[18]

The first two cyberian claims, regarding the purported efficiency benefits and unregulability of cyberspace "private ordering," have elsewhere been the subject of trenchant—to my mind, withering—critique.[19] My focus will be on the third cyberian claim, that a self-governing cyberspace would more fully realize liberal democratic ideals.

This claim has two parallel components. The first component, which I will call the claim of liberal perfection, views cyberspace norm creation as the paradigm of liberal rule. It contends that cyberspace self-governance more fully embodies the liberal democratic goals of individual liberty, popular sovereignty, and the consent of the governed than does the "top-down" administration of even the most democratic nation-states.[20] Cyberians view territorial representative government as a fundamentally flawed attempt to implement liberal democratic ideals. Representative democracy might be the best we can achieve in "real space," where collective action, information, negotiation, and mobility costs make unmediated forms of governance highly impractical. But, cyberians posit, the global networks of digital communication and data storage that underlie cyberspace create unprecedented possibilities to drastically reduce those costs. They offer a wealth of information, instantaneous and inexpensive mass communication, and a seemingly infinite choice of virtual communities, discussion groups, and rule regimes. As a result, cyberians claim, cyberspace not only constitutes a jurisdiction apart from territorial nation-states; it is also a fundamentally more liberal and democratic one.

The second component, which I will call the claim of community autonomy, focuses not on cyberspace per se, but on group rights within the liberal state. A truly liberal state, it contends, grants considerable autonomy to communities and associations that wish to be self-governing. Accordingly, even if virtual communities and rule regimes do not represent

---

18. Post, *supra* note 14, at 170-71.

19. On the efficiency claim, see Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998); Radin & Wagner, *supra* note 6. On the futility of regulation claim, see LESSIG, *supra* note 12, at 34-42, 49-60; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Joel P. Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 573 (1998) ("anything wrought by the mind of man is capable of regulation by the mind of man"); *see also* 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 LEGAL STUD. 423, 435-36 (1998) (arguing that the Internet can be used as a tool to strengthen rule of law and liberal governance).

20. *See* Post & Johnson, *Civic Virtue*, *supra* note 2, at 46-51; David G. Post, *The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521, 535-42 (1998).

superior forms of political organization—indeed, even if they are autocratic and illiberal—liberal nation-states must give them ample room for self-governance.[21] Cyberspace, cyberians assert, is a self-defining community. State regulation amounts to a "colonial" usurpation of local norms and authority.[22]

The cyberian claims of liberal perfection and community autonomy pose an intriguing challenge to traditional liberal democratic theory. But I believe that challenge ultimately fails. I will argue that an untrammeled cyberspace would prove inimical to the ideals of liberal democracy and indeed that selective state regulation of cyberspace is warranted to protect and promote those ideals. I will also propose that in the absence of regulation by a democratic state, cyberians would be forced to invent a quasi-state institution to legislate and enforce liberal democratic meta-norms governing critical aspects of cyberspace organization and operation. Even if cyberians were successfully to establish such an institution, it would, at best, suffer from much the same democratic deficit that, according to cyberians, characterizes nation-state representative democracy.

With those parameters in mind, Part I of this Article will briefly examine the basic elements of liberal democracy most pertinent to the cyberian claim of liberal perfection. It will be particularly important to unpack the liberal from the democratic component of liberal democracy. Cyberians often conflate the two components. But, at bottom, the liberal perfection claim contends more that cyberspace self-governance represents an extra-democratic vehicle for actualizing liberalism than that it constitutes a purer form of democracy. As cyberians describe it, cyberspace presents opportunities for translating individual preferences into collective decision in ways that, for the most part, resemble more the operation of the market than the polis.

Following this conceptual foundation, Part II will elucidate and critically examine the cyberian claim of liberal perfection. The claim consists of three variants or sub-claims. Each sub-claim presents an alternative

---

21. *See* Johnson & Post, *Law and Borders*, *supra* note 2, at 1393 (calling for a "convergence of the intellectual categories of comity in international relations and the local delegation by a sovereign to self-regulatory groups" to support cyberspace self-governance); *cf.* NICHOLAS NEGROPONTE, BEING DIGITAL 7 (1995) (predicting that in the digital age the "values of a nation-state will give way to those of . . . electronic communities," and that "[w]e will socialize in digital neighborhoods in which physical space will be irrelevant").

22. *See* Gibbons, *supra* note 2, at 503 (referring to federal regulation of cyberspace as "colonialism"); Johnson & Post, *Law and Borders*, *supra* note 2, at 1393 ("If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government."); *cf.* ESTHER DYSON, RELEASE 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE 43, 104-05 (1997) (contending that state regulation would stifle the community spirit needed for cyberspace self-governance); Perritt, *supra* note 2, at 425-32 (proffering criteria for accepting autonomy of cyberspace communities).

vision of cyberspace self-governance, and each overlaps and to some extent contradicts the others.

What I label the "cyberpopulist" claim does focus largely on the democracy side of the liberal democracy equation. It views cyberspace as a mechanism for direct democracy. The Internet, cyberpopulists assert, has the potential to serve as an electronic town hall, an arena where individuals can deliberate and vote on issues of mutual concern. Such online plebicites might transpire on the level of virtual discussion groups, networks, or the entire Internet. In that manner, decision-making power will devolve from self-regarding elected officials and return to the people.

What I refer to as the "cybersyndicalist" claim sees the multifarious virtual communities developed through online discussion groups as the principal sites for the realization of liberal democracy. Through ongoing interaction and discussion, cybersyndicalists maintain, each discussion group generates a unique set of social norms reflecting the values and preferences of its participants. Expanding upon recent literature touting the purported efficiency benefits of the "bottom-up" generation of social norms,[23] cybersyndicalists portray virtual communities as the paradigms of consensual self-governance.

What I call the "cyberanarchist" claim anchors cyberspace self-governance in the spontaneous order arising from freedom of exit, rather than in community norm generation. Cyberanarchists place singular emphasis on each individual's "real freedom of movement" among diverse "rule spaces," rather than on the consensual, discursive formation of social norms by members of a close-knit community.[24] It does not matter whether online discussion groups or even entire networks of such groups are internally autocratic, since individuals can always choose "their own more congenial online homes."[25] Cyberanarchists, then, see cyberspace as a

---

23. *See, e.g.*, ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643 (1996); Richard A. Epstein, *Enforcing Norms: When the Law Gets in the* Way, 7 RESPONSIVE COMMUNITY, Fall 1997, at 4; Peter H. Huang & Ho-Mou Wu, *More Order Without More Law: A Theory of Social Norms and Organizational Cultures*, 10 J.L. ECON. & ORG. 390 (1994); Avery Katz, *Taking Private Ordering Seriously*, 144 U. PA. L. REV. 1745 (1996); Jonathan R. Macey, *Public and Private Ordering and the Production of Legitimate and Illegitimate Legal Rules*, 82 CORNELL L. REV. 1123 (1997); Richard H. McAdams, *Accounting for Norms*, 1997 WIS. L. REV. 625; Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997); Randal C. Picker, *Simple Games in a Complex World: A Generative Approach to the Adoption of Norms*, 64 U. CHI. L. REV. 1225 (1997); Cooter, *supra* note 12 (reviewing ELLICKSON, *supra*). For a more critical assessment, see David Charny, *Illusions of a Spontaneous Order: "Norms" in Contractual Relationships*, 144 U. PA. L. REV. 1841 (1996); Lawrence Lessig, *Social Meaning and Social Norms*, 144 U. PA. L. REV. 2181 (1996); Eric A. Posner, *Law, Economics, and Inefficient Norms*, 144 U. PA. L. REV. 1697 (1996); Lewis A. Kornhauser, *Are There Cracks in the Foundations of Spontaneous Order?*, 67 N.Y.U. L. REV. 647, 659-668 (1992) (reviewing ELLICKSON, *supra*).

24. *See* Post & Johnson, *Civic Virtue*, *supra* note 2, at 49-50.

25. *Id*. at 50.

market of alternative rule regimes. It is the ease of exit and the abundance of alternatives—in essence consumer choice in conditions approaching perfect competition—that bring to fruition the liberal ideals of liberty and consent.

Part II also presents my critique of the cyberpopulist, cybersyndicalist, and cyberanarchist claims. I will put forth four basic propositions. First, the cyberians give insufficient weight to representative democracy's support for liberal ideals, incorrectly viewing representative democracy as a mere second-best alternative to nonmediated systems for effecting individual choice. Second, the cyberians greatly exaggerate the propensity of online communication and communicative networks to support their visions of self-governance. As cyberians correctly assert, cyberspace is characterized by considerable freedom of movement. But that freedom of movement significantly undermines the stability required for community generation of social norms, and thus cuts against the cyberpopulist and cybersyndicalist claims. Indeed, given the unraveling of bottom-up online communities and the growing prevalence of autocratic determination of local online norms, the cyberanarchists present the only potentially viable claim for cyberspace self-governance. At the same time, however, online freedom of movement—both exiting from existing rule spaces and finding or establishing new ones—may be significantly more costly than cyberanarchists assume. As a result, liberal ideals can be realized only through the enforcement of meta-norms that protect those dissenters for whom exit is a less than tenable alternative.

Third, the cyberanarchist claim of liberal "government" by individual decision making is vulnerable to many of the standard criticisms of the Hayekian view of the market as fundamentally superior to democratic institutions.[26] In cyberspace, no less than in real space, consumer decisions may represent an impoverished account of individuals' true preferences for many types of social goods. By the same token, market failure is no less endemic to online decision making than to its offline counterpart. In particular, the cyberanarchist vision would countenance some of the very externalities that liberal democracy seeks to minimize, including status discrimination and the suppression of minority viewpoints.

---

26. Hayek posited (and here I am necessarily oversimplifying) that a "spontaneous order," the result of countless interactions in a market tamed only by rules of law arising organically from those interactions and designed to allow each individual to pursue his own ends in accordance with his subjective preferences, represents a far better guarantee of individual liberty than does collective, democratic decision making. *See* 1 F.A. HAYEK, LEGISLATION AND LIBERTY: RULES AND ORDER 39-43 (1973) (describing concepts of spontaneous order and rule of law); F.A. HAYEK, THE ROAD TO SERFDOM 88-100 (1944) (contending that "political freedom is meaningless without economic freedom" and economic freedom can be sustained only through competition and individual choice without government intervention).

Finally, cyberians give insufficient weight to the distributive function of liberal government. Liberal ideals can be realized only if the incidents of citizenship are distributed among all citizens. Yet opportunities to communicate, process information, and even gain access to cyberspace are vastly unequal. The cyberian vision lacks a vehicle to provide such citizenship resources to those who currently lack them. Without state intervention, therefore, cyberspace self-governance will, at best, resemble the Athenian democracy of the privileged few, not participatory liberalism.

Part III considers the cyberian claim for community self-governance within the liberal state. Political liberalism, I readily concede, does contain room for community and associative autonomy. But liberalism rightly imposes limits on that autonomy, and there is nothing about the nature of virtual communities to justify granting them greater leeway than their territorial counterparts. In fact, there may well be reason to impose greater restrictions on virtual communities.

Part IV discusses a number of areas in which a democratic state might regulate cyberspace activity or provide resources for online actors in order to further liberal ideals. These include countering status and viewpoint discrimination, protecting Internet user privacy, and promoting a broad distribution of citizenship resources. In line with my discussion in Part III, my conclusion is not that state intervention is always appropriate. Rather, in each instance the benefits of state intervention must be balanced against possible harms to speech and association interests that themselves have inherent value for liberal democracy.

Part V raises and rejects the possibility that cyberians might set up their own representative body to create and enforce meta-rules designed to promote liberal democratic ideals. It concludes that democratic institutions of territorial nation-states are far more likely effectively to protect liberal rights and to further the liberal ideal of government by consent of the governed.

Part VI briefly address an additional cyberian political claim. That claim invokes liberal and liberal democratic principles on an international level, augmenting cyberian claims regarding the failings of nation-state territorial democracy. Cyberians argue that a nation-state's imposition of jurisdiction over persons who reside outside the nation-state and who therefore lack a direct say in determining that nation-state's leadership or laws runs contrary to the fundamental liberal democratic principle of government by consent of the governed.[27] They also suggest that the democratic deficit plaguing domestic governments is exacerbated in the

27. *See generally* Johnson & Post, *Law and Borders*, *supra* note 2; Post, *supra* note 20.

international arena, where international agencies are even further removed from those they seek to regulate.[28]

I
LIBERAL DEMOCRACY

Cyberians maintain that cyberspace self-governance represents a fuller expression of liberal democratic principles than do the constitutional, representative democracies of territorial nation-states. To assess that claim, it will be helpful to explicate briefly the principles underlying liberal democracy. That, of course, is no simple task. As Don Herzog has aptly remarked, "liberalism is a tradition, not a single view, and like any other tradition it is best conceived of as a family of disagreements."[29] What follows, then, is a brief restatement of those elements of liberal democracy most pertinent to the cyberian claim. In particular, I will adumbrate the basic fault lines in liberal democratic theory to locate the cyberian claim within its theoretic context.

Liberal democracy is a political system with representative governments elected by popular majority, the rule of law enshrined to protect individuals and minorities, and a significant sector of economic, associational, and communicative activity that is largely autonomous from government control.[30] It rests upon the principles of individual liberty, civic equality, popular sovereignty, and government by the consent of the governed. Liberal democracy's institutional characteristics and principles are mutually dependent. Popular sovereignty exercised through the periodic election of representatives, together with a representative government constrained by the rule of law, a separation of powers, and constitutional rights, helps to secure individual liberty.[31] Concomitantly, individual liberties, civic equality, and limited government support democratic

---

28. *See* 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, *supra* note 6, at 62, 71-73 (arguing that the Internet poses problems of democratic deficit and regulatory capture).

29. Don Herzog, *Some Questions for Republicans*, 14 POL. THEORY 473, 480 (1986).

30. *See* Michael W. Doyle, *Kant, Liberal Legacies, and Foreign Affairs*, 12 PHIL. & PUB. AFF. 205, 206-09 (1986) (defining liberal democracies as having four major characteristics: (1) protection of private property; (2) a market economy; (3) equality under the law and respect for human rights; and (4) a representative government deriving its authority from the consent of individuals); Steven R. Ratner, *New Democracies, Old Atrocities: An Inquiry in International Law*, 87 GEO. L.J. 707, 707 (1999) (defining liberal or constitutional democracy as "a political system with governments elected by popular majority, and with the rule of law enshrined to protect those not in the majority").

31. Indeed, the existence of democratic institutions may be seen as an instance of individual liberty. International law has increasingly recognized the right to political participation in democratic elections as an independent human right, not merely as good policy in support of individual rights against an overreaching state. *See, e.g.*, European Parliament Resolution 78/95, P60, 1995 O.J. (C 126) 126 ("[T]he right to political participation in the political process is a fundamental and universal human right, as is the establishment of representative democracy.").

governance. They undergird a vibrant civil society, a prerequisite for the effective exercise of popular sovereignty.

Yet there is a certain—some would say fundamental—tension between liberalism and democracy. While democracy aims to actualize the popular will, liberalism gives primacy to individual liberty. Or more precisely, while democracy promotes *public liberty*, the right to belong to a self-governing community, liberalism champions *personal liberty*, in the "negative" sense of the absence of interference with individual choice.[32] A democratic order demands individual involvement in the political process and adherence to collective decision. A liberal order enables individuals to pursue their private ends in the manner of their own choosing.

I do not mean to make too much of this dichotomy. To be certain, personal (negative) liberty and limited government are central to liberal thought. But modern liberalism, stretching back at least to the American Revolution, also bears the imprint of the democracy component of liberal democracy.[33] In particular, most liberals would place civic equality, in the sense of both equal treatment under the law and equal right to participate in political life, squarely within the pantheon of liberal rights.[34] Numerous liberal theorists, including John Rawls, Stephen Holmes, and John Stuart Mill in his later work, also insist that a liberal government must secure the necessary social and material conditions for individuals' realization of liberal rights, not merely to accord those rights formal recognition.[35]

---

32. *See* PHILIP PETTIT, REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT 18 (1997). Pettit juxtaposes "negative liberty" not only against "public liberty" (also termed "ancient" or "positive" liberty), but also against "republican liberty," meaning freedom from domination, another's privilege to interfere arbitrarily with one's individual choice. *Id*. at 18-31. In his classic discussion of negative liberty, Isaiah Berlin contrasts it with "positive liberty," an individual's right of self-mastery and political participation, which may or may not be coterminous with others' understanding of "public liberty." *See generally* ISAIAH BERLIN, TWO CONCEPTS OF LIBERTY (1958). As Stephen Holmes points out, the borders between these various types of individual liberty are far more permeable than Berlin and others have suggested. STEPHEN HOLMES, PASSIONS AND CONSTRAINT: ON THE THEORY OF LIBERAL DEMOCRACY 28-30 (1995). Indeed, all play some part in traditional liberal theory. *See* Joshua Cohen, *Democracy and Liberty*, *in* DELIBERATIVE DEMOCRACY 185 (John Elster ed., 1998) (maintaining that negative liberties may be a necessary condition for democratic governance in a pluralist society).

33. For a cogent refutation of the notion that liberalism is inherently hostile to democracy, see HOLMES, *supra* note 32, at 27-36.

34. *See* DAVID HELD, MODELS OF DEMOCRACY 88 (2d ed. 1996) (noting that modern liberal democracy posits that "[t]he protection of liberty requires a form of political equality among all mature individuals: a formally equal capacity to protect their interests from the arbitrary acts of either the state or fellow citizens"); *see also* JOHN RAWLS, POLITICAL LIBERALISM 289-371 (1993) (including "political liberties" among basic liberal liberties).

35. *See* HOLMES, *supra* note 32, at 236-66 (arguing that the redistributionist welfare state fully comports with traditional liberal theory); 4 JOHN STUART MILL, PRINCIPLES OF POLITICAL ECONOMY 775-941 (J.M. Robson ed., 1965) (1848) (decrying capitalism's stultifying impact on wage earner dignity and independence of thought and advocating syndicalist system of worker ownership and election of management); JOHN RAWLS, A THEORY OF JUSTICE 225-27 (1971) (noting that political liberties and democratic institutions "lose much of their value whenever those who have greater private means are permitted to use their advantages to control the course of public debate"); JOSEPH RAZ, THE

Nevertheless, expanding upon Locke and much of Mill's earlier writing, neoliberals, including F.A. Hayek, Robert Nozick, and James Buchanan, have insisted upon a radical separation between liberalism and democracy.[36] In traditional Lockean liberalism, individual liberties conceptually precede the state (and, in Locke's metaphoric account, they chronologically precede the state as well). Individuals decide, or rational individuals would decide, to establish a state to serve their private ends. The state thus arises from, and its legitimacy depends upon, the express or tacit consent of individuals. The state, in turn, may rightfully exercise its authority only in accordance with the terms of that "social contract."

For traditional liberals and liberal democrats, the "social contract" yields two basic understandings of the state. The first is limited government. Since individuals consent to a state to serve their private ends, the social contract limits government authority to securing individuals' rights, persons, and property (although modern liberals differ significantly on the extent to which those ends demand state intervention in civil society and the market). Second, the relation between a nation's citizens and government is one of trustor and trustee.[37] Government must serve and take direction from the people (although in liberal democracies the people's will finds expression in a complex, highly stylized arrangement of broad constitutional directives and the periodic election of representatives).

Neoliberals, in contrast, define the relation between citizen and state more in terms of the metaphoric prepolitical state of nature than the social contract's prospective application to civil government. In their view, collective choice is nothing but the aggregation of individual decisions, and the creation of a political community or government is at best a necessary evil, the burden individuals must bear to secure their private ends. Law and a minimal state may sometimes be necessary to protect individuals from others' harmful acts (however defined), facilitate voluntary exchange, and arrange for or stimulate the production of public goods. But except for this "minimal collectivization,"[38] the only legitimate allocation of resources is that "contingently negotiated by the unhindered activities of individuals in

---

MORALITY OF FREEDOM 425-29 (1986) (arguing that the liberal state must promote individual autonomy by guaranteeing that certain goods are made available to its citizens).

36. *See* HELD, *supra* note 34, at 253-60 (describing neoliberal thought).

37. As Locke put it, legislative power is "but a delegated Power from the People" and "the Legislative being only a Fiduciary Power to act for certain ends, there remains still *in the People a Supreme Power* to remove or *alter the Legislative*, when they find the *Legislative* act contrary to the trust reposed in them." JOHN LOCKE, TWO TREATISES OF GOVERNMENT, II, § 149. *See also* HOLMES, *supra* note 32, at 181 (discussing Mill's support of a trustee as opposed to a delegate theory of representation). For further discussion of this liberal basis for representative democracy, see HOLMES, *supra* note 32, at 32-34; PETTIT, *supra* note 32, at 9.

38. JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT: LOGICAL FOUNDATIONS OF CONSTITUTIONAL DEMOCRACY 46 (1962) (referring to human and property rights as "minimal collectivization").

competitive exchanges with one another."[39] As Hayek and Nozick emphasize, any collective decision to which an individual has not consented is a restriction of his liberty since it denies him the possibility of acting in a manner he otherwise could have acted and of judging his own ends.[40] Or, to cast that proposition in Buchanan's public choice terms, rational individuals will choose democratic over individual decision making only when transaction costs prevent the reaching of private, voluntary agreements.[41] In sum, by its very nature constitutional representative democracy offers inadequate protection for liberal rights. Majoritarian rule is a second-best alternative, to be employed only when market failure obstructs private bargains.

Where do the cyberians fit in this colloquy? Cyberians often use the terminology of liberal democracy. They argue, for example, that rule of a territorial representative democracy over cyberspace belies the liberal democratic principle of "government by the consent of the governed."[42] But for the most part, the cyberian project is a neoliberal one.[43] They view liberal democracy as a second-best alternative to private agreement. Moreover, they see in cyberspace the unprecedented possibility of dramatically reducing individuals' decision-making and transaction costs. As they describe it, cyberspace represents the fruition of the neoliberal dream, the possibility of a society ruled by myriad private, voluntary agreements. In cyberspace the state, even a liberal democratic state, is an unnecessary and deleterious appendage.

II
THE CYBERIAN CLAIM OF LIBERAL PERFECTION

Cyberspace offers numerous arenas for potential self-governance.[44] At the most local level, these include a multitude of discussion groups and sites for ongoing virtual interaction. Virtual fora such as email listservs, Usenet newsgroups, chat rooms, and multi-user games are built upon varied rule structures.[45] Some local rules reflect considerable participant input, although group moderators autocractically determine most local rules. At

---

39. HELD, *supra* note 34, at 255 (paraphrasing Robert Nozick). *See* ROBERT NOZICK, ANARCHY, STATE AND UTOPIA 149-74 (1974).

40. *See generally* HAYEK, *supra* note 26; NOZICK, *supra* note 39.

41. *See* BUCHANAN & TULLOCK, *supra* note 38, at 62.

42. *E.g.*, Barlow, *supra* note 1; DYSON, *supra* note 22, at 1.

43. *See, e.g.*, Post, *supra* note 20, at 538 (viewing the social contract, in Nozick's terms, as an agreement among prepolitical individuals, not between a sovereign people and their governing institutions).

44. Such self-governance, of course, transpires only within the framework of state-created subsidy and law. *See* sources cited *supra* note 6.

45. For an illuminating discussion of such rules, see Siegal, *supra* note 7. *See also* Mnookin, *supra* note 10. Multi-user games include MUDs (multi-user dimensions) and MOOs (object-oriented MUDs). *See* sources cited *supra* note 10.

what might be termed the "regional level," many virtual fora are organized within networks such as the WELL,[46] the Usenet, and the multiple discussion groups sponsored by America Online, CompuServe, and other Internet service providers.[47] Virtual networks also comprise groupings of sites, such as the World Wide Web, devoted more to relaying information than to participant interaction. Like virtual fora, virtual networks constitute—and are constituted by—formal and informal rules that reflect varying degrees of participant input. Finally, cyberspace might be seen as a single, global unit of governance. In this view, cyberspace as a whole is "ruled" by technical protocols governing internetwork communication and by the numerous individual choices among alternative fora and networks, choices that favor certain matrices of local and regional rule regimes and disfavor others.

But in parallel with such nascent self-governance, countless cyberspace transactions and local norms parallel the sort of offline activities that have given rise to state regulation. Some of these concern the sale of expressive content or services, such as web sites that sell pornography or Internet gambling. Others involve the unauthorized use of intellectual property, whether copyrighted expression or trademark. Still others touch upon what are often seen as fundamental political or autonomy interests. These include the exclusion of certain viewpoints from online discussion groups or entire networks; similar discrimination based on the would-be speaker's race, gender, or other status; the collection of personal information gleaned from Internet users' web site visits; and unsolicited email advertising.

Cyberians argue that the state, as a general rule, should refrain from regulating such behavior, even when regulation of parallel offline activity might be warranted. A political fount of this claim is that cyberspace offers unique possibilities for private ordering that more fully embody the democratic liberal ideals of individual liberty and government by the consent of the governed than does the representative democracy of territorial nation-states. Territorial representative government, cyberians assert, is a fundamentally flawed second-best alternative, necessitated by the collective action, information, transaction, and mobility costs that make more democratic structures impractical. But within cyberspace such costs are drastically reduced. Accordingly, those engaging in online communication should receive considerable leeway to govern themselves, or at least to govern their online activity, from the "bottom-up" as it were. In this view,

46. The WELL is the acronym for the Whole Earth 'Lectronic Link, a network of moderated discussion groups based in San Francisco. For an in-depth study of this pioneer network of virtual communities, see HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993).

47. *See* Jonathan Zittrain, *The Rise and Fall of Sysopdom*, 10 HARV. J.L. & TECH. 495, 502-03 (1997) (discussing AOL and CompuServe fora).

cyberspace self-governance centers political decision making in the individuals whose lives those decisions affect, rather than in representatives who can only approximate their constituents' preferences and choices.

The cyberian claim of political superiority presents three overlapping, but also somewhat contradictory, approaches to cyberspace self-governance. These include cyberpopulism, which views the Internet as a vehicle for electronic direct democracy; cybersyndicalism, which focuses on the generation of social norms by virtual communities as an alternative to state-centered law making; and cyberanarchism, which sees cyberspace as the epitome of Hayekian spontaneous order, a regime "governed" by the constant, variable interaction of a multitude of individual decisions rather than by norms enunciated and enforced by an overarching state or quasi-state. Each approach claims to achieve the radical disintermediation that cyberians insist is necessary to fulfill liberal ideals. In this Part, I will further explicate the three approaches. I will also call into question their basic assumptions.

A. Cyberpopulism

1. The Cyberpopulist Claim

Cyberpopulists see in cyberspace the possibility for direct voting and citizen deliberation, a virtual equivalent of the much idealized New England town meeting. Cyberpopulism differs in important ways from the rest of the cyberian claim of liberal perfection. In both aspiration and theoretical grounding, it is considerably more intertwined with offline liberal democratic institutions than are cybersyndicalism and cyberanarchy. First, cyberpopulists see Internet voting not only as a basis for cyberspace governance but also as a direct challenge to territorial representative democracy.[48] For cyberpopulists, citizen voting on a continuous stream of Internet

48. Much cyberpopulism contemplates the use of the Internet for citizen initiatives, deliberation, and voting on real world issues, as opposed to those involving cyberspace interaction per se. *See, e.g.*, GRAEME BROWNING, ELECTRONIC DEMOCRACY; USING THE INTERNET TO INFLUENCE AMERICAN POLITICS 84-88 (1996) (advocating use of Internet in offline politics); Clive Walker & Yaman Akdeniz, *Virtual Democracy*, PUB. L., Autumn 1998, at 489 (discussing possibilities for use of Internet for citizen plebiscites). In fact, the vast majority of cyberspace rule making takes place by rough consensus, fiat, or contract, not formal vote. But rule by vote has also found expression within cyberspace administration. Most notably, perhaps, the establishment of new Usenet newsgroups (other than those in the "alt." or alternative hierarchy) requires a super-majority vote of those Internet users casting votes. *See Guidelines for Usenet Group Creation, Newsgroups: The Results* (last modified Sept. 24, 1997) <http://news.acns.nwu.edu/usnt_end.html> (providing that a new newsgroup may be created "if 100 more valid YES/create votes are received than NO/don't create AND at least 2/3 of the total number of valid votes received are in favor of creation"). Various newsgroups, chat rooms, and listservs have also sometimes reached crucial decisions regarding internal policy through deliberation and vote. *See* Siegal, *supra* note 7, at 203-06 (discussing ballot procedure concerning disputes within a LambdaMOO group). Similar methods of vote or agreement have been suggested as a basis for cyberspace-wide rule making. *See* David R. Johnson, *Lawmaking and Law Enforcement in Cyberspace*, (visited Apr. 27, 1994) <http:www.eff.org/pub/Legal/cyberlaw_johnson.article> (suggesting

initiatives—what Andrew Shapiro disparagingly labels "push-button politics"[49]—can supplement or even replace parole boards, administrative agencies, and legislatures.[50]

In addition, unlike its cybersyndicalist and cyberanarchist counterparts, cyberpopulism begins with the democracy side of the liberal democracy equation. It initially proffers direct majoritarian democracy as the solution to representative democracy's purported failure to support liberal democratic principles.[51] For cyberpopulists and real world populists alike, the plebiscite represents a purer form of democracy than legislation enacted by bodies of periodically elected representatives. In the cyberpopulist vision, the liberal ideal of government by the consent of the governed is most fully realized when the governed govern themselves. The people are truly sovereign only when they deliberate on the issues that affect them and determine the outcome by consensus or majority vote.

In this view, representative government suffers from two basic deficiencies. The first is agency costs.[52] By accident, inefficiency, or design, representatives do not always reflect the views of their constituents. So-called representatives, populists contend, too readily become entrenched political elites, with interests inconsistent with those who have elected them.[53] Moreover, even if elected officials could put self-interest aside, their best efforts to represent their constituents would still be beset by difficulties in determining what voters want and in accurately translating popular will into legislation. As a result of these information and communication costs, populists contend, mediated government will systematically garble the voice of the people, yielding a significant democratic deficit.

---

cyberspace-wide voting or agreement). For a discussion of voting within the Internet Corporation for Assigned Names and Numbers, established to assume responsibility for managing the Internet domain name system, see *infra* notes 375-76 and accompanying text.

49. ANDREW L. SHAPIRO, THE CONTROL REVOLUTION 150 (1999).

50. *See id*. at 150-54; *see also* Ken Dolbeare & Janette Hubbell, *Saving the American System: A Four-Part Program Including New Forms of Direct Democracy* (visited Jan. 4, 2000) <http://www.auburn.edu/tann/cp/features/sos.htm> (proposing system of regular plebiscites, including email voting, on "all major issues").

51. *See infra* text accompanying notes 97-104, 109.

52. Agency costs are all costs incurred by a principal in relying upon another person to accomplish the principal's tasks. They include the principal's monitoring expenses, the agent's bonding expenses, and the residual losses from agent shirking. *See* Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 308 (1976). For a discussion of agency costs in the context of constitutional politics, see A.C. Pritchard & Todd J. Zywicki, *Finding the Constitution: An Economic Analysis of Tradition's Role in Constitutional Interpretation*, 77 N.C. L. REV. 409, 448-50 (1998).

53. Of course, traditional liberals were also keenly aware of officials' propensity to follow their personal interests at the expense of the community at large. Liberal constitutional democracy strives to check that propensity (populists would say unsuccessfully) through institutions such as divided authority, a free press, and frequent elections. *See* HOLMES, *supra* note 32, at 5.

The second deficiency that populists claim afflicts representative government is even more fundamental. It concerns the conceptual tension between popular sovereignty and rule by elected officials. If the people are truly sovereign, then elected officials must serve as agents of the people. But in representative democracy, elected officials, not the people, have supreme law-making power. For populists, elected officials cannot possess that power and still meaningfully be considered as mere agents of the people.[54] By both definition and consequence, therefore, representative government belies popular sovereignty.

Given its purported deficiencies, representative government is, for populists, at best a second-rate democracy. Yet populists have traditionally recognized that rule by elected officials is a necessary evil in any territory larger than a very small town.[55] In municipalities, states, and nation-states, citizens can neither meet face-to-face nor keep abreast of the many complex issues facing the polity. In real space, therefore, the populist impulse has been limited to seeking to diminish agency costs, through measures such as term limits, and introducing inklings of direct democracy, including single-issue popular initiatives, into what essentially remains a representative government.

For cyberpopulists, on the other hand, the Internet presents new possibilities for a greatly expanded role for direct democracy, both within cyberspace and without. In this vision, cyberspace is free of the geographical and informational obstacles that prevent rule by plebiscite in real space.[56] The Internet enables deliberation among large numbers of geographically dispersed users. Such deliberation is akin to a virtual town hall meeting, but better. In cyberspace, cyberpopulists argue, "everyone has a chance to speak, no one is shouted down, and people have time to develop and explain their ideas."[57] The Internet also makes possible the exchange of information and opinion at a fraction of the cost of real space media. Cyberpopulists assert that as a result, Internet users are able to gain a far more informed understanding of a far greater number of issues than are their poor cousins in real space.

---

54. *See* Post, *supra* note 20, at 527.

55. *See, e.g.*, CAROLE PATEMAN, PARTICIPATION AND DEMOCRATIC THEORY 109 (1970) (conceding that despite the desirability of local participatory democracy, "[i]n an electorate of, say, thirty-five millions the role of the individual must consist almost entirely of choosing representatives").

56. *See, e.g.*, Perritt, *supra* note 2, at 420; *see also* Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. (forthcoming 1999) (suggesting that cyberspace enables direct communication of individual preferences and cost-effective feedback on those preferences, thus obviating the need for intermediaries who would reflect the aggregate will of their constituents).

57. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1669 (1995) (citing Mike Godwin, *The First on a New Frontier*, QUILL, Sept. 1991, at 18, 19).

2. Critique of the Cyberpopulist Claim

The cyberpopulist claim is vulnerable on three broad grounds. The first involves the populist characterization of liberal democratic ideals. Contrary to the cyberpopulist claim, traditional conceptions of liberal democracy do not equate the consent of the governed with government that effectuates the popular will. The second ground goes to the question of outcome. Even assuming that popular will is the correct measure of liberal democratic rule, it is by no means clear that the plebiscite reflects the popular will more faithfully than does representative government. The third concerns the problem of majority tyranny. Cyberpopulism fails to provide a workable mechanism for protecting the liberties of minorities and dissenters. And in attempting to remedy this failing, cyberpopulism moves towards an equally unworkable neoliberal regime of unanimous consent and dissenter exit.

a. The Populist Mischaracterization

Cyberpopulists incorrectly equate the liberal democratic principle of government by consent of the governed with government by popular will. The traditional liberal conception of popular sovereignty is of self-rule reflected in and filtered through "an empire of laws, not of men."[58] In that view, both individual liberty and collective self-rule require constraints on the ability of temporal majorities to effect their will.[59] They require a system of balanced government, like that embodied in the constitutional structure of the United States, replete with counter-majoritarian measures designed to curb the unhindered, arbitrary exercise of power.[60]

By the same token, "government by consent of the governed" does not mean that "the people," whether individually or collectively, must actively consent to each government decision. Even the contractarian strand within the liberal tradition views consent in decidedly formal terms, far removed from actual consent.[61] For Locke, Hobbes, and Rawls, the

---

58. JAMES HARRINGTON, THE COMMONWEALTH OF OCEANA AND A SYSTEM OF POLITICS 81 (J.G.A. Pocock ed. 1992). Harrington is generally associated with republican thinking, to the extent it can be meaningfully separated from traditional liberalism. *See also* PETTIT, *supra* note 32, at 173 (describing belief in an empire of law, shared by liberal and republican theorists alike).

59. *See* Samuel Issacharoff & Richard H. Pildes, *Politics as Markets: Partisan Lockups of the Democratic Process*, 50 STAN. L. REV. 643, 712-13 (1998).

60. *See* Marci A. Hamilton, *The People: The Least Accountable Branch*, 4 U. CHI. L. SCH. ROUNDTABLE 1, 3-10 (1997) (describing the Framers' view). Indeed, the original Constitution reflected a highly elitist conception of democratic politics, in which representatives were seen to stand above their constituents, and both senators and presidents were elected by other public officials, not popular vote. *See* Issacharoff & Pildes, *supra* note 59, at 713-15.

61. As David Post notes, "There has always been a strong fictional element to using this notion of a social contract as a rationale for a sovereign's legitimacy." David G. Post, *New World War: Cancelbunny and Lazarus Battle It Out on the Frontier of Cyberspace—and Suggest the Limits of Social Contracts*, REASON, Apr. 1996, at 30, 33.

consent of the governed denotes a metaphoric agreement to the establishment of civil government, a logical premise for the move from the proverbial state of nature and a heuristic for elucidating the type of government upon which all might be deemed to agree.[62] Its continuing import in the age of civil government relates, at most, to the broad constitutional legitimacy of representative government.[63] It is not meant to be a recipe for daily governmental decision making.[64]

Nor does "government by the consent of the governed" contemplate that elected officials act as mere agents for the majority that elected them. Popular sovereignty, rather, lies more in the permanent possibility, enjoyed by the people individually and collectively, of evaluating and contesting what the government decides.[65] "Consent" is presumed by a legislative process in which public decision making must survive public scrutiny. Legislation must be defensible by "public reason," by justifications that proponents may "reasonably think that other citizens might also reasonably accept."[66] Citizens, in turn, must have access to effective fora for debate, including the periodic opportunity to "throw the rascals out" in the event that elected officials stray too far from popular sentiment.[67] But, again, this does not mean that citizens must dictate every government decision. Rather, as William Riker has provocatively, but not implausibly, asserted: "Liberal democracy is simply the veto by which it is sometimes possible to restrain official tyranny."[68]

b. Popular Will

In distinguishing liberalism from populism, I do not mean to overstate the case: There is a real tension between popular sovereignty and representative government within the liberal tradition, and many readings of

---

62. *See* HELD, *supra* note 34, at 81; Murray Forsyth, *Hobbes's Contractarianism: A Comparative Analysis*, *in* THE SOCIAL CONTRACT FROM HOBBES TO RAWLS 35 (David Boucher & Paul Kelly eds., 1994) [hereinafter SOCIAL CONTRACT]; *see also* Jeremy Waldron, *John Locke: Social Contract Versus Political Anthropology*, in SOCIAL CONTRACT 51, *supra* (noting that "[m]odern contractarians accept without question that most of the social and political institutions which interest them are not in fact the upshot of any contract or agreement among those whose lives they affect" and arguing that Locke intended, at most, to make the historical claim for tacit consent to civil government).

63. *See* HELD, *supra* note 34, at 81.

64. For an illuminating discussion of the highly stylized and hypothetical nature of "consent" in the context of nation-states' territorial sovereignty, see Lea Brilmayer, *Consent, Contract, and Territory*, 74 MINN. L. REV. 1 (1989).

65. *See* PETTIT, *supra* note 32, at 183-85.

66. John Rawls, *The Idea of Public Reason Revisited*, 64 U. CHI. L. REV. 765, 770-71 (1997).

67. PETTIT, *supra* note 32, at 183-85.

68. WILLIAM H. RIKER, LIBERALISM AGAINST POPULISM: A CONFRONTATION BETWEEN THE THEORY OF DEMOCRACY AND THE THEORY OF SOCIAL CHOICE 244 (1982); *see also* JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY 284-85 (1942) (1976) (asserting that democracy does mean actual rule by the people, but "only that the people have the opportunity of accepting or refusing the men who are to rule them").

liberal democracy do insist on a place for popular will far beyond a simple veto.[69] Moreover, cyberpopulists need not cling to traditional limitations of liberal democracy. They might, and sometimes do, claim that those limitations reflect technological, not ideological, constraints.[70] In this view, traditional liberalism has presented a metaphoric account of the "consent of the governed" only because predigital technology did not make possible a concrete realization of that ideal. In the age of global, low-cost digital communication, however, there is no longer any reason to divorce popular sovereignty from the direct, daily effectuation of the people's will. If Locke were alive today, this argument runs, he would be a cyberpopulist.

But the cyberpopulist claim fails even to the extent that effectuating the popular will is seen as a genuine and desirable liberal goal. The reason for that failure is two-fold. First, cyberpopulists overestimate the extent to which the plebiscite, whether territorial or virtual, can truly reflect the voice of the people. Second, they ignore significant democracy-enhancing benefits of representative government.

i. Plebiscites Inadequately Reflect Popular Will

Popular referenda and initiatives have been the subject of extensive scholarly criticism.[71] In practice the plebiscite falls far short of the populist ideal. Uneven voter turnout, ambiguous or misleading drafting of ballot issues, the influence of moneyed special interests, voter ignorance of the issues, and other factors regularly obscure popular input.[72]

More fundamentally, and perhaps more controversially, the populist romance with the plebiscite wrongly equates popular will with an

---

69. At the very least, liberal constitutionalist institutions such as frequent elections, divided government, and free speech are designed in large part to enhance the strength and effectiveness of the popular veto. *See* HOLMES, *supra* note 32, at 271 (contending that the theory behind divided government is "that public officials will act more consistently in the interest of the public if they believe they are being scrutinized by rival politicians who, in turn, have clear incentives to alert otherwise distracted voters to gross public malfeasance and ineptitude"); Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RESEARCH J. 523, 527 (identifying the centrality of the "checking value" of the First Amendment, defined as "the value that free speech, a free press, and free assembly can serve in checking the abuse of power by public officials").

70. *Cf.* Johnson & Post, *Civic Virtue*, *supra* note 2, at 26-29, 46-51 (contending that in cyberspace "voting with one's modem," meaning consumer choice among rule regimes, can and will replace geographically defined representative democracy).

71. *See, e.g.*, Derrick A. Bell, Jr., *The Referendum: Democracy's Barrier to Racial Equality*, 54 WASH. L. REV. 1 (1978); Sherman J. Clark, *A Populist Critique of Direct Democracy*, 112 HARV. L. REV. 434 (1998); Julian N. Eule, *Judicial Review of Direct Democracy*, 99 YALE L.J. 1503 (1990); Hans A. Linde, *Who is Responsible for Republican Government?*, 65 U. COLO. L. REV. 709, 721-22 (1994); Daniel H. Lowenstein, *Campaign Spending and Ballot Propositions: Recent Experience, Public Choice Theory and the First Amendment*, 29 U.C.L.A. L. REV. 505 (1982).

72. *See* Eule, *supra* note 71; Linde, *supra* note 71; *see also* Elizabeth Garrett, *Money, Agenda Setting, and Direct Democracy*, 77 TEX. L. REV. 1845 (1999) (arguing that wealthy individuals and groups have a disproportionate ability to place initiatives on the ballot and suggesting reforms to even the playing field).

aggregation of existing preferences. A contrary, arguably more plausible view sees popular will as endogenous to the political process. "What the people want" is determinable only through a deliberative process, such as that in a "face-to-face, press-covered legislative assembly," in which positions are openly and critically tested by public reason.[73] In this view, it is the "considered will of the people," rather than "transient popular preference,"[74] that is the proper standard for democratic fidelity—and, arguably, representative government better meets this standard than rule by plebiscite.[75]

Cyberspace might provide greater possibilities for bottom-up deliberation than do the obscenely expensive spot-advertising media campaigns increasingly associated with territorial initiatives.[76] But especially as elaborate and costly content production gain an increasing hold on the Internet,[77] cyberplebiscites are likely to be afflicted with the same flaws as their territorial counterparts. Already, commentators have labeled much touted electronic town meetings as "electronic town manipulation," given the distorted nature of information presented and partial framing of ballot

---

73. Frank I. Michelman, *"Protecting the People from Themselves," or How Direct Can Democracy Be?*, 45 U.C.L.A. L. REV. 1717, 1723 (1998); *see also* CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH 244 (1993) (arguing that the "requirement of justification in public-regarding terms . . . might well contribute to public-regarding outcomes" and "might even bring about a transformation in preferences and values, simply by making venal or self-regarding justifications seem off-limits").

74. Clark, *supra* note 71, at 440 (describing the argument that democracy should follow the will of the people).

75. Of course, as plebiscite supporters and others aptly note, most of the time representative government actually falls far short of the deliberative ideal. *See* Lynn A. Baker, *Direct Democracy and Discrimination: A Public Choice Perspective*, 67 CHI.-KENT L. REV. 707 (1991); Clayton P. Gillette, *Is Direct Democracy Anti-Democratic?*, 34 WILLAMETTE L. REV. 609, 631 (1998). Legislators often have little idea of the content of the legislation on which they vote. *See* Baker, *supra*, at 745-47. And the debate that transpires in legislative chambers often consists largely of canned speeches designed to give voters what they want to hear, not reasoned deliberation. *See* Gillette, *supra*, at 631. Nonetheless, given the right mix of campaign finance reform, judicial vigil, and increased investment in the legislative process, there does seem to be greater possibility for legislatures than for the public-at-large to approximate the deliberative ideal. *See* Julian N. Eule, *Representative Government: The People's Choice*, 67 CHI.-KENT L. REV. 777, 785-89 (1991) (contending that the combination of bicameralism, executive vetoes, logrolling, and judicial review can block bigoted legislation and lead to a greater quality of deliberation than can citizen plebiscites). It should not be forgotten, moreover, that the ability to communicate cheaply and abundantly via the Internet may improve the efficiency, professionalism, and responsiveness of legislatures no less than it may create possibilities for citizen exchange of view. The Internet is already used extensively to enhance communication between legislatures and citizens and to make more information available to legislators and their staffs. *See* Michael Remez, *Policy, Persuasion Take Shape on Internet*, HARTFORD COURANT, Feb. 26, 1998, at A12 (describing an American University study on congressional use of the Internet).

76. For a thoughtful proposal for deliberative direct democracy in one aspect of cyberspace governance, see James S. Fishkin, *Deliberative Polling as a Model for ICANN Membership* (last modified Feb. 22, 1999) <http://cyber.harvard.edu/rcs/fish.html>.

77. For a discussion of such developments, see *infra* text accompanying notes 181-83.

issues.[78] Moreover, given cyberspace's global reach and the difficulty of authenticating the identity of Internet voters, online voting may well be subject to levels of vote buying and voter fraud that make Tammany Hall look like the League of Women Voters.[79] Finally, even aside from the problems of vote manipulation and irregularity, one suspects that Internet voters would generally engage in less, not more, careful deliberation than their offline counterparts. Internet voters facing a daily stream of virtual initiatives would have little time to consider each issue. And the very ease of Internet voting is likely further to militate against deliberation. Supporters of real-world plebiscites argue that voters who must invest the time physically to go to the polls are inclined as a result to consider carefully the issues on which they plan to vote.[80] Internet users voting from home or at work with a click of the mouse would lack that incentive.

ii. Representative Government May Better Reflect Popular Will

Even assuming that liberal government should reflect aggregate voter preferences, representative government may more fully realize that populist vision than does direct democracy. Single-issue initiatives, such as whether to permit the creation of a neo-Nazi newsgroup or whether to prohibit Internet spam, lack a mechanism for reflecting voter priorities among issues.[81] In contrast, an open-ended and rolling legislative agenda enables voters with intense preferences regarding a given issue to bargain for support of their position by conceding issues in which they have less at stake. Through such legislative "logrolling," representative government provides a means for citizens not only to express their preferences on issues (albeit through their elected representatives), but also to express their judgments on the relative importance of those issues.[82] In that sense, representative government can be more reflective of the popular will than is rule by

78. Evan I. Schwartz, *Direct Democracy: Are You Ready for the Democracy Channel?*, WIRED, Jan. 1994, at 74.

79. *See ICANN Membership Advisory Committee Singapore Report* ¶¶ 4.2, 7.2.2 (Mar. 3, 1999) <http://cyber.law.harvard.edu/rcs/macsing.html#4.0> (describing dangers of fraud, manipulation, and vote buying in voting of at-large membership of Internet Corporation for Assigned Names and Numbers).

80. *See* Clayton P. Gillette, *Plebiscites, Participation, and Collective Action in Local Government Law*, 86 MICH. L. REV. 930, 968-69 (1988). On the other hand, as Lynn Baker points out, "issues for plebiscitary decision typically appear on a ballot that includes candidates for elective office," and those who have already gone to the polls to vote for a candidate need invest very little in addition to vote in the plebiscite as well. Baker, *supra* note 75, at 724.

81. Supporters of real world plebiscites argue that citizen initiatives and referenda do reflect the intensity of voter preferences because only voters who care about the issue on the ballot will invest the time to go to the polls to vote. *See* Gillette, *supra* note 80, at 968-69. However, even where this might be the case (as when a ballot includes only the issue for plebiscitary decision), this vote/do not vote option does not enable voters to bargain among issues through vote-trading, which reflects many more gradations of intensity of preference. *See* Baker, *supra* note 75, at 725. Moreover, the argument has little force with respect to Internet voters, who need not go to the polls in order to vote.

82. *See* BUCHANAN & TULLOCK, *supra* note 38, at 134; Clark, *supra* note 71, at 456-63.

plebiscite.[83] Indeed, when plebiscites appropriate issues from the legislative arena, they diminish logrolling opportunities, thus hindering the expression of voter priorities.[84]

Of course, direct democracy need not necessarily be a single-issue plebiscite, and an ongoing multiple-issue direct democracy could conceivably obtain the same or better intensity-measuring benefits as representative government. Logrolling can take place in any setting with an ongoing rule-making agenda, a multiplicity and diversity of issues, open voting, and a mechanism for deliberation and bargaining on votes. But given citizens' limited time and ability to process information, such complex, full-fledged direct democracy is exceedingly rare.

Cyberpopulists might contend that cyberspace overcomes such barriers, making possible a more complex direct democracy. Granted, the Internet makes a plentitude of information available relatively cheaply and provides an inexpensive means by which citizens can communicate their opinions, priorities, and bargaining positions regarding virtual plebiscites.[85] But those cost reductions are insufficient to yield meaningful possibilities for complex virtual democracy. Cyberspace does not materially increase citizens' available time and innate ability to digest information regarding multiple complex issues.[86] Indeed, citizens who are awash in cheap information, most of it unfiltered by trusted intermediaries, may face considerable difficulties in evaluating the accuracy of Internet content and even in assessing the relative import of purported issues.[87] Inexpensive communication for the exchange of opinions and bargaining positions will not make up for this deficit.

---

83. A major caveat: logrolling can be said to reflect the popular will only when citizens stand in a roughly equal bargaining position. This is not the situation in the United States today, where gross disparities in financial and communicative resources, coupled with the absence of meaningful campaign finance regulation, lead to a situation in which representative government reflects more the ability of the wealthy to expend vast resources to lobby and elect representatives who will support their positions on a broad range of issues than it reflects true give and take among issue positions. Even putting aside those distortions, moreover, the desirability of reflecting the intensity of popular preferences is by no means certain. I merely argue here that it can be a more precise indication, or better definition, of popular will.

84. On the other hand, plebiscites may have the beneficial effect of acting as an external check on legislative capture by currently dominant political parties. *See* Issacharoff & Pildes, *supra* note 59, at 669 n.100.

85. The Internet would also make possible a system of ranked voting or electronic vote trading regarding a series of initiative issues. Such systems enable voters to express intensity of preference. However, they are subject to strategic bargaining and other collective action problems. *See* Saul Levmore, The Case for Limited Vote Selling 29-30 (Sept. 21, 1999) (unpublished manuscript, on file with author).

86. *See* Elkin-Koren & Salzberger, *supra* note 56. Browser technology can be expected to provide better ways to filter and organize that information in the future.

87. *See* SHAPIRO, *supra* note 49, at 188-92 (discussing need for trusted intermediaries to sort out bad data from good); CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 185-87 (1997). For a colorful depiction of this problem, see DAVID SHENK, DATA SMOG: SURVIVING THE INFORMATION GLUT (1997).

Finally, voting for representatives enables citizens to express their broad opinions as opposed to merely their issue-specific preferences.[88] In part because of the complexities of modern economic and social life and the difficulty of processing information regarding numerous issues, citizens often do not have a preference one way or another on many given issues.[89] What citizens do have are opinions, a broad political and social outlook, and view of leadership.[90] To the extent that political candidates and parties can be identified with such opinions, voting for representatives may thus reflect "what people want" more than would popular input on specific issues.[91]

c. Tyranny of the Majority

Majority rule by plebiscite may significantly shortchange the liberal democratic ideal of individual liberty. As critics of popular initiatives emphasize, untrammeled majorities can ride roughshod over dissenting individuals and minorities.[92] For that reason, liberal democracy places significant limits on what sheer force of dominant political will may obtain. A regime of rule by online plebiscite[93] would lack such familiar majority-checking devices as constitutional liberties, both substantive and procedural; a balance of power among governing institutions; and an institutional and political requirement that officials' decisions be publicly defensible.[94]

Likewise, at least as narrowly conceived on an issue-by-issue basis, rule by popular majority belies the literalist, cyberian understanding of government by consent of the governed. The losing minority in any given vote has not in fact consented to the decision it has opposed. Anything less than unanimous consent on each discrete issue suffers from an inherent

88. *See* Clark, *supra* note 71, at 464; *cf.* Christopher H. Schroeder, *Rational Choice Versus Republican Moment: Explanations for Environmental Laws, 1969-73*, 9 DUKE ENVTL. L. & POL'Y F. 1, 29 (1998) (contending that voting for representatives who favor environmental protection is a vehicle for overcoming the collective action problem of broad, but moderate support of such protection in face of intense industry opposition).

89. *See* Clark, *supra* note 71, at 476-77.

90. *See id.*

91. *See* JOHN R. ZALLER, THE NATURE AND ORIGINS OF MASS OPINION (1992) (finding that people are ambivalent about specific issues and thus rely on political leaders and other opinion elites).

92. *See* Eule, *supra* note 71.

93. Of course, one could conceivably institute a mixed regime of virtual plebiscite, constitutional liberties to protect dissenters and minorities, and judicial review, akin to what exists in the offline world. But that would move cyberpopulism significantly in the direction of the constitutional territorial democracy that it criticizes. Moreover, there is little reason to think that such cyberconstitutionalism would afford more effective minority protection than its real world counterpart. *See* Part V *infra*.

94. *See* Rawls, *supra* note 66 (discussing the role of public reason in constitutional democracy). Logrolling might also be protective of minorities. *See* Michelman, *supra* note 73, at 1723. *But cf.* Baker, *supra* note 75 (contending that logrolling would not afford greater protection to racial minorities).

consensual governance deficit, at least in the sense that the polity's decision does not reflect the will of the losing minority.

Individuals might consent ex ante to what they conceive to be fair decision-making procedures, such as a majority vote to determine the outcome on any given issue. But to call this rule by consent requires considerable abstraction from the notion of actual universal consent to each discrete decision. It requires a belief that consent to process is tantamount to ongoing consent to outcome. In practice it also requires the consistent application of procedures and decisions that are continually perceived to be fair, and that protect dissenters' ability to influence future votes. Such measures would have to include institutional differentiation and substantive and procedural rights that protect temporal minorities against overbearing temporal majorities. In this abstract sense, rule by consent looks as much or more like representative, constitutional democracy than rule by plebiscite.

Cyberpopulists might proffer two solutions to the twin problems of majority tyranny and defeated minorities. The first is that cyberspace makes possible a regime of unanimous consent, thereby eliminating the problem of defeated minorities.[95] The second, which would apply only to online, not real space, communities, is that, even absent consent, cyberspace offers dissenters easy exit from fora that are not to their liking.[96]

i. Unanimous Consent

Building on early work by Knut Wicksell and Erik Lindhal,[97] public choice theorists argue that, given certain assumptions, a unanimity rule of collective choice is more equitable (that is, Pareto efficient) than majority rule.[98] Unanimity rules effectively transform collective decision making into a neoliberal regime of individual exchange. Under a unanimity rule, no policy can be adopted if anyone votes against it. Thus, no decision

---

95. *See infra* text accompanying notes 97-105.

96. *See infra* text accompanying notes 109-10.

97. Wicksell and Lindahl posited that since public goods are of potential benefit to everyone, it should be possible to provide and distribute their benefits and costs in a manner that would secure each person's agreement. *See* Knut Wicksell, *A New Principle of Just Taxation* (1896), *reprinted in* CLASSICS IN THE THEORY OF PUBLIC FINANCE 72 (Richard A. Musgrave & Alan T. Peacock eds. & J.M. Buchanan trans., 1958) [hereinafter CLASSICS]; Erik Lindahl, *Just Taxation—A Positive Solution* (Elizabeth Henderson trans.) (1919), *reprinted in* CLASSICS 168, *supra*. For further discussion of what has been called the Wicksell-Lindahl tax, *see* JULES L. COLEMAN, MARKETS, MORALS AND THE LAW 278-81 (1988).

98. *See, e.g.*, BUCHANAN & TULLOCK, *supra* note 38, at 85-96; DENNIS C. MUELLER, PUBLIC CHOICE II 43-49 (1989). The unanimity requirement is said to be interchangeable with the concept of Pareto efficiency, which requires that in order for a policy decision to be acceptable, it must make at least one person better off while leaving no one else in a worse position. Pritchard & Zywicki, *supra* note 52, at 449 n.164. *But see* COLEMAN, *supra* note 97, at 284-86 (questioning the equivalence of unanimous vote and Pareto exchange on the grounds that voting contains such ample opportunity for strategic behavior that it cannot be said with confidence to reflect each person's honest preferences for outcomes).

imposes on any person the will of any other person and every decision reflects universal consent. Unanimity may be obtained, at least in theory, by fashioning rules that are acceptable to all, achieving consensus through deliberation and compromise, or buying dissenters' votes by compensating them for their loss.

As proponents of offline universal consent have readily conceded, however, unanimity rules face daunting obstacles in practice. Information and negotiating costs make it impossible to achieve unanimous agreement in many cases.[99] Unanimity rules are also "famously susceptible to holdout problems and abuse by fanatics."[100] Opportunistic bargainers may either extract rents for their consent or simply thwart a decision altogether. As a result, public choice theorists generally limit their proposed application of unanimity rules to narrow circumstances in which the benefits of agreement are substantial and the costs of reaching consensus (including paying subsidies to dissidents) are relatively low.[101] Alternatively, theorists assert, unanimity might be an effective rule-making regime in small, homogenous groups where voters publicly cast their votes and are involved in ongoing interaction, and thus have strong disincentives to engage in strategic bargaining.[102]

Following the cyberian emphasis on consensual decision making,[103] cyberpopulists might posit that cyberspace creates unique opportunities for implementing unanimous rule-making regimes. In cyberspace, some commentators contend, collective decisions are cheaper to reach than in the offline world because of substantially lower information, negotiation, and communication costs.[104] Armed with ready access to a wealth of information and to worldwide digital communication networks, "netizens" (citizens of the Internet) avoid the collective decision-making barriers that plague their poor offline cousins. As a result, it has been argued, cyberspace enables a shift in "the decision-making rule from simple majority

99. *See* Pritchard & Zywicki, *supra* note 52, at 450.

100. Clayton P. Gillette, *The Exercise of Trumps by Decentralized Governments*, 83 VA. L. REV. 1347, 1350 (1997).

101. These include constitutional conventions in which individuals foresee great gains from the formation of a government, must agree only on issues of process and relatively abstract substantive rights, and face considerable uncertainty over their future preferences and positions. *See* BUCHANAN & TULLOCK, *supra* note 38, at 76-81, 251; Dennis C. Mueller, *Federalist Government and Trumps*, 83 VA. L. REV. 1419, 1422-23 (1997).

102. *See* BUCHANAN & TULLOCK, *supra* note 38, at 115; Gillette, *supra* note 100, at 1373-74. Theorists also invoke super-majority requirements as second-best alternatives to actual unanimity. *See* Pritchard & Zywicki, *supra* note 52, at 450.

103. *See infra* note 115.

104. *See, e.g.*, Elkin-Koren & Salzberger, *supra* note 56 (contending, without necessarily favoring cyberspace self-governance, that collective decisions are cheaper in cyberspace).

towards unanimity."[105] Through informed and inexpensive negotiation, Internet users can reach unanimous—or near-unanimous—agreement about such issues as which proposed Usenet newsgroups to admit, how to resolve conflicting claims to Internet domain names, and whether to allow web sites to collect information about visitors' web surfing habits. To the extent the unanimity rule is realized, cyberspace rule making comes to embody the consensual basis for collective decision said by cyberians to underlie the liberal theory of the state.

To my mind, however, Internet communication lacks the capacity to overcome real-space barriers to consensual decision making. For one, while cyberspace contains a plentitude of cheap information, inherent human limitations in sorting and processing that information effectively lead to many of the same information costs and distortions that afflict real world decision making. The same is true of negotiation costs. While digital networks can dramatically reduce the cost of communicating bargaining positions, such communication is, of course, only one component of reaching agreement. No less crucial to negotiation are deliberation, assessment, consideration of alternatives, identifying possible partners and problems, and drafting position papers. Each of these requires a significant amount of offline human thought, time, and effort.[106]

In addition, even assuming a meaningful reduction in information and negotiation costs, it is strategic behavior, not such costs, that poses the most significant obstacle to unanimity rules; and there is nothing about cyberspace rule making per se that reduces incentives for strategic behavior. "Netizens" whose votes are necessary to adopt proposed policy are no less likely to extract rents or cleave to ideological dogmatism than are their offline counterparts (many of whom, of course, are also netizens). As a result, online regimes will suffer many of the same inefficiencies and impediments to reaching consensus as real space communities. In fact, close-knit offline communities may be able, through social pressure, to curtail strategic behavior to a greater extent than highly fluid and heterogeneous online regimes.

---

105. Niva Elkin-Koren & Eli Salzberger, The Economic Analysis of Cyberspace: Challenges Posed by Cyberspace to the Economic Approach Towards Law, at text following note 144 (Dec. 1998) (unpublished manuscript, on file with author).

106. It is likely that computer programs will soon act as "electronic agents" to negotiate contract terms for many Internet transactions. *See* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. (forthcoming 2000) (draft available at <http://www.stanford.edu/class/law453/contracts/Texas92299rev.doc>). Such negotiation, however, will be limited to standardized terms in routine transactions, such as industrial procurement or enabling or denying web site access to a prospective user depending on whether the user's privacy requirements conform to the web site's privacy practices. *See id*.; TIM BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 147 (1999) (describing Platform for Privacy Preferences Project). Negotiation involving more complex issues of community governance will continue to entail considerable real-time human input (at least for the foreseeable future).

Finally, unanimity rules, both in cyberspace and offline, are deeply conservative. When each person's consent is necessary to change the status quo, the status quo is likely to remain unchanged. Since unanimity rules do not arise in a vacuum, their effect is thus to freeze preexisting distributions of entitlements and assets.[107] Generally speaking, this effect may be either desirable or undesirable, depending largely on how one views the antecedent system of holdings. But in cyberspace the fundamental conservatism of unanimity rules would be highly detrimental to liberal democratic values because there entitlements largely involve speech, and controversial speech is unlikely to garner universal acceptance. Were prospective Usenet newsgroups required to obtain unanimous acceptance, rather than the supermajority they currently require, fringe newsgroups would likely be voted down, leaving a thoroughly mainstream Usenet.[108] Unanimity rules in cyberspace would thus cut against the wide-open, robust exchange of views that is central to liberal democracy.

Moreover, preexisting real-space holdings may also have a significant impact on virtual voting. Players with the resources to compensate dissidents are far more likely to overcome both strategic and honest opposition than are those who must depend on the persuasive force of their argument. Thus, to the extent that consensual decision making (or, for that matter, majority referenda) is used to determine arrangements regarding issues such as the use of web visitors' personal information, permissibility of email advertising, or allocation of Internet domain names, commercial entities with the wherewithal to buy votes will be at a decided advantage.

ii. Ease of Exit

The cyberpopulists' favored solution to the problem of majority tyranny focuses on the ease of exit. Cyberpopulists assert that dissenting netizens can, if they so wish, find a haven from the strictures of majority rule by simply leaving the cyberspace forum or network in question and choosing or establishing a new one to their liking.[109] Such exit, cyberpopulists emphasize, is much easier and less costly in cyberspace than in real space. A cyberspace dissenter need only discontinue visiting a forum

---

107. For a discussion of this quality of unanimity rules, see COLEMAN, *supra* note 97, at 286-87.

108. On the voting procedures for the establishment of new Usenet newsgroups, see *supra* note 48. In reality, to say that voting down fringe newsgroups would leave a mainstream Usenet overstates the situation. Usenet administrators have created a hierarchy of alt. (alternative) newsgroups, which do not require voter approval. But that need not be the case with respect to other cyberspace issues and networks.

109. *See* DYSON, *supra* note 22, at 109 (contrasting easy exit for citizens of Internet governments with the "terrestrial government game" which is "all-or-nothing (despite the possibility of loyal opposition)"); Johnson, *supra* note 48 (proposing a system of cyberspace voting in which dissenters would be free to disconnect from networks that adopt a rule they oppose). The classic text on the alternatives of voting and exit in territorial institutions is ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY (1970).

and find, or fairly cheaply establish, an alternative one more closely aligned with the dissenter's views or preferences. Losers in real world plebiscites, in contrast, can usually avoid the result only if they endure the cost and disruption of physically moving to another jurisdiction. As a result, cyberpopulists assert, netizen dissenters and minorities, unlike their real world counterparts, have no need for liberal rights. The capacity for easy exit substitutes for constitutional liberty, and the abundance of alternative rule regimes provides a near certainty of consent.[110]

This argument that exit and abundant alternatives can make up for the illiberal aspects of majority rule is unconvincing. Certainly, exit from a cyberspace forum is considerably cheaper than moving from a physical jurisdiction. Indeed, in many, perhaps most, instances it might entail no more psychic cost than terminating a subscription to a journal or discontinuing watching a television program that has moved to a new time slot. But as cyberians often note, involvement in a virtual community is not always so trivial. Individuals may develop deep feelings of attachment and loyalty to virtual communities and may be devastated by perceived wrongs within those communities.[111] In such instances, exit is far from costless.

In addition, exit is not always as simple as moving from one discussion group to another. There might not be another forum on the same or similar topic that is available to the excluded individual. Nor is it easy to establish a new forum.[112] Indeed, like those whose proposal for a new Usenet newsgroup is voted down, dissenters may be denied the possibility of establishing a new forum within a particular network.[113] In such cases,

---

110. Cyberians also contend that the threat of dissenter exit constrains majority tyranny. *See* Johnson & Post, *Civic Virtue*, *supra* note 2, at 48 (asserting that no tyrannical majority can impose its will on an unwilling minority in cyberspace communities, because users can freely exit and can demand whatever degree of "due process" they wish as a condition to remaining); *cf.* Richard A. Epstein, *Exit Rights Under Federalism*, 55 LAW & CONTEMP. PROBS. 147 (1992) (depicting exit as a check on states' power in a federal system). That proposition strikes me as highly fact-specific, at best. Communities, both virtual and real, differ in the extent to which they wish to attract new participants and keep existing ones. In addition, any constraint imposed by a dissenter's threat of exit depends largely on how much the majority values the particular dissenter's continued presence. Large corporate employers may well extract significant rents for agreeing to forego moving to another location; persistent gadflies, in both territorial and cyberspace communities, will often happily be shown the door.

111. As David Johnson, a leading proponent of cyberspace self-governance, concedes: "While those who disagree with local rules are free to migrate, many users will have invested very substantial amounts of time and effort in establishing a particular online identity (building a reputation based on a particular email address or Web page location, for example). And many seek to participate actively in particular online cybercommunities, over long periods of time. For them, separation from their cybercommunities would impose a very substantial personal loss." David R. Johnson, *Due Process and Cyberjurisdiction*, 2 J. COMPUTER-MEDIATED COMM. (June 1996) <http://www.ascusc.org/jcmc/vol2/issue1/>; *see also* Zittrain, *supra* note 47, at 504 n.10; *Developments in the Law: The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1590-92 (1999) [hereinafter *Developments—Cyberspace*].

112. *See* Siegal, *supra* note 7, at 233 n.350.

113. In reality, Usenet newsgroups that are voted down may now be established within the "alt." (alternative) hierarchy.

and in others involving dissension at the network level, the dissenter faces exit not merely from a single forum, but from an entire network. Since networks, such as the Usenet or the set of proprietary fora administered by America Online, are far less abundant than discussion groups, exclusion from a network may entail a significant diminution in the availability of rule regime alternatives. To the extent that such exclusion substantially reduces the number of persons with whom the dissenter might potentially communicate, it also carries a loss of "network benefits," the value, typical of telecommunications systems, of being a part of a network in which communication with many others is possible.[114]

d. Summary (and Caveat)

Cyberpopulists underestimate representative democracy's capacity to reflect popular will while protecting dissenters. They also grossly overestimate the Internet's capacity to overcome the majority tyranny problem that is endemic to direct democracy.

To identify the cyberpopulist miscalculation, however, is not to prescribe a full array of constitutional rights and majority-checking institutions for the protection of cyberspace dissenters. Rather cyberspace fora and networks should have considerable leeway to treat dissenters as they wish. This is not because cyberspace offers a substitute for the protection of liberal rights; it does not. Instead, as I will discuss more fully below, cyberfora should enjoy some leeway primarily because independent and diverse civic association has its own constitutive value for territorial liberal democracy.

B. Cybersyndicalism

1. The Cybersyndicalist Claim

While cyberpopulists offer an intriguing vision of virtual democracy, Internet rule making is only rarely the direct outcome of anything approaching a formal vote.[115] Accordingly, cyberians generally locate their claims for cyberspace governance in alternative conceptions of "bottom-up" ordering. The cybersyndicalist approach finds consensual self-governance in the social norms that arise from repeat interactions within virtual communities.[116] At one time, the entire Internet was seen to share a

---

114. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 488-89 (1998).

115. In some cyberspace quarters, indeed, voting is viewed with no less disdain than other structures of formal governance. The motto of the Internet Engineering Task Force is "We reject Kings, Presidents, and voting; we seek rough consensus and working code." David G. Post, *Of Horses, Black Holes, and Decentralized Law-Making in Cyberspace*, at text accompanying note 25 (draft version Mar. 1, 1999) <http://www.temple.edu/lawschool/dpost/blackhole.html>.

116. *See, e.g.*, *Developments—Cyberspace*, *supra* note 111, at 1608-09; Gibbons, *supra* note 2, at 518-23.

common meta-culture, roughly characterized by a belief that "information must be free" from proprietary control, government censorship, and the taint of commercial dealing. As the Internet has expanded and become more commercial, however, that common culture has largely, though not entirely, given way to a multitude of local cultures based in Usenet newsgroups, email discussion groups, chat rooms, and other fora.

Drawing heavily upon the literature regarding private ordering and social norms,[117] cybersyndicalists see these local cultures as the site of a political order highly reflective of consensual governance and individual liberty.[118] Their rationale is quite similar to that of the cyberpopulists except that, for cybersyndicalists, netizens manifest active consent to local rule regimes not by voting, but by engaging in the conversation and repeat behavior that generates and perpetuates social norms. Akin to the cyberpopulist argument for unanimity-based rule regimes, cybersyndicalists place great weight on consensus. The development and maintenance of social norms requires substantial, near universal accord and compliance. A social norm will not arise or survive amidst significant intracommunity dissension concerning the norm's acceptability, as it will in majority rule voting.[119]

Also like the cyberpopulist vision, the cybersyndicalist approach places great import on the availability of exit. Traditional close-knit, real-world communities are notorious for their suppression of dissent. For cybersyndicalists, no less than for cyberpopulists, the key to individual liberty and consent in virtual communities is the relative ease with which a dissenter may exit her current community and join or establish another more in line with her preferences or values.[120] In sum, the cybersyndicalist vision mirrors the neoliberal redescription of the liberal order: a network composed of multiple voluntary organizations and individual agreements.[121]

---

117. *See* sources cited *supra* note 23.

118. *See, e.g.*, Gibbons, *supra* note 2, at 519 (contending that the model of "governing cyberspace through informal social norms . . . is the most decentralized and democratic"); *cf.* Zittrain, *supra* note 47, at 499 (discussing generation of local cultures by early newsgroups).

119. In addition, as Larry Lessig aptly notes, norms have a radically different tenor than rules determined by vote. Norms often arise organically from what people do within a close-knit community. The need to resolve issues by discussion and ballot (or formal negotiation) generally signals the fall of a thick, homogeneous community. *See* LESSIG, *supra* note 12, at 77-78.

120. *See, e.g.*, DYSON, *supra* note 22, at 8 (noting that "people who don't like the rules can leave"); Gibbons, *supra* note 2, at 522 ("A violator of the rules of a self-governing cyberspace community who is 'excommunicated' from the community can locate a new community and create a new identity there.").

121. For an illuminating discussion contrasting this contractarian view of groups with a communitarian view, see Gregory S. Alexander, *Dilemmas of Group Autonomy: Residential Associations and Community*, 75 CORNELL L. REV. 1, 19-23 (1989).

2. Critique of the Cybersyndicalist Claim

Given the large overlap between the cyberpopulist and cybersyndicalist claims, my criticisms of the former largely apply to the latter as well. The cybersyndicalist claim, however, is especially vulnerable to the tension, if not fundamental contradiction, between community and exit. Studies emphasize that a high degree of homogeneity and stability of membership is critical to a group's generation and perpetuation of social norms.[122] Virtual communities, with their relative ease of exit (and, in many cases, entrance), present classic counterexamples to the types of territorially bound close-knit groups in which rule by social norms is possible. Accordingly, it is hardly surprising that cyberfora most characterized by bottom-up norm generation (as opposed to rule by moderator or administrator fiat) rapidly degenerate into a familiar pattern of mutual recrimination ("flame wars") and disillusionment.[123]

A game theoretic model may help to explain the often cited and frequently lamented unraveling of virtual communities.[124] The prisoner's dilemma and similar such games have been used to model social phenomena in which the participants would benefit by cooperating with one another, but nevertheless fail to do so.[125] In the typical prisoner's dilemma situation, each participant enjoys the greatest gain if all participants cooperate. But each participant would suffer the greatest loss—a loss in excess of that incurred by the universal failure to cooperate—if she seeks to cooperate but others defect. At the same time, the model assumes, no participant can be certain of the others' cooperation, and thus each participant has an incentive to defect. As a result, defection will often be the participants' overall dominant strategy, even though universal defection is a less desirable alternative than universal cooperation.

---

122. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 88-89 (1990); Epstein, *supra* note 23, at 7-8; *see also* ELLICKSON, *supra* note 23, at 283 (noting that people are increasingly likely to turn to legal rules, rather than social norms, to resolve disputes "when the social distance between them increases").

123. *See* Siegal, *supra* note 7, at 191; *see also* Peter Kollock & Marc Smith, *Managing the Virtual Commons: Cooperation and Conflict in Computer Communities*, *in* COMPUTER-MEDIATED COMMUNICATION 109, 125 (Susan C. Herring ed., 1996), *available at* (visited Dec. 25, 1999) <http://www.sscnet.ucla.edu/soc/csoc/papers/virtcomm> (noting that as a result of flaming and off-topic postings, conflicts in Usenet newsgroups are "fairly common").

124. For discussion of disintegration of virtual communities, see Zittrain, *supra* note 47, at 500-01. For an illuminating application of game theory to group solidarity, see Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action*, 63 U. CHI. L. REV. 133 (1996).

125. For an illuminating discussion of the prisoner's dilemma and other game theoretic models in the context of the production of social norms, see Kornhauser, *supra* note 23, at 659-68.

Civil discourse is a collective good that is the product of the contributions of individual discussants.[126] Civility requires active cooperation; its maintenance requires constant effort and diligence among community members. Discussants must express their views and disagreements in a civil manner, suppressing the desire for cutting retort. They must also educate newcomers as to the need for civility. Moreover, a norm of civility requires universal, or at least near universal, compliance. One or two individuals engaged in flaming or off-topic diatribe may radically alter the character of community discourse, much like the eruption of a heated argument between two guests fundamentally changes the tenor of a small social gathering.[127]

Assuming that civility is a universally shared goal,[128] flaming and other active flouting of the civility norm clearly constitutes prisoner's dilemma defection. But so does doing nothing. Civil discourse, as just noted, is a collective good that can emerge only through the ongoing active contributions of community members. Cooperation in the establishment and perpetuation of the civility norm thus entails more than simply refraining from flouting the norm while silently "lurking" in the background.[129] It also requires making periodic civil contributions to community discussion and helping to educate newcomers as to the norm. Concomitantly, the failure actively to participate in the maintenance of the civility norm in that manner also constitutes defection. In other words, when cooperation entails making contributions to the production of a collective good, free riding on others' contributions constitutes defection.[130]

The prisoner's dilemma and other game theoretic models would predict that, absent some mechanism for compelling or inducing cooperation, virtual community members will have every incentive to defect, whether by failing to suppress the urge to flame or by free riding off others' efforts

126. *See* COLEMAN, *supra* note 97, at 253-54 (defining collective good). For an illuminating discussion of this point in the context of Usenet newsgroups, see Kollock & Smith, *supra* note 123, at 115-17.

127. *See* Siegal, *supra* note 7, at 191 (noting prevalence and destructive impact of flaming on Usenet newsgroups).

128. Civility may not be a shared goal. In some instances, individuals may take delight in disrupting and even in destroying newsgroup discussion by flaming. *See* Siegal, *supra* note 7, at 191. When that occurs, civility will be impossible to obtain without excluding such individuals from the group. In game theory terms, such individuals enjoy a greater pay-off from universal defection from the civility norm than any other alternative. *See* Kornhauser, *supra* note 23, at 661-63 (presenting game theoretic analysis of distributional differences and lack of consensus in context of group generation of social norms).

129. "Lurking" is a commonly used term for listening in on Internet discussion without actively participating.

130. *See* COLEMAN, *supra* note 97, at 255. For a discussion of Usenet "lurking" (that is, failing actively to participate in discussion) as free riding, see Kollock & Smith, *supra* note 123, at 116.

to produce civility.[131] This is true for two reasons. First, given that the absence of a single individual's ongoing active contribution will not noticeably weaken the civility norm, each individual has the incentive to free ride on others' contributions.[132] Second, for any given individual, it is not worth incurring the costs of cooperation when cumulative defections by others may radically undermine the civility norm, thus depriving the individual of the benefits of incurring those costs. And so, as often happens in unmoderated cyberfora, one or two individuals actively defect by engaging in flaming or off-topic diatribe and others then defect by counterflaming or simply ceasing to participate in community discussion.

Close-knit, real-world communities may generally diminish, and often overcome, the incentive to defect.[133] In such settings, persons have a permanent stake in cooperation, are able to communicate to coordinate their behavior, and suffer social sanctions of varying degrees if they fail to cooperate.[134] As a result, each person has a relatively high degree of trust ex ante that others will contribute their share to the production of collective goods (although even in many real-world communities, shirking is a perennial source of social tension).

Virtual communities may share some of these cooperation-inducing attributes. Certainly, discussants communicate to attempt to bring about mutual cooperation. Shaming through written criticism could also be an effective tool to enforce civility norms against those who contravene them, albeit of lesser effectiveness than when members must literally face each other and cannot hide behind the anonymity made possible by Internet technology. Finally, violators may be silenced by software enabling users to filter out messages from certain persons[135] or by exclusion from the community (although the latter generally entails a top-down act from the local system operator rather than bottom-up norm enforcement per se).[136]

---

131. *See* Kollock & Smith, *supra* note 123, at 117 (noting temptation among Usenet newsgroup discussants "to free-ride on others' efforts to maintain norms of civility while violating those norms [themselves]").

132. *See* Daphna Lewinsohn-Zamir, *Consumer Preferences, Citizen Preferences, and the Provision of Public Goods*, 108 YALE L.J. 377, 392-93 (1998) (discussing role of greed and hopelessness underlying prisoner's dilemma defection).

133. Repeated or ongoing business dealings, or simply situations in which an individual or business obtains benefits from a reputation for cooperation also diminish incentives to defect. *See* Andrew Rutten, *Anarchy, Order, and the Law: A Post-Hobbesian View*, 82 CORNELL L. REV. 1150, 1155-56 (1997); Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOC. REV. 55, 65 (1963).

134. *See* ELLICKSON, *supra* note 23, at 164-66; Rutten, *supra* note 133, at 1155 (noting that the prisoner's dilemma is not applicable when transactions occur within "a rich web of social relations").

135. Such technical devices, known as "kill files" or "bozo filters" have the disadvantage that other participants not using a filter and not subject to the filter may view the offending post and comment on it. *See* Kollock & Smith, *supra* note 123, at 120.

136. Punishing someone who does not conform to a norm, whether by exclusion, shaming, or some other sanction, is itself a public good for the community that wants the norm enforced. Since it may be costly for individuals to sanction others, norm enforcement also gives rise to a collective action

All told, however, individuals will invest in such cooperation-inducing measures only if they have a sufficient stake in the outcome. Here is one place where exit undermines norm creation. The greater the freedom of movement among virtual communities, the greater the cost of perpetuating social norms (given the outflow of those with knowledge of the norm and the influx of ignorant newcomers) and the lesser the stake of any given individual in any particular community.[137] Mobility also undermines each individual's trust that others will match her contributions to the production of collective goods rather than free riding on those contributions.[138] Mobility may be substantially more limited when the relevant "community" is an entire network of discussion groups rather an individual group itself. But such networks are generally too large and too diverse to generate a stable, cohesive set of norms from the bottom up, as opposed to by network administrator fiat.[139]

At bottom, then, as I discussed in my critique of cyberpopulism, when individuals have a substantial stake in a particular virtual community, exit is not a tenable option to protect them against majority oppression. But when individuals lack that investment, the result is a flame-ridden cacophony rather than a cohesive community capable of government by the "bottom-up" generation of social norms. Neither prospect, I will again emphasize, necessarily calls for systematic state intervention. They do, however, belie the notion that either cyberpopulism or cybersyndicalism may form a basis for the claim that cyberspace self-government is a viable mechanism for realizing liberal democratic ideals.

---

problem. *See* MICHAEL TAYLOR, THE POSSIBILITY OF COOPERATION 30 (1987); *see also* Steffen Huck & Michael Kosfeld, *Local Control: An Educational Model of Private Enforcement of Public Rules*, Tilburg University for Economic Research Discussion Paper 126, at 2-3 (Oct. 1998) <http://ideas.uquam.ca/ideas/data/Papers/dgrkubcen1998126.html> (noting that rational individuals aiming to maximize short-run payoffs will never report deviant behavior to local authorities). Individuals are often, but certainly not always, willing to engage in shaming the offender. But especially when norm enforcement warrants more severe punishment, overcoming the collective action problem typically requires the appointment of a leader (or governing body) with the authority and willingness to select and impose a sanction. For a fascinating account of a virtual community faced with such a collective action problem following one of its member's "virtual rape" of another, see Julian Dibbell, *A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, *in* INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 293 (Mark Stefik ed., 1996).

137. *See* SHAPIRO, *supra* note 49, at 121 (noting that, given mobility, "there is little incentive to keep online associations intact"); Kollock & Smith, *supra* note 123, at 119-20 (noting mobility's deleterious effect on Usenet newsgroups); *see also* BUCHANAN & TULLOCK, *supra* note 38, at 114 (noting that while mobility enables individuals to avoid losses from adverse collective decisions, it also means that an individual will find it disadvantageous "to invest too much time and effort in persuading his citizens to agree with him").

138. *See* OSTROM, *supra* note 122, at 90 (noting that successful communities require clearly defined boundaries in order to prevent outsiders from reaping benefit of collective good or destroying it).

139. Social norm theorists concede that the bottom-up generation of social norms requires a relatively stable, close-knit community. *See supra* note 122.

C. Cyberanarchism

1. The Cyberanarchist Claim

Cyberanarchists see cyberspace as a market of alternative rule regimes. In their view, cyberspace "governance" consists of the contingent aggregate result of a multitude of individual decisions.[140] In the cyberanarchist vision, cyberspace is a system characterized by the ready ability of (1) each individual to choose which cyberspace sites and networks she wishes to visit, (2) site and network administrators to define local norms and use technology to enforce them, in large part by excluding dissenters, and (3) dissenters to find alternative sites (or networks) or establish new ones.[141] In this scheme, it is entirely irrelevant whether local norms are produced by vote, cohesive community, negotiation, or administrator fiat. Individual liberty and consent are guaranteed by individuals' ability to shop for desirable rule regimes. As Esther Dyson puts it:

> A Net-based government can operate *only* by consent of the governed. Any Net government must therefore provide its citizens with real benefits if it wants them to stick around. Those benefits may not be just personal goods or services, but rather the broader benefits of a regulatory regime: a clean, transparent marketplace with defined rules and consequences, or a supervised community where children can trust the people they encounter or individuals' privacy is protected.[142]

As we will presently see, Dyson's halcyon portrait widely misdescribes the cybermarketplace. However, the cyberanarchist paradigm does approximate the potential nature of cyberspace governance for the vast majority of Internet users far more closely than do the cyberpopulist and cybersyndicalist visions. Most of us encounter cyberspace rule regimes, knowingly or unknowingly, in the form of standard adhesion contracts or their digital equivalent. When we obtain Internet access through America Online or another Internet service provider (ISP), we do so subject to the ISP's standard "Terms of Service." Such terms cover a broad spectrum of issues, including restrictions on the type of messages subscribers may upload to discussion fora, ISP rights to copy and modify subscriber messages, ISP use of subscribers' personal information, and ISP perogatives unilaterally to modify the Terms of Service and to terminate subscriptions at its discretion. Likewise, many web sites contain standard conditions of

---

140. *See, e.g.*, Gibbons, *supra* note 2, at 490; Post & Johnson, *Civic Virtue*, *supra* note 2, at 46-50; Post, *Anarchy*, *supra* note 2.

141. *See* Post & Johnson, *Civic Virtue*, *supra* note 2, at 46-50.

142. DYSON, *supra* note 22, at 109; *see also* Johnson, *supra* note 111 (contending that a market in rule regimes will induce some Internet service providers to accord subscribers due process rights before terminating a subscriber's service).

use,[143] governing similar topics, to which the user purportedly agrees by clicking on the appropriate button or simply entering the site.[144] Less formally, moderators unilaterally set the norms of participation in many newsgroups and email discussion groups. Finally, those who design and implement program code and network architecture essentially prescribe the terms of much Internet use.[145] Digital encryption increasingly governs the terms for gaining access to and making use of text, music, graphics, and films available on the Internet.[146] And the program code for browsers effectively determines what web sites users may or are likely to visit and what information site operators may obtain about them.[147]

At the margins, users might be able to negotiate for desired terms or, in some instances, to establish their own web sites or discussion groups with rules more to their liking. In a regime of cyberanarchy, they might even be able to deploy technology to circumvent encryption-enforced restrictions on use and access.[148] But for the vast majority of us, in the vast majority of cases, user input will consist entirely of consumer purchasing behavior. At bottom, the cyberanarchist claim is that consumer's "power to switch" from one rule regime to another will discipline the market, yielding an array of rule regime choices that comport with consumer demand.[149]

---

143. *See, e.g.*, The New York Times on The Web, *Subscriber Agreement* (visited Jan. 5, 2000) <http://www.nytimes.com/subscribe/help/agree.html>.

144. Such "click-wrap" agreements are currently of uncertain enforceability. However, they would be enforceable under the proposed Uniform Computer Information Transactions Act (UCITA), which the National Commissioners on Uniform State Laws approved for presentation to state legislatures in July 1999. UCITA is available at (visited Jan. 5, 2000) <http://www.law.upenn.edu/library/ulc/ucita/citam99.htm>. Of course, true cyberanarchists would have to find extra-legal methods of enforcing such agreements, including technological self-help and barring offenders from further access.

145. *See* sources cited *supra* note 11.

146. Such digital encryption rights management systems are commonly called "trusted systems." Mark Gimbel, Note, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 STAN. L. REV. 1671 (1998); Radin & Wagner, *supra* note 6, at 1315 (referring to trusted systems as a "regime of technological self-enforcement" that is "anarchic rather than legal").

147. Web browsers, such as Netscape Navigator and Microsoft Internet Explorer, contain software protocols ("cookies") that create files about web sites that have been visited and that accept and save on the user's hard drive data sent by a web site operator regarding the user's visit to the site. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1629-31 (1999).

148. Users would face significant restrictions in doing so under current law. Recent federal legislation prohibits the circumvention of technological measures designed to control online access to and uses of copyrighted works. *See* Digital Millennium Copyright Act, Oct. 28, 1998, Pub. L. No. 105-304, § 1, 112 Stat. 2860.

149. *Cf.* Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462, 529 (1998) (describing conventional economic model of consumer power in mass-market transactions).

2. Critique of the Cyberanarchist Claim

The cyberanarchist claim falls apart at a number of key points, which I group into two categories.[150] First, the cyberanarchist claim depends upon a greatly exaggerated view of consumer sovereignty in the cyberrule regime marketplace. Second, the claim is vulnerable to many of the standard criticisms from liberal democratic theory regarding the use of the market as a mechanism for individual and collective choice.

a. Individual Autonomy (as Consumer Sovereignty) in Cyberspace

The cyberanarchist claim depends on the notion that individuals' choice of rule regimes reflects their true preferences regarding rules. That claim comprises two parts: first, that Internet users exercise at least some modicum of meaningful, informed choice in selecting rule regimes, and, second, that Internet users enjoy free mobility among a plethora of alternative rule regimes. In reality, however, Internet user autonomy of choice and mobility are both far more constrained than cyberanarchists suggest. I will first discuss a number of limitations on Internet users' meaningful choice in selecting rule regimes. I will then examine constraints on mobility, including both barriers to exit and a likely dearth of alternative rule regimes from which to choose.

i. Meaningful Choice

I must confess: I have never chosen one web site over another because I preferred the former's conditions of use over the latter's. Indeed, I rarely bother to read a web site's conditions of use. Nor have I sought to determine whether my Internet browser is set to filter out certain content or allow web site operators to leave "cookies" (information regarding my site visits) on my hard drive for their later use.[151]

My failure to assess and compare such rule regimes is no doubt typical of Internet users.[152] In fact it parallels the inaction of offline consumers faced with a standard form contract. No one expects consumers to read, let alone negotiate, such contracts.[153] Nevertheless, the law presumes consumer consent from the customer's signature (or other objective

150. I will not discuss another potential fault line in the cyberanarchist claim: To the extent self-proclaimed cyberanarchists depend on the state, rather than technological self-help, to enforce cyberspace contracts and even to protect computer network installations from real world theft and trespass, cyberanarchists are neither truly anarchists nor, arguably, believers in cyberspace independence. *See* Radin & Wagner, *supra* note 6, at 1297.

151. *See supra* note 147 (describing "cookies").

152. *Cf.* SHAPIRO, *supra* note 49, at 95-96 (describing "screen bias" effect of Microsoft Explorer interface leading users to Microsoft corporate partner web sites and noting that few users will reconfigure default desktops).

153. *See* Todd Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1179 (1983); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. b (1979) ("Customers do not in fact ordinarily understand or even read the standard terms.").

manifestation of assent), and an adhesion contract is enforceable unless manifestly oppressive.[154] The market could not function otherwise. Indeed, a primary purpose of standardization is to eliminate bargaining over details of individual transactions when bargaining costs and unpredictable, customized bargains would deter producers from making valuable products and services available. We would all be worse off, the argument goes, if customer understanding and consent were prerequisites for standard form contract enforceability.

But the cyberanarchist claim is about neoliberal individual autonomy, not social welfare.[155] Cyberanarchists want to say that each individual chooses his or her rule regimes. In their view, the resultant rule regime configuration manifests individual liberty, not a utilitarian calculus. It is this claim of individual liberty, not efficiency, that undergirds the cyberanarchist political claim.

So a cyberanarchist must say, following a neoclassical economics model of consumer sovereignty, that my inaction—my failure even to attempt to inform myself of the rules that govern my cyberspace activity—expresses my choice to accept cyberspace rule regimes as they are, whatever they are. If potential web site use conditions truly concerned me, I would read the fine print and factor it into my choice of web sites. If my browser settings were of sufficient importance to me, I would reconfigure them to my liking. Since I do not do these things, I must place little value on the matters they regulate. I must not really mind if others use my personal data or if I cannot freely access and use the information I glean from a web site.

In cyberspace, no less than offline, however, the neoclassical model of consumer sovereignty applies much better to comparison shopping for price or transparent product quality than to shopping for terms.[156] Rule-regime shopping entails the costs of acquiring and processing information on terms, including appraising the many contingencies that adhesion contracts typically address.[157] Such costs greatly exceed those involved in comparing price or web sites' visual appeal, ease of use, and expressive content. On the Internet, indeed, the cost of discovering and evaluating alternative rule regimes may well be prohibitive. The Internet's central value lies in providing a wealth of information in a fraction of the time that

154. *See* RESTATEMENT (SECOND) OF CONTRACTS § 211 (1981).

155. Of course, cyberanarchists might also make efficiency arguments favoring cyberspace self-governance. But individual liberty, not efficiency, stands at the root of their liberal perfection claim.

156. *See* Cohen, *supra* note 149, at 488.

157. *See* J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, *in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY, at text beetween notes 14 & 15 (Deborah Hurley et al. eds., forthcoming 2000) (discussing absence of transparency in the information-based sectors of the digital economy); Rakoff, *supra* note 153, at 1221-27 (contrasting incentives on adhesion contract drafters to contain even remote contingencies with consumers' difficulty in assessing such risks).

would be required to obtain the information offline. But if Internet users were to read and consider the conditions of use for each web site they visit, that value would be lost. If we were to assess and compare alternative rule regimes whenever we surfed the Internet, we would have to sharply curtail our Internet use.

The cybermarket in rule regimes, then, contains significant information, collective action, and efficiency asymmetries. ISPs and web site operators are repeat players. They can spread the cost of developing standard terms of use among thousands and, in some cases, millions of potential users. Firms also reap significant organizational benefits from term standardization, reducing transaction costs within the firm as well as in customer dealings.[158] Moreover, the Internet dramatically reduces interfirm coordination costs; it makes standard terms publicly accessible, enabling rule regime producers to "coordinate" with one another simply by replicating each others' terms. Finally, in a dynamic market such as cyberspace, where firms must place a premium on flexibility, it is far more rational for firms to compete on price and product improvements than on terms of use that lock in the parties for the entire duration of their relationship.[159]

Internet users, on the other hand, face material information and collective action costs in responding to producers' standard terms. Individual consumers must first find and assess a producer's terms. Neither is an easy task. Indeed, when the terms are embedded in program code many Internet users do not even know of their existence.[160] Moreover, when users do appraise producers' terms, they have only the choice of accepting or rejecting the terms, not negotiating changes. (And even if users could negotiate, they might have limited bargaining power. In many cases, the informational goods available over the Internet lack perfect substitutes, giving producers a degree of market power.)[161] Thus, even at best, users would enjoy limited benefits from expending the time and effort to compare rule regimes.

To be certain, Internet communication reduces collective action costs for users, in theory laying the groundwork for user representatives or

---

158. As Todd Rakoff points out, a firm's internal hierarchical and organizational structure provides a significant incentive for firms to employ standard contracts. *See* Rakoff, *supra* note 153, at 1222-25.

159. *See* David J. Teece & Mary Coleman, *The Meaning of Monopoly: Antitrust Analysis in High-Technology Industries*, 43 ANTITRUST BULL. 801, 812 (1998) (discussing premium on dynamic capabilities and firm flexibility in the high-tech market). Web site standard contracts often provide that the producer may unilaterally modify the terms and that the user is deemed to agree to such modifications if she continues to visit the site or fails to cancel her subscription. *See, e.g.*, THE NEW YORK TIMES ON THE WEB *Subscriber Agreement* (visited Jan. 5, 2000) <http://www.nytimes.com/subscribe/help/agree.html> ¶¶ 1.2, 1.3.

160. *Cf.* LESSIG, *supra* note 12, at 181 (favoring open regulation through law over regulation hidden within code because "[o]nly when regulation is transparent is a political response possible").

161. *See* Cohen, *supra* note 149, at 520-21.

organizations to assess producer rules or propose their own counter-terms. But given the wide diversity and sheer number of Internet users, coupled with innate human limitations in processing information and coordinating positions, collective action costs would remain significant, and would likely prevent any serious user challenge.[162] In addition, individual users would not enjoy the repeat player and other efficiency benefits that standard terms provide for many ISPs, web site operators, and other rule regime producers. As a result, rule shopping and drafting is generally more costly for users, both in absolute terms and relative to potential benefits, than for producers.[163]

Of course, market efficiency requires neither that consumers coordinate their positions nor that every consumer have full information regarding a product. Often, the presence of some number of sophisticated consumers is sufficient to discipline the market. It might be argued, therefore, that it does not matter if most Internet users do not know that certain browsers are set to leave "cookies" and that certain web sites are set to receive them.[164] So long as some users do know and have a preference for cookie-free alternatives, the market will make cookie-free alternatives readily available to all.

Significantly, however, such market discipline does not comport with the cyberanarchists' political claim. Consumers who have to rely on their more sophisticated counterparts are not themselves exercising ongoing individual consent to the prevailing rule regimes. They are rather relying on sophisticated consumers as their "agents." Moreover, in contrast to representative democracy, the unsophisticated consumers have not elected their sophisticated counterparts, and sophisticated consumers owe no duty to represent and have no particular self-interest in representing the unsophisticated masses. If the sophisticated consumers can realize their preferences by buying goods that are tailored specifically to them at the same or lesser cost than goods that are available to the public at large, they will do so, and producers will have no incentive to alter the rule regime for

---

162. Of course, an enterprising lawyer might set up a web site to sell his advice regarding alternative rule regimes (and we can assume that such activity would be permitted in a cyberanarchist world). But collective action costs would apply to that scenario as well. Legal advice is a nonexcludable, nonconsumable quasi-public good. Accordingly, unless users banded together to pay for the advice, the lawyer would be unable recover his costs in producing it.

163. Developing Internet technology might enhance user ability to shop for terms. Users might deploy program code, known as an electronic agent, to identify disfavored web site terms. *See* Radin, *supra* note 106. Upon identifying the terms, the agent would then direct the user's browser not to enter the offending site or conceivably would submit a counteroffer to the site proprietor (or the proprietor's electronic agent). It is too soon to tell how such technology might develop, whether producers will deploy technology to circumvent it, or whether it would compel producers to forgo the institutional benefits of standard contracts (or overcome producers' possible market power).

164. A "cookie" consists of information regarding a users' web site visits that resides on the user's hard drive for use by the web site operator whenever the user visits the site.

others.[165] And, given that digital technology enables producers to engage in considerable price and product discrimination among consumers, producers may well provide noncookie goods for those sophisticated consumers who insist on them and cookie goods for everyone else.[166]

ii. Mobility

The cyberanarchist vision does not depend solely upon individual autonomy in assessing alternative rule regimes. It also posits near frictionless mobility among rule regimes. Mobility, in turn, comprises both free exit from existing rule regimes and a plethora of alternative regimes from which to choose. But as I will discuss in this Section, Internet users enjoy neither the ease of exit nor the limitless choice that cyberanarchists presume.

As we have seen, Internet users have limited voice in altering rule regime terms. Users may also have limited possibilities for exiting rule regimes they have already joined. As noted above in connection with cyberpopulism and cybersyndicalism, individual exit is not always feasible. Individuals who have invested in learning the technology, user interface, and rules associated with a particular virtual forum may face considerable switching costs in moving to another.[167] Moreover, over and above that rational cost barrier, individuals exhibit a systematic tendency to place an inflated value on what they already have.[168] Especially when combined with the feelings of loyalty and attachment to virtual communities that I have discussed above,[169] such endowment effects and status quo biases may themselves create material exit costs.[170] And when individuals exit from the entire network, their exit costs are further magnified. The

165. For example, producers might grant more advantageous terms in business-to-business Internet transactions, which make up a growing portion of electronic commerce. *See* Radin, *supra* note 106.

166. Many producers will resist even this level of flexibility towards consumer demand. In many cases producers' "institutional costs of changing forms and procedures are greater than would be warranted by the profits to be made by satisfying the demands of marginal customers." Rakoff, *supra* note 153, at 1226 n.190. In addition, a provider that provides preferential terms for some customers may face an adverse selection problem, whereby the most costly customers will be drawn to that provider. *See* Einer Elhauge, *Allocating Health Care Morally*, 82 CALIF. L. REV. 1449, 1477 (1994) (discussing scenario in which high-risk subscribers flock to insurance company that offers preferential terms). For example, an Internet service provider that unilaterally acceded to prospective subscribers' demands that it accord them due process rights before terminating their subscription might well attract particularly troublesome subscribers who have particular reason to want such rights.

167. *See* Teece & Coleman, *supra* note 159, at 828-31 (1998) (discussing switching costs in the market for high-tech consumer goods).

168. *See* Daniel Kahneman et al., *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, J. ECON. PERSP., Winter 1991, at 193.

169. *See supra* note 111 and accompanying text.

170. Status quo bias also impedes user ability to negotiate changes in provider rules. *See* Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583 (1998).

exclusion of a user from America Online, an email host from communication with other hosts, or a web site from a domain name registry cuts off the excluded party from vast amounts of information or from contact with large numbers of other netizens. Given that loss of network benefits, the notion of freedom to exit and choose an alternative in such situations is highly chimerical.[171]

Internet users will increasingly face parallel constraints in their menu of rule regime alternatives. The early Internet promised, and to a large extent delivered, a communications revolution. Previously only those with the financial wherewithal to own a newspaper or broadcast station could reach a mass audience. But the availability of digital networks drastically reduces entry costs into the mass communication market. The result is the cacophony of diverse voices that has come to characterize the Internet.

The Internet, however, is poised to change in ways that will bring back many of the structural characteristics of the pre-digital mass media market. At the low end, the Internet will continue to feature a lively and widely diverse array of virtual street corner podia, including discussion groups, chat rooms, individual web sites, and other fora heretofore unimagined. But the high end—where most people will spend most of their cyberspace time—will be controlled by the media and telecommunications mega-conglomerates that have already begun to flex their muscles on the Internet.

It seems as if not a day goes by without another media, telecommunications, and, increasingly, Internet content- or service-provider company merger.[172] That phenomenon is hardly surprising. The negligible marginal cost of Internet communication and connection creates unprecedented economies of scale for the business of producing and disseminating information. As economists have long recognized, "where technology creates

171. The same is true with regard to starting a new forum or virtual community. Such an enterprise may require a significant investment of time, energy, and money. It may also depend on the meta-norms within a given network for accepting new sites. If the network is unwilling to allow the new site, then its would-be creators must exit the network, with the attendant costs and possible loss of network benefits.

172. One recent day provides an example: On October 5, 1999, the *New York Times* reported (1) the acquisition by MCI WorldCom, the nation's second largest long-distance carrier, of Sprint Corp., the nation's third largest long-distance carrier and a major purveyor of wireless voice, video, and data transmission services; (2) the acquisition by Clear Channel Communications, the nation's largest owner of radio stations, of AMFM, Inc., the nation's second largest owner of radio stations; and (3) the acquisition by Travelocity, an online travel service, of a smaller rival, Preview Travel, vaulting Travelocity past Microsoft's Expedia to become the largest travel site on the Web. *See MCI WorldCom to Buy Sprint in $115 Billion Deal*, N.Y. TIMES, Oct. 5, 1999, at A1; Bill Carter, *The Leader in U.S. Radio to Buy No. 2*, N.Y. TIMES, Oct. 5, 1999, at C1; Saul Hansell, *Travelocity Makes a Deal to Dominate Web Market*, N.Y. TIMES, Oct. 5, 1999, at C7.

Of even greater likely significance for cyberspace concentration is American Online's acquisition of Time-Warner, announced just before this Article went to press.

significant economies of scale, markets tend towards dominance by a few large players."[173]

Moreover, a number of additional phenomena will add fuel to the centripetal force of producers' economies of scale, amplifying the threat of oligopolistic constraints on competition.[174] I will briefly mention two: network effects and emerging Internet technology.

The network benefits inherent in communications systems, particularly systems such as the Internet in which users can disseminate as well as receive communication, make those systems a natural monopoly.[175] When users must choose among two or more incompatible communicative networks, market power can quickly tip the scales in favor of a single communicative network as users stampede to the network that gives them the ability to communicate with the greatest number of other users. Such a result circumscribes user choice of rule regimes. Just as Microsoft's marketing and exercise of market power has led to the near-universal adoption of a computer operating system that many disparage as suboptimal,[176] so may market power result in near-universal adherence to dominant rule regimes that do not reflect ongoing free and informed user choice.

Emerging Internet technology fuels rule regime centralization by effectively raising cyberspace market entry costs. In a world awash in cheap information, audience attention becomes a scarce and highly sought-after resource.[177] Not surprisingly, then, commercial players compete vociferously to draw Internet users to their portals and web sites, and to keep

---

173. Cohen, *supra* note 149, at 522; *see also* Philip E. Agre, *supra* note 5. Apparently, only more vigilant federal antitrust regulation and telecommunications service ownership restrictions, no doubt anathema to cyberanarchists, will maintain even a modicum of diversity among the major players in cyberspace communication in the coming decades. Unfortunately, most regulation in this area focuses on economic efficiency rather than expressive diversity. The Federal Communications Commission, for example, has recently relaxed ownership restrictions, enabling heavy concentration in one industry, such as cable television, if such concentration holds the promise of increased competition and thus lower prices in another, such as local telephone service. *See* Stephen Labaton, *Ownership Rules in Cable Industry Loosened by F.C.C.*, N.Y. TIMES, Oct. 9, 1999, at A1.

174. For a study of such constraints in traditional media, see Neil Gandal & David J. Salant, *Hollygopoly: Oligopolistic Competition for (Hollywood) Movies*, 40 ANTITRUST BULL. 699 (1995). For a survey of the empirical and theoretical literature on oligopoly, see F.M. SCHERER & DAVID ROSS, INDUSTRIAL MARKET STRUCTURE AND ECONOMIC PERFORMANCE 199-315 (3d ed. 1990).

175. *See* Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93 (1994); Lemley & McGowan, *supra* note 114, at 488-90, 551-52. While economies of scale are a producer-side characteristic describing increasing returns as inputs are scaled up, network effects are a demand-side phenomenon associated with value to the consumer. *See* Teece & Coleman, *supra* note 159, at 814.

176. For a discussion of the role of network effects in leading to market dominance for Microsoft operating systems, see SHAPIRO, *supra* note 49, at 94-95.

177. As Bill Gates presciently describes the Internet's near future: "If a stranger . . . wants to send you [electronic] mail, [he'll] have to put up a certain amount of money in order to get you to read it because your time is the valuable resource." Bill Gates, Public Lecture (Nov. 1995), *quoted in* SHAPIRO, *supra* note 49, at 130.

users there as long as possible.[178] As in the offline world, producers with the financial resources to market their products, exploit synergies with corporate partners and affiliates, and produce high-quality, attention-grabbing content will likely succeed in capturing the lion's share of audience attention.[179]

Emerging Internet technologies will give commercial players a significant additional advantage in the market for user attention. Prominent among these technologies, high speed modems, digital signal compression, and broadband infrastructure make possible the transmission of high-quality video programming.[180] As a result, much of what we will see on the next generation Internet will be indistinguishable from tomorrow's high-definition television.[181] And, of course, it costs a great deal more to produce television programming than to put together a typical home web page.[182]

In short, with the growth of broadband digital communication, cyberspace will consist of at least two largely distinct communicative matrices. The realm of email, traditional web pages, and the like will continue to have negligible entry costs and foster a highly diverse plurality of expressive fora and rule regimes. But most of cyberspace, in terms of both bandwith and user attention, will bear scant resemblance to the early Internet's soap box world. Media and telecommunications conglomerates' high-production, star-studded video content will be the stuff of most cyberspace communication.[183] And, concomitantly, for most Internet travelers, most of

178. *See* SHAPIRO, *supra* note 49, at 98-99 (describing efforts of search engine companies to keep users at portal sites); *see also A CBS Internet Portal Builds In Data for Ads*, N.Y. TIMES, Oct. 6, 1999, at C14 (reporting that in order to induce Internet users to visit its new portal, CBS will expend $70 million in advertising and will give visitors chances to win cash prizes).

179. *See* Wu, supra note 10, at 1179 (concluding aptly that given the increasing cost of attracting users to one's web site, "describing today's World Wide Web as a free and open forum of equal speech is a bit delusional").

180. *See* Edward D. Horwitz, *The Ascent of Content, in* THE FUTURE OF THE ELECTRONIC MARKETPLACE 91, 96-101 (Derek Leebaert ed. 1998) [hereinafter ELECTRONIC MARKETPLACE].

181. *See* SHAPIRO, *supra* note 49, at 99-100 (discussing WebTV, a technology purchased by Microsoft in 1997, that offers basic Internet access over a television and a menu of channels accessible through a specially designed remote control); *see also* Andrew Pollack, *Feature Film to Be Produced for Release on Web*, N.Y. TIMES, Aug. 24, 1999, at C1. Our hardware gateway to cyberspace will also resemble some combination of computer, high-definition television, and digital radio. *See Is It Tellynet or Netelly? If Ever Two Media Were Meant to Wed, They are Television and the Internet*, THE ECONOMIST, Dec. 13-19, 1997, at supp. 10 (discussing NetChannel, a Web-enhanced television service that can be personalized for each viewer).

182. Production costs will not be the only factor favoring commercial players. At least for the near future it appears that broadband networks will be built with the lion's share of carrying capacity downstream to the Internet user, leaving relatively little bandwith for user-initiated video programming.

183. *See* SHAPIRO, *supra* note 49, at 181 (noting that "without the brand recognition or the advertising budget to compete with the big online players, [individuals, nonprofits, and small commercial outlets] will likely be about as prominent as the outcasts on public access cable or ham radio").

the time, the standard conditions of use for those conglomerates' networks, portals, sites, and channels will comprise the rules of the virtual road.[184]

b. Cyberanarchy Versus Liberal Democracy

As we have seen, the cyberanarchist claim depicts cyberspace as a near ideal market and equates that market with a quintessential liberal order. For cyberanarchists, cyberspace approaches the Coasean ideal of a universe of perfect competition and no transaction costs. It is a world of extensive consumer choice among existing alternatives and easy entrance to the market to create new ones. In that world, state-created law has little place. In the absence of transaction-cost barriers to collective action and private bargaining, netizens can, through ongoing negotiation or simply the choice of one rule regime over another, determine and modify entitlements to suit their local needs.[185] By definition, therefore, an untrammeled cyberspace reflects individual liberty and choice.

I have argued that cyberspace in fact falls far short of that Coasean paradise. But even if the cyberanarchists' depiction of cyberspace comports with cyberspace reality, the cyberanarchist neoliberal vision is vulnerable to attack from both the liberal and democratic components of liberal democracy. For one, the cyberanarchist claim evokes longstanding and often repeated concerns regarding the inconsistencies between markets, on one hand, and liberal democratic ideals on the other. In addition, the unregulated cyberspace that cyberanarchists envision would give rise to some of the very types of negative externalities that liberal democracy serves to minimize. I briefly consider each in turn.

i. Inconsistencies Between Markets and Liberal Democracy

Commentators have highlighted significant discrepancies between rule by market, on the one hand, and both liberal and liberal democratic rule, on the other. First, individual market preferences may represent an impoverished account not only of "what the people want," but also of what individuals want. People often express different preferences in nonmarket

184. To be certain, concentration does not necessarily mean an absence of competition. But given producers' institutional commitment to rationalizing the rules governing user access and the difficulty in combating otherwise rational consumer apathy in order to sell new standard terms, any competition between dominant cyberspace players will likely focus on price and content attractiveness rather than conditions of use. *See* Rakoff, *supra* note 153, at 1226-27; *see also* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488 (1970) (showing that producers may find it prohibitively costly to inform consumers of higher-quality product and thus may tend to settle on lower-quality, lower-price product).

185. *Cf*. Richard A. Epstein, *Holdouts, Externalities, and the Single Owner: One More Salute to Ronald Coase*, 36 J.L. & ECON. 553, 555 (1993) (contending that in a Coasean universe of zero transaction costs, "[t]he choice of legal rules . . . becomes a matter of supreme indifference" because private parties can bargain legal rules away).

contexts than they do as consumers.[186] In such instances, individuals' positions taken in settings of collective choice or in crafting personal ideals reflect individual preferences more accurately than do consumer purchases. Second, the political process, including formal deliberation, open critique, and law making, may modify individual preferences. Some argue, accordingly, that considered opinions tested in deliberative process constitute a fuller account of people's autonomous choices than do people's decisions as consumers.[187] Third, the existing matrix of legal rules, social norms, and resource distribution may play a significant role in determining consumer preferences.[188] Accordingly, in contrast to market-centered notions of consumer sovereignty, consumer preferences are necessarily endogenous to the political process. An authentic liberal democracy, therefore, cannot simply take revealed preferences as it finds them.[189] Finally, according to some theorists, the popular will can only be found in the outcomes of democratic political discourse, not in an aggregation of atomist decision making.[190] In that view, the democratic side of the liberal democratic equation assumes a more prominent position than the liberal side.

These are cogent arguments and, I would contend, well within the mainstream of liberal democratic thought. Beyond that statement, I cannot assess their validity in these several pages. My point here is simply that the cyberanarchist equation of consumer sovereignty with individual liberty and government by consent of the governed is far from uncontroversial. To the extent that the liberal democratic critique of markets holds outside of cyberspace, it applies equally to cyberanarchism.

ii. Illiberal Externalities

The cyberanarchist vision might well give rise to negative externalities that fly in the face of liberal and liberal democratic ideals. For one, a cyberanarchist universe would countenance unhindered discrimination based on race, gender, and other immutable personal characteristics. Today's largely text-based Internet makes it difficult to determine user status and therefore to discriminate on the basis of that status.[191] But the

---

186. *See* SUNSTEIN, *supra* note 87, at 14-16, 21-24.

187. *See id*. at 24.

188. *See* C. Edwin Baker, *The Media That Citizens Need*, 147 U. PA. L. REV. 317, 333 n.31 (1998) (presenting this argument in the context of liberal pluralist and republican critiques of the neoclassical model of consumer sovereignty); SUNSTEIN, *supra* note 87, at 13-31.

189. *See* SUNSTEIN, *supra* note 87, at 13-31.

190. *See* JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS: CONTRIBUTIONS TO A DISCOURSE THEORY OF LAW AND DEMOCRACY (William Rehg trans., MIT Press 1996).

191. *See* Suzanne P. Weisband et al., *Computer-Mediated Communication and Social Information: Status Salience and Status Differences*, 38 ACAD. MGMT. J. 1124, 1124 (1995) ("Many studies have found that groups that interact by computer-mediated communication . . . are less prone to domination by high-status members than are face-to-face groups."), *quoted in* Gibbons, *supra* note 2, at 520 n.304.

growth of video chat rooms,[192] digital identification,[193] and "online profiling,"[194] which may include photographs identifying the profiled user,[195] raise a nontrivial threat of such status-based exclusion from virtual communities, web sites, or even entire networks.[196] In addition, as discussed above, while today's Internet is characterized by diversity of expression, the growth of WebTV and other high-cost content production, coupled with fierce competition for user attention, may push minority voices to the margins.[197] Indeed, given the narrowcast character of Internet content, it may be that most people have even less contact with dissenting opinion in cyberspace than they do as consumers of traditional media.[198]

Finally, cyberanarchists take no account of the vast inequalities in the distribution of the resources required to gain access to cyberspace, let alone exercise meaningful choice within it. Much of the world's population has no connection to the telephone infrastructure, let alone the Internet.[199] Even within developed Western countries, Internet users are overwhelmingly white, educated, and affluent.[200] Moreover, with the spread of cable modems, high-cost content, and encrypted access, cyberspace itself may well fracture into networks with high-quality content and technology effectively reserved for the wealthy, and class B networks available for everyone else.[201] The cyberanarchist vision, based on competing rule

---

192. Internet videophones are already in use. *See* Matt Richtel, *Videophone Call-Ins on a Cable TV Channel*, N.Y. TIMES, Oct. 22, 1998, at G3.

193. *See* LESSIG, *supra* note 12, at 41 (discussing plans to deploy and build compelling incentives for individuals to use digital identification on the Internet).

194. Schwartz, *supra* note 147, at 1621-31 (detailing methods of obtaining user profile data).

195. *See Judge Rejects State's Request to Block Sale of Drivers' Photos*, N.Y. TIMES ON THE WEB (Feb. 13, 1999) <http://www.nytimes.com/library/tech/99/02/biztech/articles/14phot.html> (reporting that South Carolina judge refused to block state officials' sale of driver's license photos to a company that wants to use them in an antifraud system for businesses). The Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (1994 & Supp. II 1996), forbids states from disclosing an individual's driver's license photograph, as well as other personal information. *See id.*§ 2721(a). However, that prohibition does not apply if the disclosure falls within one of fourteen categories of permissible uses or if the state has established an "opt-out" procedure and the individual has not availed herself of the opportunity to prohibit disclosure. *See id.* § 2721(b).

196. *See* Steve Lohr, *Seizing the Initiative on Privacy: On-Line Industry Presses Its Case for Self-Regulation*, N.Y. TIMES, Oct. 11, 1999, at C1, C8 (reporting concerns regarding "on-line profiling" and "digital red-lining").

197. *See supra* notes 177-83. For an illuminating "dystopic commodified vision" of future cyberspace, see Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J.L. & COM. 509, 521-22 (1996).

198. *See* SHAPIRO, *supra* note 49, at 124-32 (discussing "freedom from speech").

199. *See* Walker & Akdeniz, *supra* note 48, at 501.

200. *See* Gibbons, *supra* note 2, at 497; *see also* NATIONAL TELECOMMS. AND INFO. ADMIN., US. DEP'T OF COMMERCE, FALLING THROUGH THE NET: DEFINING THE DIGITAL DIVIDE viii (July 1999), *available at* <http://www.ntia.doc.gov/ntiahome/digitaldivide> [hereinafter DIGITAL DIVIDE] (finding significant disparities in Internet access across wealth, ethnic, and geographic lines (but not gender) in the United States).

201. *See* Saskia Sassen, *On the Internet and Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 545, 551-54 (1998) (discussing emergent "cyber-segmentation").

regimes with the right and technological capacity to exclude unwanted or nonpaying users, would inevitably exacerbate these inequalities.

D. Summary

The cyberian liberal perfectionist claim advances a tripartite challenge to representative liberal democracy: cyberpopulism, cybersyndicalism, and cyberanarchism. Much of that claim boils down to the descriptive argument that cyberspace offers an unprecedented opportunity for realizing a neoliberal order of unanimous consent through social norms, buying off hold-outs, individual exchange, and frictionless mobility among rule regimes. Building upon that descriptive argument, cyberians then make a normative claim. A neoliberal order, they assert, more fully expresses the liberal democratic ideals of individual liberty and government by consent of the governed than does collective decision making through elected representatives within a framework of constitutional protections for minorities and dissenters.

I have sought in this Part to refute the cyberians' descriptive arguments and to cast doubt on their normative claims. I have shown that cyberspace rule making falls far short of a neoliberal regime of individual choice. I have also questioned whether such a regime—even in its ideal form—would truly realize liberal and liberal democratic principles.

Equally important is what I do not contend. First, I do not contend that our current political institutions represent the ultimate fruition of liberal democratic ideals. I have sought simply to refute the cyberian claim of liberal perfection, leaving for further study a comparative analysis of the relative efficacies of cyberspace versus governmental rule making.[202] Second, I do not call for state intervention whenever cyberspace might stray from or even prove inimical to liberal democratic ideals. Indeed, as I will presently discuss, the liberal democratic state must leave considerable (although not unlimited) room for individual and associative autonomy. That is so even when private actors promote illiberal results.

III
THE CYBERIAN CLAIM OF COMMUNITY AUTONOMY

Over and above their claim of liberal perfection, cyberians base their argument for presumptive cyberspace self-governance in liberal principles of community autonomy.[203] That claim stands independently of any suppositions regarding the consensual character of cyberspace rule making. It looks rather to the nature of the liberal nation-state. Political liberalism, it

202. Significantly, such a study would have to address potential, as well as current, advancement of liberal democratic ideals; the Internet will revolutionize government administration, not merely provide a "bottom-up" alternative to state regulation.

203. *See supra* notes 21-22 and accompanying text.

insists, must make considerable room for community self-governance. The liberal state must accord religious communities, insular ethnic minorities, fraternal organizations, and other private associations considerable latitude to govern themselves, even in ways that run contrary to liberal values. So must the state give way before virtual community self-governance. Johnson and Post put it categorically:

> If the sysops and users who collectively inhabit and control a particular area of the Net want to establish special rules to govern conduct there, and if that rule set does not fundamentally impinge upon the vital interests of others who never visit this new space, then the law of sovereigns in the physical world should defer to this new form of self-government.[204]

The question of associational self-governance—and especially the question of how the liberal state should respond to separatist or illiberal communities and associations—hits a fault line in liberal democratic theory and practice.[205] It is helpful in this regard to distinguish between two sorts of self-rule claims. Strong self-rule claims are generally propounded by ethnic or religious groups who seek to establish a geographically distinct local government to live exclusively among themselves and to pursue without fetter their own idiosyncratic practices, culture, and vision of the good. A strong self-rule claim thus insists upon community autonomy in the governance of a broad panoply of social and political institutions, including education, property, criminal and civil legislation, adjudication, and taxation. A weak self-rule claim is one of partial associative autonomy. Typical examples involve civic association by-laws, church or club membership requirements, bowling league rules, and professional standards. In each case persons seek autonomy from state interference in the determination of norms governing a discrete set of mutual commitments. In contrast to strong self-rule claims, such claims do not entail a profound, geographic separation from the rest of society. They involve a scope of activity of far lesser dimension than that generally associated with full-scale local government.

Cyberians imbued with the culture of the early Internet phrase their community autonomy claims in terms approximating those of strong self-rule. For them, cyberspace offers a comprehensive culture and value system, one highly distinct from the offline world.[206] It also offers possibilities for many of the attributes of government, including rule making, adjudication, education, and punishment.[207] More plausibly, though,

---

204. Johnson & Post, *Law and Borders*, *supra* note 2, at 1393.

205. For an illuminating discussion, see WILL KYMLICKA, MULTICULTURAL CITIZENSHIP: A LIBERAL THEORY OF MINORITY RIGHTS, 181-92 (1995).

206. *See* Barlow, *supra* note 1; Johnson & Post, *Law and Borders*, *supra* note 2, at 1387-90.

207. *See* Johnson & Post, *Law and Borders*, *supra* note 2, at 1387-90.

arguments for cyberspace self-governance fall closer to the category of weak self-rule claims. Netizens are also citizens. They eat, work, sleep, pay taxes, vote, and go to school in the real world.[208] For the most part, and this is increasingly so as the multitudes discover the Internet, cyberspace activity and virtual community make up only a fraction of their interactions, transactions, and commitments. Cyberians, accordingly, seek autonomy for particular, discrete association, for rules governing the part of their lives and activity that concerns that association.

In any event, with the partial exception of Indian tribes, American law has been generally unaccommodating to strong self-rule claims.[209] Statutory prohibitions of various member practices and judicial invocation of the Establishment Clause have consistently thwarted efforts by Mormon, Oneida, Rajneesh, Satmar Chasidic, and other such communities to achieve significant powers of self-governance.[210] Commentators share this skepticism about granting significant autonomy to self-defining, predominantly illiberal groups.[211] Some theorists stress the primacy of democratic liberal values. John Rawls argues, for example: "The adult members of families and other associations are equal citizens first. . . . No institution or association in which they are involved can violate their rights as citizens."[212] Others view the inclusion of cultural and religious minorities within the political community as a requisite of liberal democracy. As Christopher Eisgruber has recently propounded, "[A]ssimilation, far from being the enemy of diversity, is perhaps the only means for reconciling this country's commitment to pluralism with its commitment to justice."[213]

---

208. As Larry Lessig colorfully puts it:

> While they are in that place, cyberspace, they are also here. They are at a terminal screen, eating chips, ignoring the phone. They are downstairs on the computer, late at night, while their husbands are asleep. They are at work, or at cyber cafes, or in a computer lab. They live this life there, while here. And then at some point in the day, they jack out, and are only here. They step up from the machine, in a bit of a daze; they turn around. They have returned.

Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1403 (1996).

209. *See* Mark D. Rosen, *The Outer Limits of Community Self-Governance in Residential Associations, Municipalities, and Indian Country: A Liberal Theory*, 84 VA. L. REV. 1053, 1056-59 (1998).

210. *See id.*

211. *See id.* at 1059-61 (summarizing the skeptical view, and ultimately disagreeing with it); *see also* KYMLICKA, *supra* note 205, at 167 (complaining that "contemporary liberals . . . have become more reluctant to impose liberalism on foreign countries, but more willing to impose liberalism on national minorities").

212. Rawls, *supra* note 66, at 791.

213. Christopher L. Eisgruber, *The Constitutional Value of Assimilation*, 96 COLUM. L. REV. 87, 103 (1996). Rawls also supports this argument, suggesting that common citizenship will benefit minorities by promoting the political virtues of "reasonableness and a sense of fairness, a spirit of compromise and a readiness to meet others halfway." John Rawls, *The Idea of an Overlapping Consensus*, 7 OXFORD J. LEGAL STUD. 1, 21 (1987).

There are commentators who see granting group autonomy as intrinsic to political liberalism.[214] But even they would limit autonomy to discrete geographically and culturally insular groups, such as the Amish or the Satmar Chasids, for whom self-rule is an integral part of their pursuit of deeply-held values and who do not impose significant externalities on their neighbors.[215] There are two principal reasons why even supporters of group autonomy would place such sharp constraints on strong self-rule. First, as researchers of close-knit groups have often noted, such groups exhibit a marked tendency to impose externalities on outsiders.[216] Geographic and cultural isolation reduce opportunities for contact with outsiders and thus might lessen the chances that a group will impose harmful externalities. Second, the proliferation of otherwise benign separatist communities can lead to a balkanization of society that undermines liberal rule. Liberal democracy requires citizens to have a relatively high level of self-restraint and mutual recognition.[217] Rampant separatism would "undermine the degree of social cohesion necessary to sustain an 'enduring and secure democratic regime.'"[218]

The cyberian strong self-rule claim runs squarely up against these liberal barriers to such claims. Even taking the most favorable view of community self-governance, virtual communities, as noted above, are insufficiently insular and insufficiently free from imposing harmful externalities to warrant strong self-rule. Given the growing numbers of persons involved in cyberspace activity, strong self-rule—if we are to take that claim seriously—might also pose a destabilizing threat to the civic identity and broad social unity required to support the liberal state.

Indeed, here we see yet another deleterious effect of cyberspace mobility. Cyberians tout the benefits of mobility, both among cyberspace rule regimes and from territorial rule to cyberspace self-governance. They argue that regulatory arbitrage—allowing individuals maximum freedom to exit rule regimes not to their liking and to choose new regimes that suit their preferences—yields positive welfare and collective rule benefits across communities.[219] Following the work of Charles Tiebout and his progeny, cyberians contend that intercommunity mobility improves the allocation of public goods by enabling individuals with similar tastes for local public goods to sort themselves into groups.[220] Similarly, they see

---

214. *See, e.g.*, Abner S. Greene, Kiryas Joel *and Two Mistakes About Equality*, 96 COLUM. L. REV. 1, 13-16 (1996); Rosen, *supra* note 209, at 1089-1106.

215. *See, e.g.*, Greene, *supra* note 214, at 49-51; Rosen, *supra* note 209, at 1095-97.

216. *See, e.g.*, Posner, *supra* note 124, at 143-44.

217. *See* KYMLICKA, *supra* note 205, at 174-76, 192.

218. Rosen, *supra* note 209, at 1097 (quoting JOHN RAWLS, POLITICAL LIBERALISM 38 (1993)).

219. *See supra* text accompanying notes 140-42.

220. *See* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). For surveys of literature addressing Tiebout's hypothesis, *see, e.g.*, MUELLER, *supra* note 98, at 149-76.

mobility as a vehicle for bringing about collective rule regimes built upon social consensus since mobility enables persons of like preferences and opinions to associate with one another and distance themselves from those with whom they disagree.

But mobility itself can have significant negative externalities. As Dennis Mueller notes: "The family leaving community A to find better schools decreases A's tax base and thereby imposes costs on those left behind who must maintain the schools that were built on the assumption that this family would pay taxes."[221] Similarly, those who exit territorial liberal society eschew (to the extent they can) the financial and political burdens of maintaining and improving the institutions of that society. They also undermine the sense of solidarity, mutual recognition, and social commitment that are themselves collective goods central to a liberal society. Finally, while sorting individuals into isolated, self-governing, like-minded groups may bring about greater overall social consensus (to the extent those groups do not impose harmful externalities on others), that, too, is a mixed blessing in political liberal theory. The liberal state, many commentators assert, depends upon robust debate among contrary views.[222] It is only through interaction and deliberation with those of opposing ideas and perspectives that citizens can test their preferences and produce better collective decisions.[223]

In short, the cyberian strong self-rule claim fails to meet the criteria that even liberal supporters of strong community autonomy lay down for recognizing community self-governance. Given the intermingled and porous nature of virtual communities, the strong self-rule of such communities would likely impose significant negative externalities on outsiders. At the same time, the proliferation of strongly autonomous virtual communities would tend to eat at the foundations of the territorial liberal state. At least from the point of view of the liberal state, therefore, the cyberian strong self-rule claim must be rejected.

The cyberian weak self-rule claim is somewhat more tenable, but this is largely because it has far less bite. Traditional liberalism not only tolerates, but also encourages semi-autonomous civil association. Indeed, civil association, of which cyberspace is a part, plays a central constitutive role in the liberal state. Representative government best reflects the consent of the governed through interaction with an alert and politically competent

---

For references to Tiebout in the cyberspace literature, see Burk, *supra* note 17, at 962-69; Johnson & Post, *Law and Borders*, *supra* note 2, at 1399 n.102.

221. Mueller, *supra* note 101, at 1426.

222. *See, e.g.*, Harper & Row, Publishers Inc. v. Nation Enters., 471 U.S. 539, 605 (1985) (Brennan, J., dissenting) (emphasizing that "the robust debate of public issues" is the "essence of self-government"); *see also* HOLMES, *supra* note 32, at 179-81 (discussing John Stuart Mills' thesis that liberal state requires a robust exchange of view.).

223. *See* SUNSTEIN, *supra* note 87, at 186-87.

citizenry. The discursive fora of civil society can help engender the independent thought, self-direction, and political acumen required to pass judgment on elected officials and influence political agendas.[224] Even civil associations that espouse or embody illiberal views can be seen ultimately to contribute to a liberal polity by challenging majority or government-imposed orthodoxy.[225]

The generation of norms through civil association can also be seen as part of the matrix of political decision making. Social norms may have a profound influence on our individual and collective understandings of reality.[226] Accordingly, the determination and contesting of norms in the multiple discursive fora of civil society carries a socio-political valence that at times rivals that of state-enunciated law. For the state overly to burden such constitutive activity would be to undermine "democratic culture"—the political awareness, mutual recognition, and social accountability—upon which a vibrant representative democracy depends.[227]

Yet, while the importance of autonomous civil association cautions against stifling, heavy-handed state intervention, neither does it obviate or detract from the desirability for state regulation in certain circumstances. Civil association activities and rules that impose negative externalities, violate public policy, or result from information asymmetries and other forms of market failure are commonly the subject of ameliorative state action.[228] As trenchant critics of cyberspace independence reiterate, cyberspace activity and virtual communities are hardly free from such problems.[229] Indeed, cyberspace is highly porous: Virtual defamation may destroy territorial reputations, copyright infringement on the Internet may undermine creative incentives offline, cyberspace hate speech may inspire physical violence, and fraud in web site sales transactions may deprive real persons of real money expended for real goods. Accordingly, while from the point of view of the liberal state, virtual association might be entitled to the same degree of quasi-autonomy generally accorded to territorial association, it certainly is entitled to no more.

---

224. *See* DENNIS F. THOMPSON, THE DEMOCRATIC CITIZEN 60-62 (1970).

225. *See* Julian N. Eule & Jonathan D. Varat, *Transporting First Amendment Norms to the Private Sector: With Every Wish There Comes a Curse*, 45 UCLA L. REV. 1537, 1617-27 (1998).

226. *See* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903 (1996).

227. *See* Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 342-344 (1996). The term "democratic culture" is from ROBERT A. DAHL, A PREFACE TO ECONOMIC DEMOCRACY 30 (1985).

228. *See, e.g.*, Dale v. Boy Scouts of Am., 706 A.2d 270, 283 (N.J. Super. Ct. App. Div. 1998), *cert. granted*, No. 99-699, 2000 U.S. Lexis 509 (Jan. 14, 2000) ("It is well-settled that courts will invalidate an expulsion from a private organization when the expulsion is based on reasons that violate public policy." (quoting Rutledge v. Gulian, 459 A.2d 680 (N.J. Sup. Ct. 1983)), *aff'd*, 734 A.2d 1196 (N.J. 1999))).

229. *See* Lemley, *supra* note 19, at 1277-81 (noting ubiquitous spillover effects from cyberspace activity to the offline world).

IV
STATE REGULATION

My critique of the cyberian claim of liberal perfection has highlighted the contradictions between the cyberpopulist, cybersyndicalist, and cyberanarchist visions on the one hand, and the liberal democratic ideals, on the other. My assessment of the cyberian claim for community autonomy has sought to counter the notion that cyberspace self-rule has any special purchase within political liberalism. As I have sought to emphasize, however, the failings of the cyberian claims do not necessarily call for the systematic corrective intervention of the liberal democratic state. Indeed, like other civil associations, virtual community and discursive interaction are generally supportive of the democratic culture upon which the liberal state depends. It is thus in the interest of territorial liberalism that state intervention, at least in the associative and discursive fora of cyberspace (as opposed simply to sites for electronic commerce), be narrowly drawn.

In this Part, I will consider a number of areas in which state intervention in cyberspace activity might nevertheless be warranted. In keeping with my focus on the cyberians' political claim, I will limit myself to a narrow universe of possibilities. I will examine several instances in which cyberspace activity might threaten liberal democratic values, including through status discrimination, content discrimination, the appropriation of personal information, and the maintenance of vast inequalities in the resources required for the effective use of Internet networks and content. In each instance I will ask to what extent the state should intervene in order to protect liberal democratic values.

A note of caution before I do so: as I have suggested above, a complete assessment of the desirability of state intervention would need to examine the state side of the equation as well as the cyberspace side. It would need to ask not only whether cyberspace fails to protect liberal democratic values, but also whether, even in those areas in which state intervention seems warranted, the state can be expected to act effectively in the interest of oppressed individuals and minorities. Political liberalism already contains within it a healthy skepticism of the state. Much liberal doctrine is designed to cabin state power and to prevent majorities from using state institutions to oppress minorities. But in the areas I will discuss, liberalism also requires an activist state. The concentration of private power and majority prejudice, self-regard, or indifference in civil society can also deprive minorities of the incidents and requisites of liberal citizenship.

A public choice theorist might argue, however, that the powerful will tend to capture state institutions and thus that government cannot be relied upon to protect the weak. Or the theorist might argue that state agencies are institutionally inept and thus are unable effectively to carry out a defense

of liberal democratic values. With respect to cyberspace, this argument, at its core, is that the failings of cyberspace must be viewed in comparison to the gross imperfections of the liberal democratic state.

In principle, this is a point well taken. In a world of second-best alternatives, identifying the failings of one alternative does not necessarily mean that another is preferable. At bottom, however, I join with many other commentators in rejecting the radical, determinist skepticism of state competence and integrity.[230] It should not be forgotten, moreover, that digital communication and information storage can also dramatically improve the efficacy of state decision making and regulation.[231] The Internet might also serve to broaden public input into state policy.[232] A further investigation of the competency and integrity of the liberal state in the digital age is beyond the scope of this Article. In this Part, I will rest on the assumptions of reasonably sufficient state competence and integrity that regularly justify state intervention in the offline world.

A. Status Discrimination

Status discrimination is endemic in cyberspace. Numerous listservs, newsgroups, and other cyberfora restrict access based on a person's professional standing, occupation, knowledge, or affiliation. The Cyberprof listserv, for example, is generally restricted to professors who teach courses related to cyberlaw. Similarly, nonlawyers cannot generally gain access to Counsel Connect and none but select Internet pundits may join any of a number of "virtual gated communities" that screen out uninvited hoi polloi.[233]

Such discrimination can perform a useful function. It can serve to ensure that discussants share a common language and expertise. Copyright lawyers may wish to dissect the Digital Millennium Copyright Act without having to read and delete messages from Internet hackers ranting that information must be free or even from general counsel who do not know the difference between fair use and fair play. Status discrimination can also

---

230. *See, e.g.*, DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE 8 (1991) (rejecting the "deep pessimism of some portions of the public choice literature"); MARGARET JANE RADIN, CONTESTED COMMODITIES 214-23 (1996) (presenting a cogent critique, from a Deweyan perspective, of public choice theory's reductive description of democracy as a marketplace of self-interested profit maximizers); Eric A. Posner, *Law, Economics, and Inefficient Norms*, 144 U. PENN. L. REV. 1697, 1703 (1996) (noting that "crude" public choice arguments "do not account for the complicated motives of legislators, the institutional constraints on legislation, or the numerous statutes that seem to improve on the common law") (footnote omitted).

231. *See* Perritt, *supra* note 19, at 435-36 (noting that the Internet can be used to increase government transparency and strengthen the rule of law).

232. *See* SUNSTEIN, *supra* note 87, at 183-85. Sunstein also notes the potential dangers of reflexive rule by Internet public opinion poll. *See id.* at 185-87.

233. *See* Margie Wylie, *Virtual Snobbery: If You're Not on the List, You Don't Get into Some Net Areas*, NEW ORLEANS TIMES-PICAYUNE, Jan. 14, 1999, at E1.

serve as a proxy for screening out off-topic messages. Web designers may wish to canvass sources for the latest enhanced graphics, and postmodern artists may wish to exchange ideas about artistic appropriation, without unsolicited monitions from client-hungry copyright lawyers. Finally, status discrimination can enhance civility. People who know each other offline or who belong to the same close-knit professional or religious associations are less likely to engage in online affront than are anonymous strangers. Status discrimination, in short, can make the difference between a discussion that is informative and meaningful for its participants and one that serves no useful purpose for those who initiated the discussion.

Of course, just as status discrimination can center on expertise, occupation, and association, so can it focus on race, gender, physical disability, age, sexual orientation, or other immutable physical characteristics. Given the limitations of current Internet technology, such status discrimination has thus far been relatively uncommon in cyberspace.[234] The vast majority of virtual discussion takes place through the exchange of text, and those who wish to participate without revealing their offline identity may generally do so.[235] As the Internet develops, however, text-based anonymity will increasingly become a thing of the past. Software such as CU-SeeMe makes possible Internet video chat, a phenomenon that can be expected rapidly to proliferate as high-speed modems and increased network bandwidth enable high-quality video conversation.[236] Moreover, "online profiling" of Internet users, digital identification, and the possible availability of digitized driver's license photographs and other visual identification will enable web site operators and other Internet players to determine users' race, gender, age, and other physical characteristics.[237] As a result of these developments, Internet technology will no longer constrain status-based discrimination. Whether for economic motives or because of simple prejudice, cyberspace redlining may become increasingly prevalent.

As Eugene Volokh has aptly noted, cyberspace discrimination based on race, gender, or other immutable characteristics may, in certain

---

234. *But see* U.S. Department of Education, Office for Civil Rights, Docket No. 09-93-2202, Letter from John E. Palomino, Regional Civil Rights Director to Robert F. Agrella, President, Santa Rosa Junior College, June 23, 1994, at 4 (conveying that the "OCR anticipates finding that the College violated Title IX [of the Educational Amendments of 1972] when it established . . . gender segregated computer bulletin board conferences").

235. As the *New Yorker* cartoon depicting two dogs facing a computer screen puts it, "'On the Internet, no one knows you're a dog.'" Peter Steiner, cartoon, NEW YORKER, July 5, 1993, at 61. In *ACLU v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997), a federal district court held unconstitutional, on First Amendment grounds, a state law prohibiting anonymous and pseudonymous electronic communication. It is highly unlikely that similar prohibitions by nonstate entities, such as Internet service providers, would meet a similar fate.

236. *See* Jeri Clausing, *New Data Pipeline Holds Promise of a Better Internet*, N.Y. TIMES, Mar. 1, 1999, at C1.

237. *See supra* notes 192-96; *see also* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 576-77 (1998).

circumstances, be no less conducive to effective online discussion than is discrimination based on profession or expertise:

> Blacks might want to argue how they as blacks should react to Louis Farrakhan; whites might want to debate how whites should deal with the problems of police racism; men or women might want to share thoughts on why their own sex is superior. In each situation, people might specifically want to hear the voices of their fellow group members (whatever they have to say) and not of others (no matter how sympathetic to the group they might be).[238]

Yet despite its efficacy in certain discursive settings, race, gender, and other such discrimination can also grossly contradict liberal values. Much depends on historical and social context. If the Hopi Indian tribe set up a network of email listserv discussion groups exclusively for Hopi Indians, most non-Hopis would view that as a legitimate effort to preserve the beleaguered group identity of an insular ethnic group.[239] On the other hand, if Rotary International established an all-white, all-Protestant, or all-male virtual network, that, in the context of American history, culture, and power relations, would properly be viewed as an instance of pernicious subordination.[240]

The invidious nature of status discrimination also depends on extent. If widespread across multiple spheres of activity, discrimination based on race, gender, sexual orientation, age, or disability can transform what is generally "a morally irrelevant characteristic into a pervasive source of social disadvantage."[241] Systemic discrimination on the basis of such characteristics deprives large groups of people of the education, employment, political influence, and economic opportunity required for self-advancement and basic participation as citizens in a democratic society.[242] Somewhat more symbolically, but ultimately no less tangibly,

---

238. Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harrassment, and Sex*, 1996 U. CHI. LEGAL FORUM 377, 391.

239. *Cf*. KYMLICKA, *supra* note 205, at 108-15 (canvassing arguments for special rights for national minorities in order to rectify political and cultural disadvantages and thus to further the liberal principle of equality); *id.* at 121 (discussing argument that preserving cultural diversity has value for the liberal polity as a whole); *see also* Jonathan Lesser, *For Indian Nations, Virtual Trade Routes*, N.Y. TIMES, Oct. 14, 1999, at D1 (reporting on efforts to rekindle trade among Indian tribes through the use of an electronic bulletin board closed to non-Indians).

240. Rotary International is an organization of business persons and professionals, founded in 1905, with chapters in numerous communities in the United States and other countries. *See Rotary International* (visited Dec. 25, 1999) <http://www.rotary.org>. In *Board of Directors of Rotary Int'l v. Rotary Club of Duarte*, 481 U.S. 537 (1987), the Supreme Court held that a California antidiscrimination law that required California Rotary Clubs to admit women did not violate Rotary International's First Amendment right of association and that Rotary International could not expel a California Rotary Club for admitting women. I am told that Rotary International no longer discriminates against women, and I do not mean to suggest that the organization would actually establish a network that discriminates on the base of race, gender or religion.

241. SUNSTEIN, *supra* note 87, at 165.

242. *See id.* at 163.

such status discrimination creates a stigma of second-class citizenship, placing its victims under the constant threat of domination at the hands of another.[243]

For those reasons, numerous federal and state laws prohibit discrimination based on race, gender, age, disability, and other factors in a broad range of contexts. Antidiscrimination laws typically apply in the workplace, the housing market, and "places of public accommodation,"[244] which include hotels, restaurants, theaters, and other businesses and entertainment facilities of a kind generally open to the public. Private clubs,[245] parades,[246] and associations such as the Boy Scouts and Jaycees have also been held to be places of public accommodation.[247] Discrimination in such contexts can cause considerable personal discomfort to its victims. The hotel or restaurant that excludes may be the only one in town. Such discrimination can also deprive victims of the tools for self-realization, isolate them from sources of political power, deprive them of economic opportunity, and brand them as second-class citizens.

Cyberfora and networks that are generally open to the public should similarly be seen as "places of public accommodation," whether by statutory construction or legislative extension.[248] Cyberspace is fast becoming a central source of information, opinion, and entertainment. The discursive arenas of cyberspace also increasingly serve as important avenues for social contact and market transaction, just as they present vital opportunities to make one's voice heard and to seek to influence others.[249] Pervasive discrimination in cyberspace would cause no less deprivation than does discrimination in places of public accommodation offline. As cyberspace assumes an increasingly greater part in public discourse, civil association, social intercourse, cultural expression, and market transaction, the effects

---

243. *See* PETTIT, *supra* note 32, at 70-73.

244. *See, e.g.*, Civil Rights Act of 1964, 42 U.S.C. § 2000a (1994); CAL. CIV. CODE § 51.5 (West 1982 & Supp. 1999); 775 ILL. COMP. STAT. ANN. 5/5-102 (West 1993 & Supp. 1999); MASS. GEN. LAWS ANN. ch. 272, § 92A (West 1990 & Supp. 1999); MO. ANN. STAT. § 213.065 (West Supp. 1999); N.J. STAT. ANN. § 10:5-1 to 10:5-42 (West 1993 & Supp. 1999); N.Y. CIV. RIGHTS LAW § 40 (McKinney 1992 & Supp. 1999).

245. *See* New York State Club Ass'n v. City of New York, 487 U.S. 1 (1988).

246. *See* Hurley v. Irish-American Gay, Lesbian and Bisexual Group, 515 U.S. 557 (1995).

247. *See* Roberts v. United States Jaycees, 468 U.S. 609 (1984) (holding that the Jaycees is a "public accommodation" under Minnesota Human Rights Act); v. Boy Scouts of Am., 706 A.2d 270 (N.J. Super. Ct. App. Div. 1998), *cert. granted*, No. 99-699, 2000 U.S. Lexis 509 (Jan. 14, 2000) (holding that the Boy Scouts of America is a "place of public accommodation" under New Jersey's law against discrimination), *aff'd*, 734 A.2d 1196 (N.J. 1999). *But see* Welsh v. Boy Scouts of Am., 993 F.2d 1267 (7th Cir. 1993) (holding that the Boy Scouts of America is not a place of public accommodation under Title II of the Civil Rights Act of 1964).

248. For an illuminating discussion of whether existing public accommodation statutes might pertain to cyberspace, see Volokh, *supra* note 238, at 390-97.

249. Significantly in that regard, a recent Department of Commerce study found that persons of color are much more likely than whites to use the Internet to look for a job. DIGITAL DIVIDE, *supra* note 200, at 40.

of virtual discrimination would flood into real space. They would work a fundamental impairment not only of "netizenship," but also of citizenship in territorial polities.

Cyberians might contend that antidiscrimination regulation is unnecessary in cyberspace. They might argue, first, that unlike a black family denied lodging in a small town motel, Internet users enjoy an abundance of choice. A person who is excluded from one virtual forum, for whatever reason, can always find a suitable substitute in which she will be accepted. A whites-only listserv or an Internet service provider that refuses to sell access to known homosexuals will be one discrete option among a multitude of highly diverse virtual communities. Many virtual communities are exclusive. After all, borders are what make a community. But many cyberfora are not exclusive, and even those that are exclude on the basis of widely varying criteria. Surely the excluded netizen, cyberians would contend, can easily find another suitable site. Even if she cannot, given low entry and communication costs, she could readily set up a new one. In sum, cyberians might argue, even if directed against subordinated offline groups, virtual discrimination lacks the sting, the insurmountable deprivation, of its offline analogue.

As I have discussed, however, substitute fora may be considerably less plentiful than cyberians assume. And the more pervasive the discrimination against a particular group, the more difficult it will be for members of that group to find a suitable alternative. The availability of suitable alternatives would substantially diminish even further if discrimination occurs at the network level, where Internet service providers or groups of discussion groups discriminate, or at the carrier level, where entities that carry Internet communication signals discriminate. That possibility, it bears emphasizing, is far from remote. Concerns that carriers were engaging in redlining led Congress, as part of the Telecommunications Act of 1996,[250] to prohibit racial, ethnic, or gender discrimination in the provision of telecommunications service.

Of course, cyberspace also contains structural disincentives to discriminate. Commercial players, including carriers and commercial

---

250. Pub. L. No. 104-104, § 104, 110 Stat. 56, 86; *see also* Angela J. Campbell, *Universal Service Provisions: The "Ugly Duckling" of the 1996 Act*, 29 CONN. L. REV. 187, 196 (1996) (describing those antidiscrimination provisions and their background). Somewhat more speculatively, the constraining effects of discrimination may also be exacerbated by secondary discrimination. In addition to refusing to carry messages from end users of a certain status, a network or telecommunications carrier might also deny interconnection to other networks and carriers that fail to join in such discrimination. Since cyberspace messages must travel across numerous interconnected carriers in order to connect the parties to a communication, such third-party, secondary discrimination could severely restrict user access, especially if widespread or conducted by entities with market power. For a discussion of third-party discrimination in the context of telecommunications common carrier regulation, see Eli M. Noam, *Will Universal Service and Common Carriage Survive the Telecommunications Act of 1996?*, 97 COLUM. L. REV. 955, 973-75 (1997).

operators of networks, virtual communities, discussion groups, and web sites, lose the business of those whom they exclude. But if past experience is a guide, and there is no reason to think that cyberspace would prove any different in this regard, markets produce discrimination no less than they reduce it.[251] If sufficient numbers of prospective customers would choose a virtual network or site that discriminates against a particular group over one that does not, then network and site operators will have a greater incentive to discriminate than to allow that group access. The same result will obtain when network or site operators view ethnicity or gender as rough proxies for customer trustworthiness and buying power.[252]

Significantly, moreover, widespread discrimination in cyberspace may cause intolerable harm even if it is not so pervasive as to preclude victims from finding alternative networks and sites. Discrimination is not a discrete act with discrete consequences. Rather it can be laden with symbolic potency. It can be a public statement about the presumed inferiority of a minority group. Given the global, instantaneous nature of cyberspace communication, that statement—the fact that many regard a particular group as undesirable—is all the more likely to become common knowledge. It will fuel a common awareness that the subjugated group enjoys access to the discursive foundations of civil society only at the leave of the powerful.[253]

That common awareness in turn will tend to relegate the group to the status of second-class citizenship. Equal citizenship derives not just from the possibility of finding alternative sources for the goods from which a group is deprived. Rather it comprises a subjective and intersubjective aspect, a shared knowledge that citizens are entitled to access as a matter of right.[254] Pervasive virtual discrimination on the basis of race, gender, or other such status may thus work a fundamental deprivation of the incidents of liberal citizenship even if nondiscriminatory fora are readily available.

In sum, status discrimination in cyberspace may be inimical to liberal principles of equal citizenship, but it may also be central to effective and meaningful discussion. How are we to resolve this tension? Case law regarding private associations' discriminatory membership requirements is instructive.[255] In a number of instances, private associations have brought First Amendment challenges against public accommodation statutes that forbid organizations from excluding prospective members on the basis of

---

251. *See* SUNSTEIN, *supra* note 87, at 151-57.

252. *See id*. at 155-57 (discussing racial discrimination as perceived proxy for market considerations).

253. *See* PETTIT, *supra* note 32, at 70-73.

254. *See id*.

255. *See generally* Note, *State Power and Discrimination by Private Clubs: First Amendment Protection for Nonexpressive Associations*, 104 HARV. L. REV. 1835 (1991). For an insightful discussion of that case law as it might pertain in cyberspace, see Volokh, *supra* note 238, at 390-97.

race, gender, and other such status. The First Amendment rights of free speech and association guarantee the right of individuals to form private associations to advocate their views, including views favoring status discrimination, and to exclude persons who do not share such views.[256] The Supreme Court has held, however, that immutable attributes cannot serve as an automatic proxy for viewpoint.[257] Rather, an organization has no First Amendment right to discriminate (at least on the basis of gender and, presumably, other suspect classifications such as race and national origin) unless it can "show that it is organized for specific expressive purposes and that it will not be able to advocate its desired viewpoints nearly as effectively if it cannot confine its membership to those who share [particular characteristics]."[258]

Applied literally to cyberspace, that rule would deprive the vast majority of virtual communities of First Amendment protection against public accommodation statutes. Virtual fora are fundamentally concerned with expression and thus should have little problem qualifying as organizations "organized for specific expressive purposes." And some virtual fora—probably more web sites than discussion groups—are organized to advocate a viewpoint to others. But most are simply designed to facilitate an internal exchange of ideas among discussants, not to try to convince or inform the public at large. Likewise, discussants in virtual fora that would exclude on the basis of immutable characteristics would generally do so not because inclusion would impair advocacy, but because virtual discussants want to carry on their conversation only with persons whom they perceive to be fundamentally like themselves.

Yet despite the Supreme Court's apparent focus on advocacy to outsiders, status discrimination for purposes of facilitating intragroup discussion should not face a blanket prohibition. As noted above, some conversations lose their essential purpose and meaning unless limited to persons of a particular group. In such instances, the participants' interest in discriminating (and the allied public interest in promoting discursive

256. *See* Hurley v. Irish-American Gay, Lesbian and Bisexual Group, 515 U.S. 557 (1995).

257. *See* Roberts v. United States Jaycees, 468 U.S. 609, 627-28 (1984).

258. New York State Club Assn. v. City of New York, 487 U.S. 1, 13 (1988). The Court has also recognized the possibility that members of a small, distinctly private organization might be able to discriminate on the basis of the right of intimate association. *See* Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 545 (1987) (stating that "the First Amendment [right of association] protects those relationships, including family relationships, that presuppose 'deep attachments and commitments to the necessarily few other individuals with whom one shares not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's life'") (quoting *Roberts*, 468 U.S. at 619-20); *Roberts*, 468 U.S. at 620 (stating that only relationships arising within the family or small, private organizations have the "sorts of qualities [that] are likely to reflect the considerations that have led to an understanding of freedom of association as an intrinsic element of personal liberty"). As yet, however, the Court has not accorded protection on this basis to any private club or association engaged in status discrimination. *See* Note, *supra* note 255, at 1842.

expression and association) should prevail over the interest in preventing invidious status discrimination.

In other cases, however, the participants' desire to exclude bears no reasonable relation to the topic of discussion. In that event, the discriminating virtual community should be viewed no differently than a nonexpressive private club. Virtual discussants might wish generally to associate and converse online with those of their own race or gender, just as members of the Rotary Club or Jaycees might prefer to associate and converse offline with persons who share particular attributes. But in that case, the desire to discriminate has insufficient nexus to the public interest in conducing meaningful and effective expression to override the broad harmful effects of such discrimination. In sum, so long as the virtual community is of sufficient permanence and openness to new members to be more than a distinctly private conversation, and so long as the attribute discrimination in question is particularly egregious in light of its historical and social context, the liberal state should act to prevent it.[259]

The same will be true with respect to networks of virtual fora. An Internet service provider who wishes to establish a network of white supremacy discussion groups should be entitled to exclude nonwhites from the network to the same extent that an offline association dedicated to advocating white supremacy should be entitled to exclude nonwhites from membership. An Internet service provider who wishes to establish a network of all-white discussion groups on topics ranging from gardening to pit bulls should not be permitted to do so.

B. Content Discrimination

The exclusion of speech based on the content of that speech is far more prevalent in cyberspace than even discrimination based on the status of the speaker. Listserv and newsgroup moderators commonly select which messages to distribute to discussion group members and often edit the distributed messages.[260] On the "regional" level, network administrators regularly decide which discussion groups may appear on the network and which may not.[261] They also sometimes delete or automatically screen out

259. Eugene Volokh opposes state intervention on the discussion group level out of a concern that the state should not be involved in overriding the discussants' own assessment that the discrimination is relevant to the discussion topic. *See* Volokh, *supra* note 238, at 396. Professor Volokh's point is certainly well taken, but it seems to me that the harm caused by pervasive discrimination would justify such state intervention and that assessment of the nexus between discrimination and topic would not be qualitatively different than state assessment of whether discrimination is necessary for effective advocacy.

260. Such moderator involvement distinguishes moderated from unmoderated groups. *See* Volokh, *supra* note 238, at 190.

261. For example, news administrators determine which Usenet newsgroups will be available on the local network. *See id*. at 189-90.

certain types of messages.[262] Network administrators may also employ software filters to block access to certain sites or certain types of sites. More aggressively, network administrators sometimes use self-help technology to cancel postings with which they disagree or to block all messages from targeted sources. Finally, at what might be seen as the "national" or "global" level, administrators of domain name registration systems may deny web site domain name registration based on the content of the proposed domain name or, conceivably, even the content of the site itself. Such denial effectively precludes the applicant from making his voice heard on the web (either under the requested domain name or at all).

Beyond such administrator editing and blocking, cyberspace, as currently structured, offers users an unprecedented opportunity to discriminate against content they choose not to see or hear. Unlike viewers of traditional television, readers of print newspapers, or purchasers of record albums, cyberspace users can carefully construct the matrix of speech to which they are exposed. Numerous browsers and web sites offer users the opportunity to custom-design the menu of information and content they receive, creating the equivalent of personalized newspapers and radio programming.[263] In contrast to the mainstream print and electronic press, moreover, cyberspace contains vast amounts of narrowly tailored information, opinion, and expression on a seemingly infinite variety of topics, all available to users at the click of a mouse. Cyberspace users thus enjoy considerable freedom to choose only the information they assume they want, and ignore other topics and views.[264]

Political liberalism generally requires that the state refrain from overriding private editing and content selection decisions. Indeed, the First Amendment generally protects both network administrator editing and user choice of content against such state interference.[265] Nevertheless, cyberspace content discrimination calls for a close examination of the desirability of state involvement on a number of fronts. Such state involvement may entail the promotion of expression diversity, regulation of systems for filtering web site content, and prohibition of self-help private censorship.

1. The Promotion of Expressive Diversity

Expressive diversity and robust debate are vital to democratic culture. In the offline world, however, the market skews public discourse in favor

---

262. *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (E.D. Ohio 1997) (describing CompuServe's efforts to block unsolicited email advertising from CompuServe customers).

263. *See* SHAPIRO, *supra* note 49, at 45-46 (describing personalized information services).

264. *See* SHAPIRO, *supra* note 49, at 105-14; Kathleen M. Sullivan, *First Amendment Intermediaries in the Age of Cyberspace*, 45 UCLA L. REV. 1653, 1668-69 (1998); Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805, 1807 (1995).

265. *See* Volokh, *supra* note 238, at 386-90.

of those with the financial wherewithal to own a press or broadcasting station, those likely to buy the products that advertisers want to sell, and those with majority tastes representative of the lowest common denominator of the consumer public.[266] The state has acted in a number of ways in an effort to counter these market and political failures in order to promote expressive diversity. It has imposed on certain speakers, notably private broadcasters and cable television operators, public interest and quasi-common carrier obligations. It has variously required them to devote attention to matters of public interest, present a diversity of views on such matters, and provide airway access to speakers whose views might otherwise not be heard.[267] The state has also engaged in structural regulation of the mass media, imposing local and minority ownership requirements and cross-ownership limitations designed to achieve a pluralism of voice.[268] Finally, the state has acted as speaker. It has done so directly through the dissemination of government-produced information, and indirectly by subsidizing the creation and dissemination of expression that might not find sufficient commercial support to otherwise find its way into public discourse.[269]

Cyberians contend that in an age of cyberspace "cheap speech," such state involvement is unnecessary.[270] On the Net, everyone can be a speaker and everyone can find a wealth of diverse expression and information. Concomitantly, cyberspace drastically reduces the control of publishers, broadcasters, newspapers, bookstores, and other private intermediaries over what speakers will say and audiences will hear. In cyberspace, authors

---

266. *See* C. Edwin Baker, *Giving the Audience What It Wants*, 58 OHIO ST. L.J. 311 (1997); Owen M. Fiss, *Free Speech and Social Structure*, 71 IOWA L. REV. 1405, 1412-13 (1986).

267. *See* Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180 (1997) (upholding constitutionality of statutory requirement that cable television systems dedicate some of their channels to local broadcast television stations); Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969) (upholding constitutionality of the fairness doctrine). I am, of necessity, oversimplifying; broadcast and cable regulation have followed a tortured path and have been justified by various rationales. *See* THOMAS G. KRATTENMAKER & LUCAS A. POWE, JR., REGULATING BROADCAST PROGRAMMING 277-96 (1994) (maintaining that efforts of the FCC, courts, and Congress to regulate broadcast programming reflect poor regulatory policy); Glen O. Robinson, *The Electronic First Amendment: An Essay for the New Age*, 47 DUKE L.J. 899, 908-45 (1998) (presenting critical survey of broadcast and cable regulation); Jonathan Weinberg, *Broadcasting and Speech*, 81 CALIF. L. REV. 1103, 1110-30 (1993) (discussing history of the United States' broadcast regulatory system and its current structure).

268. *See* THOMAS G. KRATTENMAKER, TELECOMMUNICATIONS LAW AND POLICY 307-20 (2d ed. 1998).

269. *See generally* Robert C. Post, *Subsidized Speech*, 106 YALE L.J. 151 (1996). Through copyright law, the state has also defined and delimited property rights in original expression so as to encourage creative contributions to the store of knowledge and to allow modifications and reformulations of existing expression. *See* Netanel, *supra* note 227, at 347-62.

270. The term "cheap speech" is from Eugene Volokh's then-prescient 1995 article. Volokh, *supra* note 264. As noted below in the text accompanying notes 275-77, I suspect that the next generation of the Internet will contain far more expensive, intermediary-directed speech than Professor Volokh envisioned in 1995. Professor Volokh is not a "cyberian" in the sense of generally favoring cyberspace self-governance, but he is a leading opponent of state regulation of online (and offline) speech. *See, e.g.*, Volokh, *supra* note 238; Volokh, *supra* note 264.

can communicate directly to readers, and readers can freely become authors, not only selecting what they read but also by responding to it.[271] In this new, highly democratic and highly diverse information marketplace, cyberians claim, the offline rationale for state regulation and intervention will no longer hold.[272]

But the cyberians' rosy picture of the digital information marketplace frays in a number of places. First, a world of custom-designed communications mixes could lead to considerable balkanization and self-insulation.[273] Given the power to screen out information or ideas they find uncongenial or simply to ignore cultural expression that does not fit their tastes, Internet users may well immerse themselves in a narrow set of familiar fare.[274] A liberal democratic polity, however, needs citizens who are exposed to competing ideals and ways of thought. In that manner, citizens can test and refine their own understandings and commitments, and gain some empathy for others even when they disagree. Citizens must also share a sufficiently common culture to engage in mutually intelligible conversation. Without some common language, some shared basis of understanding, public discourse will less resemble reasoned deliberation than cacophonous babble.

Second, as discussed above, cyberspace appears headed towards profound changes in its structure and content. Economies of scale, network effects, intense competition for user attention, and emerging Internet technology for the dissemination of high-quality, star-studded, expensive video content will radically transform cyberspace's expressive matrix. Far from its pluralist "cheap speech" origins, cyberspace will reverberate to the tune of Time Warner, Viacom, and Disney.[275] Lone authors and musicians might still post their work on listservs and web sites, and those who know and care to look will still be able to read and hear that work. But the dissemination of most information and expression will more closely resemble today's mass media marketplace than today's infant Internet. Both authors and audiences will return to depend heavily on intermediaries—the cyberspace equivalents of book publishers, film studios, newspapers, television networks, and record producers—to act as gatekeepers selecting which

---

271. *See* Jerry Berman & Daniel J. Weitzner, *Technology and Democracy*, 64 SOC. RES. 1313 (1997) (emphasizing decentralized, interactive capabilities of cyberspace communication).

272. *See* Sullivan, *supra* note 264, at 1670; Volokh, *supra* note 264, at 1836-37.

273. My comments here draw heavily on SUNSTEIN, *supra* note 87, at 186-87. *See also* SHAPIRO, *supra* note 49, at 105-14.

274. *See* Volokh, *supra* note 264, at 1834-35.

275. As of this writing, Time Warner, Viacom, and Disney are the three largest media conglomerates. Each has holdings in movie and television production, cable programming, publishing, music, broadcasting, and theme parks, and a growing presence on the web. *See Measuring a Combined Viacom/CBS Against Other Media Giants*, N.Y. TIMES, Sept. 8, 1999, at C15. America Online's acquisition of Time-Warner, announced just before this Article went to press, will likely greatly hasten cyberspace's transformation from virtual street corner to mass media market.

expression to market, to market that expression, and to invest in the production of expensive content. Those intermediaries will determine what content gets communicated to most people.[276] In turn, cyberspace intermediaries, like their offline counterparts, will tailor much of that content to mainstream tastes and to the tastes of audience segments most likely to buy advertiser products and services.[277]

If my prediction about the cyberspace future proves accurate, the cyberspace information marketplace will thus face much the same distortions and market failures that have often been seen to justify state intervention offline.[278] Still, that does not mean that the same kind of state intervention would be warranted. Even in my grim scenario, it is doubtful that the information marketplace will suffer from the same level of concentration and bottlenecks as in predigital broadcasting and cable television. Most virtual audiences may choose (or be pushed) content from large media conglomerates most of the time. But unlike today's subscribers of local cable monopolies, virtual audiences will likely have scores of such sources and distributors from which to choose. In addition, the Internet will provide some expressive outlet, the equivalent of an electronic street-corner, even for those without the funds to launch and market a digital channel.[279] Under those circumstances, state content regulation to promote expressive diversity or state mandated rights of access to commercial channels would be unnecessary and inappropriate (as well as likely unconstitutional).[280]

On the other hand, whether the digital information marketplace leans towards balkanized narrowcasting or to standard catering to the lowest common denominator, there will remain an important place for state subsidization of programming that deals with government, public affairs, the

---

276. Eugene Volokh predicts that trusted media critics will be the new intermediaries, that authors will not send their works to publisher intermediaries, but rather to reviewers for what they hope will be a positive recommendation. *See* Volokh, *supra* note 264, at 1815-16. This may well happen to a greater extent than today. But authors will still want to find a publisher-like sponsor to market their work, and advertising will still play a large role in influencing consumers' initial preferences.

277. *See* BRUCE M. OWEN & STEVEN S. WILDMAN, VIDEO ECONOMICS 101-50 (1992) (noting that content providers' congenital bias against minority tastes and in favor of large audiences' tastes is exacerbated in media characterized by firm concentration and in media supported by advertising).

278. *See* Baker, *supra* note 266; Benjamin R. Barber, *The Market as Censor: Freedom of Expression in a World of Consumer Totalism*, 29 ARIZ. ST. L.J. 501, 511 (1997).

279. In today's Internet, "to create a Web page that will be publicly accessible to millions of Internet users around the world, one need only find an Internet-connected computer and, often, pay that operator of that computer for Web-site hosting service." Berman & Weitzner, *supra* note 271, at 1314. That will not likely change in the near future. But in many instances, few Internet users will actually visit the site unless considerable sums are spent on marketing.

280. *But see* SUNSTEIN, *supra* note 87, at 199-200 (contending that congressionally mandated public access and preferential telecommunications rates in order to promote expressive diversity in the face of market homogenization might survive First Amendment scrutiny).

arts, education, and minority expression.[281] Some such content will likely find its way onto the Internet even absent state support. But without state funding for high-quality production, distribution, and marketing, it will be lost in the welter of text, voice, film, and music transmitted across the Net. The liberal state should thus be entitled and encouraged to use its fiscal power to support the dissemination of selected digital content.[282] Through such subsidies, as well as through its ability to "*legitimate* certain arguments by virtue of state endorsement,"[283] the state should seek to encourage citizens to partake of a diversity of expression and seek to counter the insularity attendant to both narrowcasting and mainstreaming.

2. Filtering

Filtering is a crucial part of any communication. We cannot process all the human-generated information that stands at our disposal. We must set aside the vast bulk of that information in order to make communication a productive, meaningful, and enjoyable activity. Nor can we even sift through any but a minute portion of that information in order to select what we want to read, look at, or listen to. Rather we must simply ignore—block out—almost all of the expression that seeks to capture our attention. The question then is not whether we filter certain speech, but how. On which technologies and social institutions do we rely to select the speech we will hear?[284] How is content-determining authority allocated and to what extent do we delegate sifting and selecting decisions?

In the offline liberal state, we rely heavily on the editorial and marketing decisions of private publishers to select the speech we will receive. I read the *New York Times*, rather than the *National Enquirer*, because I assume that the *Times'* editors will consistently select out a mix of expression containing more information and opinion of use and interest to me,

---

281. For a discussion of the possible role of public television in the digital age, see Monroe E. Price, *Public Television in America Project: Public Television and New Technologies*, 1 INT'L J. COM. L. & POL'Y (1998) <http://www.digital-law.net/ijclp_webdoc_2_1_1998.html>.

282. An interesting question is the extent to which the state may use its fiscal power to support certain types of expression and not others in cyberspace. Supreme Court jurisprudence grants the government largely unconstrained power to subsidize such speech as it prefers, and to refuse to subsidize other speech. *See* Post, *supra* note 269. Yet, commentators raise the concern that state subsidies for expression may give the state undue power in the marketplace for ideas. *See, e.g.*, Marci A. Hamilton, *Art Speech*, 49 VAND. L. REV. 73, 112-19 (1996). As Sandy Levinson argues, however, state endorsement of some ideas at the expense of others is inevitable. *See generally* Sanford Levinson, *The Tutelary State: "Censorship," "Silencing," and the "Practices of Cultural Regulation," in* CENSORSHIP AND SILENCING: PRACTICES OF CULTURAL REGULATION 195 (Robert C. Post ed., 1998) [hereinafter CENSORSHIP AND SILENCING]. In any event, the concern of undue state influence seems particularly unjustified in cyberspace, where state-supported expression faces enormous competition from all corners and expression that does not receive state support will still have some outlet.

283. Levinson, *supra* note 282, at 196.

284. *See* Frederick Schauer, *The Ontology of Censorship*, *in* CENSORSHIP AND SILENCING, *supra* note 282, at 147, 163-64.

and more writing that I will find enjoyable to read. As a society, we allocate selection and editorial decisions to those with the financial resources to own and operate a press, film or TV studio, broadcast station, book store chain, or CD distribution network. To the extent we even think about it, we trust those entities (at least more than we trust the government) to provide us with more or less the expressive mix we want, and available offline technology does not offer meaningful, more decentralized editorial alternatives.

Filtering is no less necessary in cyberspace than offline, and indeed, given the volume of information available in cyberspace, perhaps even more so. That need has spawned a growing industry in Internet filters.[285] As Esther Dyson aptly notes, "the new wave is not value-added; it's garbage subtracted."[286]

Internet filtering systems are of several different types. First, there are what we might call positive, limited filters. These comprise searching agents and browser pages that highlight a specified set of information for the user. As noted above, users can increasingly customize that information mix. I call these positive, limited filters because, while they highlight certain information and sources, they do not preclude, or impose significant costs on, user access to other content. I might configure my browser to use the *New York Times* web site as its home page, but that does not prevent me from surfing to the *Enquirer*'s site as well.[287]

Then there are more comprehensive, negative filters. These are generally configured to completely block access to certain specified sites or, even more broadly, the reverse: to allow access only to listed approved sites. Most such filters, still the most feasible negative filtering technology today, provide access to a database of blocked or approved sites, compiled by the filter manufacturer or some other intermediary. When the user's browser seeks to visit an Internet page, it first "requests permission" from the database site. Permission to access is granted or denied depending on whether and how the page is described in the database.[288]

Increasingly, however, filters employ embedded ratings systems, such as the Platform for Internet Content Selection (PICS).[289] Such systems

---

285. *See* R. Polk Wagner, *Filters and the First Amendment*, 83 MINN. L. REV. 755, 760-69 (1999); Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453 (1997); Paul Resnick, *Filtering Information on the Internet*, SCI. AM., Mar. 1997, at 62, 62-64.

286. Esther Dyson, *Intellectual Property on the Net* (visited Jan. 7, 2000) <http://www.eff.org/pub/Publications/Esther_Dyson/ip_on_the_net.article>, *cited in* Robinson, *supra* note 267, at 969.

287. On the other hand, manufacturer-customized browsers may channel users towards certain sites, creating what Andrew Shapiro calls "screen bias." SHAPIRO, *supra* note 49, at 95-97.

288. *See* Wagner, *supra* note 285, at 761-64.

289. For a more thorough explanation of PICS technology and its applications, see Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, 39 COMMUNICATIONS OF THE ACM 87 (1996), *available at* (visited Dec. 25, 1999) <http://www.w3.org/PICS/iacwcv2.htm>.

enable content providers or authorized independent entities to insert digital labels into Internet content. The user's selection software then determines how to process the content bearing specified labels—whether to block it, restrict access, allow access, organize it, or perform some other task.[290] Significantly, PICS and other such embedded ratings systems can be set to block access to unrated sites or to all sites except those bearing certain labels.[291] So configured, PICS may dramatically curtail the scope of the user's Internet access.

Moreover, even that filtering is child's play compared to the anticipated development of electronic "smart agents."[292] Such agents will consist of software programmed to browse the Internet on the user's behalf and to bring back (or allow in) only that menu of information that comports with the user's specifications.[293] We might think of smart agents as a comprehensive, positive filter. They do far more than highlight particular information. Rather, once deployed, a smart agent accords the user access only to the user's narrowly tailored pre-selection of text, graphics, video, and music. It effectively screens out everything else.

Internet filtering has been highly controversial and the critics' wrath has fallen on PICS in particular. They have variously labeled that filtering standard "the devil"[294] and "the most effective global censorship technology ever designed."[295] Much of such criticism focuses on the possibility that governments might either institute Internet filtering to prevent their citizens from gaining access to certain information or effectively require content providers to label their content so that users can more easily filter.[296] But concern has also been raised about private filtering in and of itself.[297] It has been suggested in that regard, that the state might act to curtail private Internet filtering.[298] It is that possibility that I wish to consider.

---

290. *See* Goldsmith, *supra* note 19, at 1227 n.117.

291. *See* Wagner, *supra* note 285, at 765-66.

292. Walter Forbes, *A Store as Big as the World*, *in* ELECTRONIC MARKETPLACE, *supra* note 180, at 63, 72-75.

293. Smart agents may perform other functions as well, including contract negotiation and monitoring complex systems. *See* Denos Gazis, *PASHAs: Advanced Intelligent Agents in the Service of Electronic Commerce*, *in* ELECTRONIC MARKETPLACE, *supra* note 180, at 145.

294. Lawrence Lessig, *Tyranny in the Infrastructure*, WIRED, July 1997, at 96, 96.

295. Simson Garfinkel, *Good Clean PICS: The Most Effective Censorship Technology the Net Has Ever Seen May Already Be Installed on Your Desktop*, HOTWIRED (Feb. 5, 1997) <http://www.hotwired.com/packet/garfinkel/97/05/index2a.html>.

296. *See, e.g.*, Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629 (1998).

297. *See* Joshua Micah Marshall, *Will Free Speech Get Tangled in the Net?*, AM. PROSPECT, Jan.-Feb. 1998, at 46 (contending that content filtering makes majority silencing of dissenters even more feasible than in the past).

298. *See* Sullivan, *supra* note 264, at 1679-80 (considering whether government subsidies for access to unfiltered content or bans on the use of filters would pass First Amendment muster).

Liberal democratic theory sets forth two fundamental, and partly opposing, criteria for assessing content-determination systems. First, it places a primacy on expressive diversity and citizen education. Citizens must be exposed to a wide variety of information and opinion on matters of public import in order to make critical judgments about government policy and elected officials. Second, individuals should exercise considerable autonomy in determining what expression they will see and hear, or at least in selecting the institutions on which they will rely for content selection. That means, first and foremost, that the state cannot micromanage individual choices regarding speech consumption. Somewhat more controversially (at least within traditional liberal thought), it means that we should also seek to maximize individuals' autonomy and considered judgment in their selection of private speech filtering intermediaries.

How then might we assess the allocation of content-determination authority that Internet filtering represents? To the extent that individual users configure filtering systems to suit their particular tastes and interests, Internet filtering represents a somewhat more extreme version of the narrowcasting problem discussed above. Try as they might, audiences of traditional, offline media cannot always filter out information they do not want to hear. As I flip among the channels on my TV set or leaf through the newspaper, I am bound to come across, even if only for a fleeting moment, some expression that I would not otherwise care to see. In fact, a program or article might just catch my eye, and—who knows—might even lead me to question my prior preferences or opinions. But with my customized Internet filter in place when I browse through cyberspace, or my preprogrammed electronic agent browsing for me, I will simply not come into contact with sorts of expression that I have determined in advance that I do not want to see.[299]

Such filtering, then, raises problems of excessive insularity. At bottom, it enables users to be too selective about the speech they hear. As such, Internet filtering may contribute to locking in existing preferences, and to diminishing possibilities for discourse across the political and cultural spectrum. But that is not to say that the liberal state should interfere with individualized uses of Internet filtering. Such interference would raise serious concerns about state efforts to direct individual content consumption choices. Rather, as noted above, the most the state can or should do to counter individuals' self-chosen insularity is to promote alternatives and seek to cultivate a broader civic interest among its citizens.

Yet much Internet filtering is not individually configured. Internet users often delegate their micro-filtering choices to intermediaries. That is what happens, for instance, when users rely on filter software that includes a third-party database of permitted or prohibited sites. User delegation can

299. *See* LESSIG, *supra* note 12, at 180; SHAPIRO, *supra* note 49, at 105-09.

have untoward consequences. Database filtering systems are notoriously overbroad and inaccurate.[300] They may also incorporate their developer's political agenda. A database-driven parental control software called "Cybersitter," for example, has blocked the web site of the National Organization of Women for "sexual content," as well as web sites critical of Internet filtering.[301]

Software that purports to filter for one thing and actually filters for something quite different should be subject to liability for false advertising. In addition, one can argue that filtering intermediaries should be required fully to disclose their filtering criteria, including the list of sites they block. Intermediaries regularly refuse to do so on the grounds that their filtering criteria constitutes a trade secret. That position is not unreasonable. Especially for commercial intermediaries, opening filtering criteria to possible appropriation by competitors might, to a degree, diminish incentives to develop criteria and assemble lists of prohibited sites. Nevertheless, the liberal principle of maximizing individuals' autonomy in their selection of private speech filtering intermediaries suggests that the state should require full disclosure.[302] This may dissuade some commercial entities from developing and marketing filtering systems. But there are no doubt ample numbers of civic-minded and ideologically-based organizations that would be happy to offer or commission filtering services on a nonproprietary basis.

Filtering can also take place without the user being aware of it at all. Internet service providers, employers, or universities can install filters "upstream" from the user, so that none of the users in the affected system may access materials the organization deemed inappropriate. Filters can also be embedded in browser software, with the factory default configured to deny access to unrated sites or pages.[303]

Internet service providers, employers, universities, and browser manufacturers are certainly entitled to employ filters. Service providers and browser manufacturers may do so as a service to consumers. Employers and universities might wish to curtail Internet surfing unrelated to employment and classroom study. Nevertheless, users should be entitled at

---

300. *See* Wagner, *supra* note 285, at 762.

301. *See id*. at 763 n.20. Indeed, Solid Oak Software, Cybersitter's manufacturer, has threatened to block all 2500 web sites hosted by an Internet filtering critic's network service provider, unless the provider removed the critic's site from the provider's network. *See* Rebecca Vesely, *CyberSitter Goes After Teen*, HOTWIRED (Dec. 9, 1996) <http://www.wired.com/news/politics/0,1283,901,00.html>, *cited in* Wagner, *supra*, at 763 n.20.

302. Of course, offline intermediaries are not required to disclose their editorial policies. But this seems an instance in which digital technology makes possible a greater realization of liberal principles than in the offline world.

303. Version 4.0 of Microsoft's Internet Explorer gives the user the possibility to choose whether unrated pages will be seen. Contrary to the possible scenario I have described in the text, the factory default setting for that browser is to allow unrated sites to be seen. *See* Wagner, *supra* note 285, at 765-66.

least to know that their Internet use is subject to filter, and that their browser searches are not bringing forth the full component of possible sites. Armed with that knowledge, they might choose to gain Internet access through another gateway with lesser or different filter constraints.[304]

Beyond such full and accurate disclosure requirements, however, user delegation of filtering choices to intermediaries should not give rise to any greater state interference than when users configure filtering by themselves. As in the offline world, most people do not have the time to engage in much micro-filtering on their own. Rather they choose intermediaries whom they trust to filter on their behalf. Intermediaries may sometimes block expression that the user might have chosen to see, just as the *New York Times* might not publish everything I would have wanted to read. But that is not in and of itself cause for state intervention.

3. Self-Help Censorship

Cyberspace encompasses a variety of self-help censorship technologies and strategies that are more aggressive than filters. Filtering blocks access to a site or page from one's own computer or Internet gateway. It might block access for anyone who uses that computer or gateway, including one's family members, employees, students, and customers. But it does not impede a stranger's access to the filtered site.

In contrast, self-help censorship mechanisms can be used to block or cancel all Usenet or email messages that originate from a certain site, service provider, or server. In one celebrated case, for example, the Church of Scientology used a computer program known as a "cancelbot" to cancel

304. Service provider and employer blocking of email sent to subscribers and employees should be subject to a similar notice requirement as I have proposed with regard to web filtering. A number of courts have held that Internet service providers may block unsolicited email, without implicating the First Amendment, by applying technological self-help or suing senders of unsolicited email for trespass to chattel. *See, e.g*., CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (holding that injunction prohibiting delivery of unsolicited email advertisements to CompuServe subscribers, on grounds that unsolicited deliveries were a trespass to chattel, did not implicate the First Amendment); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996) (holding that since AOL is a purely private actor, it could use self-help to block Cyber Promotions' sending of unsolicited email advertisements to AOL subscribers without implicating First Amendment). A pending action concerns whether Intel Corp. may obtain an injunction against the distribution of emails to Intel employees, detailing Intel's allegedly abusive and discriminatory employment practices, without implicating the First Amendment. *See* Intel Corp. v. Hamidi, No. 98AS05067 (Cal. Super. Ct. filed Oct. 6, 1998). Whatever the merits of the Cyber Promotions decisions and of the Hamidi claim as a matter of First Amendment doctrine, at the very least would-be recipients of such emails should be entitled, as a matter of free speech policy, to know that their service provider or employer is preventing delivery of emails and to obtain contact information for the prospective email sender so that they may arrange to receive the emails at another address if they so wish. Of course, a legal requirement that the service provider or employer provide such information might infringe that entity's free speech rights. But, on balance, I would argue, the would-be recipient's free speech interest in receiving notice should prevail. For a more detailed discussion of this issue in connection with the *Hamidi* case, see *Developments—Cyberspace*, *supra* note 111, at 1622-34.

posts of Church critics to the Usenet newsgroup, alt.religion.scientology.[305] In other instances, the self-appointed SubGenius Police Usenet Tactical Unit Mobile (S.P.U.T.U.M.), in collaboration with system administrators, has exacted the "Usenet death penalty" on service providers that allow their customers to post unsolicited bulk advertisements (known as "spam").[306] The death penalty bars all messages from any subscriber of the recalcitrant service provider. Similarly, the managers of the "Realtime Blackhole List"[307] and other antispam activists identify Internet service providers who, in the activists' opinion, have not done enough to prevent spammers from using their email relay systems to send spam email to third parties. The activists assist other service providers in configuring their systems to deny access to any email from subscribers of providers accused of such "bad e-mail practices."[308] The networks of a number of universities, including Harvard and MIT, have been targets of such antispam actions when activists deemed insufficient the networks' efforts to police the use of their respective email relay facilities.[309]

Cyberians laud such measures as an instance of "informal social control."[310] In this view, cancelbots and electronic death penalties are simply mechanisms for decentralized "norm-creation" and enforcement in cyberspace. Their value lies in not being state-imposed law that seeks to govern every cyberspace user in a standard manner; such self-help mechanisms are rather one of many alternative rule regimes. Targets can fight back with circumvention technology or by blocking their censors' messages. System administrators can choose whether to side with the censors or with the targets. From all this will emerge a norm concerning the expression in question, one arrived at from the "bottom up." As David Post argues, countering the complaint of "Professor X" that his email regularly bounces back to him after antispam activist, Paul Vixie, targeted his university computer network:

> Most significantly, if you do not agree with Vixie's particular definition of unacceptable behavior, or his choice of sanction, or

---

305. *See* Post, *supra* note 61.

306. *See* Lemley, *supra* note 19, at 1284-85; *see also* (visited Oct. 17, 1999) <http://www.sputum.com> (S.P.U.T.U.M. portal web site).

307. The web site of the Realtime Blackhole List is (last visited Oct. 17, 1999) <http://maps.vix.com/rbl>.

308. Lawrence Lessig, *The Spam Wars*, INDUSTRY STANDARD, Dec. 31, 1998, *available at* (visited Nov. 1, 1999) <http://www.thestandard.com/articles/display/0,1449,3006,00.html>. Unlike S.P.U.T.U.M., which has barred all messages from the offending service providers, the Realtime Blackhole List (RBL) activists merely assist in barring messages sent to customers of those service providers whose administrators have elected to avail themselves of RBL's assistance.

309. *See id.*

310. *See* Post, *supra* note 115; *cf.* Perritt, *supra* note 2, at 440-42 (suggesting that a group of Usenet administrators who cooperate in canceling messages may engage in "fair" rule making because anyone who objects to their decisions can post her views in their newsgroup, but questioning whether cancellation constitutes fair adjudication absent some due process for the target).

> the means he has chosen to implement that sanction, or his method of detecting violators subject to the sanction, you are entirely free to ignore them (or, if you'd like, to propose your own). Not that his behavior doesn't exercise a constraint on yours; but it does so only to the extent (and precisely to the extent) that others share his views on the definition of wrongdoing, the choice of appropriate sanction, the identity of the wrongdoers, etc. He can persuade, and cajole, and beg the hundreds of thousands of ISPs out there to join his group of Subscribing ISPs—but he cannot force them to do so in any meaningful sense of that term. It is a near-perfect preference-revealing device, it would seem, for uncovering shared definitions of unacceptable conduct; the likelihood that Professor X will feel the sting of Vixie's sanction is perfectly calibrated to the number of people who share Vixie's views in these matters. If a substantial number of people share his view of unacceptable behavior, it may become a governing norm on the net; and if a substantial number of people share his view of what constitutes unacceptable behavior, who is to say that that view is not the "correct" one?[311]

To my mind, a world such as the one Professor Post envisions would run counter to the principles of liberal democratic governance. For one, I question the democratic nature of the market-based decision-making process. That process is heavily biased towards those with the financial resources, generally acquired outside of cyberspace, to expend on convincing others (perhaps by words, perhaps by bribes, perhaps by threatening to block their sites and servers) to join one's side. If Microsoft and General Motors were ever to decide that spamming was vital for their business, I have no doubt that most system administrators would be "convinced" to accept spam.[312]

Even more basically, however, that cyberanarchist world provides inadequate protection against the tyranny of the majority. As Professor Post would apparently have it, if most system administrators decided to block service providers that allowed their subscribers or others to post messages containing certain unpopular political or religious views, that would simply entail the acceptable creation of a cyberspace social norm banning dissemination of those views. But liberal democracy, and in this case the right of free speech, is designed precisely to impede such

311. Post, *supra* note 115, at text accompanying nn.11-12.

312. Sadly, financial strength plays an inordinate role in the legislative process as well, at least in the United States. But most agree that this is an aberration from the ideal, and a problem begging for a political solution, such as through campaign finance reform. In cyberspace, however, there are no meta-rules against directly or indirectly buying votes. Indeed, the market view of alternate rule regimes would find perfectly acceptable a tying arrangement requiring acceptance of a given rule regime as part of the purchase of a given product or service.

"preference-revealing devices" when majority preferences run roughshod over fundamental political and civil rights of minorities.

The need for minority protection is even more apparent when one considers the impact of network effects on cyberspace governance. Post seems to suggest that procensorship and anticensorship regimes could co-exist on the Internet, that perhaps users could (through their selection of system administrators) choose whether to have interconnections with those that ban the particular speech or with those that allow it. But communications systems like the Internet exhibit powerful network effects. A significant value—indeed for most people the principal value—of having an Internet connection is the capacity to communicate with everyone else on the Net and to access information from a wide variety of different sources.[313] As a result, in a case of competing, incompatible sub-networks, users will tend to stampede towards the sub-network that initially attracts more users. That network will become the de facto standard setter and norm-creator.[314]

C. The Appropriation of Personal Information

Each time I visit the *New York Times* web site, the *Times* and its advertisers gather information about what I choose to read there.[315] Depending on how my browser is configured, they can also determine what other sites I have visited. The *Times* and its advertisers use the information they gather to create a profile of my reading preferences. That way they can individualize their services and offer me promotions I am more likely to buy. They also regularly transfer all or part of the information to others. These third parties may then aggregate the *Times* web site information with additional information that has been compiled about me from other sites. In that manner they can produce a more complete profile or various profiles tailored to different ends.

The *New York Times* site is not atypical, except that it purports to comply with a relatively high standard of customer privacy protection.[316] Our cyberactivity regularly generates information about us that is collected and used by others.[317] In fact, advances in digital communication, storage, and processing technology have created unprecedented possibilities for

313. *See* Lemley & McGowan, *supra* note 114, at 560. As Lemley and McGowan note, users do not always want to communicate with everyone. Users often want to filter out certain specified expression. But that applies only to the unwanted expression itself, not to messages and sources of information that bear no relation to the unwanted expression except that they are relayed by a target service provider.

314. *See id.* at 561.

315. *See* THE NEW YORK TIMES ON THE WEB, *Privacy Information* (visited Nov. 1, 1999) <http://www.nytimes.com/subscribe/help/privacy.html>.

316. *See id.*

317. *See* BERNERS-LEE, *supra* note 106, at 144-46; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1199 (1998); Schwartz, *supra* note 147.

recording and exploiting information regarding individuals' activities and preferences.[318] The ramifications are profound. It is not merely that seemingly infinite amounts of information can be collected and permanently stored. Digital information processing also entails aggregating previously scattered bits of information from different contexts.[319] It thus produces virtually limitless possibilities for compiling, analyzing, and systematizing such information.[320]

Surveys indicate that the American public has widespread apprehension about the use and misuse of personal information, especially in connection with Internet activity.[321] That in turn has prompted concern in the Clinton Administration that consumers will not use the Internet for electronic commerce unless they are assured about personal privacy protection.[322] But the issue of personal data protection goes beyond individual apprehension and the development of electronic commerce. It is widely contended (although less so in the United States than in other Western democracies) that the unrestricted collection, storage, and compilation of personal data—whether at the hands of private parties or the government—impinges upon fundamental liberal rights.[323]

International human rights treaties, including the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, recognize, in fairly general terms, individuals' right to privacy.[324] Courts,

---

318. *See* Kang, *supra* note 317, at 1223-31, 1238-40; Nissenbaum, *supra* note 237, at 575-78.

319. *See* Nissenbaum, *supra* note 237, at 586-90.

320. The Supreme Court has recognized the privacy implications of digital data aggregation in the context of criminal records:

> [T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989).

321. *See* Kang, *supra* note 317, 1196-97 (describing the results of several surveys).

322. *See* National Telecommunications and Info. Admin., Dep't of Commerce, *Privacy and the NII: Safeguarding Telecommunications—Related Personal Information* (1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>.

323. *See, e.g.*, PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 39-42 (1998) (arguing, in line with the European view, that data privacy should be deemed both an individual civil right and a precondition for individual autonomy and civic participation); *see also* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751, 777 (1999) (book review) (noting that the civil liberties view of data privacy enjoys broad support in Europe, but not in the U.S., at this time).

324. Article 17 of the International Covenant on Civil and Political Rights provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

International Covenant on Civil and Political Rights, art. 17, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 172, 177. Article 8(1) of the European Convention provides: "Everyone has the right to

commentators, legislators, and various international instruments have in turn viewed personal information protection as a necessary component of that right.[325] For example, the Council of Europe's Convention on personal data protection asserts as its principal object: "[T]o secure . . . for every individual . . . respect for his fundamental rights and freedoms, and in particular his right to privacy."[326] The European Union's 1995 Data Protection Directive expresses its purposes in similar terms.[327]

In order to fulfill its express goal of protecting individuals' right to privacy, the European Union Directive provides for comprehensive regulation of personal data collection and processing by private parties.[328] In marked contrast, the Clinton Administration, following its support for Internet "bottom-up" governance whenever possible, generally favors industry self-regulation to achieve "fair information practices" in cyberspace.[329] Like cyberians, the Administration would couple self-regulation with market forces.[330] Internet users would be free to choose between web site rule regimes that protect data privacy and those that do not. Thus the virtual "invisible hand" will generate a set of data protection alternatives,

---

respect for his private and family life, his home and his correspondence." Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

325. *See* Lee A. Bygrave, *Data Protection Pursuant to the Right of Privacy in Human Rights Treaties*, 6 INT'L J.L. & INFO. TECH. 247 (1998); *see also* INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (June 6, 1995), *available at* (visited Jan. 5, 2000) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html> [hereinafter INFORMATION INFRASTRUCTURE TASK FORCE] (defining information privacy as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used").

326. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108.

327. The Directive states that its goal "is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law." Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

328. For a comprehensive discussion of the Directive's provisions, see PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998); Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 473-88 (1995). Much to the consternation of U.S. officials, the Directive permits the sending of personal information only to countries with "adequate" privacy protection, which is to say at a level similar to that ensured in the EU.

329. INFORMATION INFRASTRUCTURE TASK FORCE, *supra* note 325; FTC PRIVACY REPORT, *supra* note 4. The Administration did support legislation, enacted by Congress in 1998, to protect the privacy of children online. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (Supp. 1999). It has also recently promulgated detailed proposed regulations requiring a measure of privacy protection for patients' medical data. *See* Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918 (1999) (to be codified at 45 C.F.R Parts 160 through 164) (proposed Nov. 3, 1999), *available at* <http://aspe.os.dhhs.gov/admnsimp/pvclist.htm>; *see also* Robert Pear, *Rules on Privacy of Patient Data Stir Hot Debate*, N.Y. TIMES, Oct. 30, 1999, at A1.

330. For a cyberian view, see DYSON, *supra* note 22, at 201.

ranging from no protection to significant protection. Users who are concerned about privacy can limit their Internet surfing to protective regimes. Users who are not concerned can freely visit web sites that offer no protection regimes, presumably in return for other benefits.[331] If enough consumers are sufficiently concerned about data privacy to refuse to visit nonprotective sites, the Administration believes, market pressure will push sites to provide protection.[332]

Far from its promise of Pareto optimality, the proffered combination of self-regulation and market forces would likely fail adequately to protect data privacy. Industry self-regulation, a group's regulation of its members' practices with the goal of reducing harmful externalities to outsiders, is notoriously inadequate to its task. As trenchant critics have shown, such self-regulation can only work under conditions of stringent government oversight.[333]

At the same time, the market for privacy protection rule regimes suffers from intractable information asymmetry and market failure.[334] As discussed above, Internet users awash in an overabundance of information are no more able to assess and compare products and rule regimes than are their offline counterparts. In this instance in particular, most users are not even aware that the web sites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed.[335] We are used to relinquishing control over bits of personal information in many seemingly unrelated contexts. The problem in cyberspace is that, given the power of data processing, storage, and aggregation, users who acquiesce in what seems like a number

---

331. *See* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 604-05 (1994) (arguing that pricing reflects different consumer preferences about privacy).

332. For further discussion of the market model, distinguishing it from self-regulation, see Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* NATIONAL TELECOMMS. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, ch. 1.A (1997), *available at* (visited Jan, 5, 2000) <http://www.ntia.doc.gov/reports/privacy/Selfreg1.htm#1A> [hereinafter NTIA REPORT].

333. *See* Angela J. Campbell, *Self-Regulation and the Media*, 51 FED. COM. L.J. 711, 758-59 (1999) (concluding that media industry self-regulation has been effective only when spurred by the threat of government regulation); William H. Simon, *The Kaye Scholer Affair: The Lawyer's Duty of Candor and the Bar's Temptations of Evasion and Apology*, 23 L. & SOC. INQUIRY 243, 245 (1998) (arguing that the bar's "self-protective" rather than "self-regulating" treatment of the Kaye Scholer affair "should be counted as a large mark against it in the current debate over the appropriate allocation of regulatory responsibilities between public authorities and professional institutions."). In the data privacy context, see Deidre K. Mulligan & Janlori Goldman, *The Limits and the Necessity of Self-Regulation: The Case for Both*, *in* NTIA REPORT, *supra* note 332, ch. 1.G, *available at* (visited Jan. 5, 2000) <http://www.ntia.doc.gov/reports/privacy/Selfreg1.htm#1G>. *See also* Swire, *supra* note 332 (concluding that "there are significant reasons to believe that government regulation will be stricter in enforcing the protection of personal information than [industry] self-regulation," but noting that "[t]he difficult question will be to balance these gains in privacy protection against the likely higher administrative and compliance costs of government regulation").

334. *See* Swire, *supra* note 332.

335. *See* Kang, *supra* note 317, at 1253.

of innocuous isolated instances of data collection, spread out over a considerable period, may well be surprised to find that all of those bits have been aggregated and compiled into a highly pervasive profile. In the face of such user ignorance, web site operators have little incentive to provide consumers with a full account of such information practices.

We thus have a situation of widespread user ignorance about data use, coupled with growing suspicion of possible unspecified privacy-invading abuses. At the same time, data regarding an individual's Internet use habits and purchasing preferences has become an extremely valuable resource for cyberspace merchants.[336] Under such circumstances web site operators who freely collect and transfer user data have every reason to hide their practices.[337] Even web site operators who refrain from the most egregious practices of user profiling, and who loudly proclaim that they do so, may not provide a full account of the information processing and profiling practices of those to whom they transfer user information. Not surprisingly, then, nondisclosure and outright deception regarding data practices abound on the Internet.[338]

Even aside from site operator opportunism, transaction costs and collective action problems also impose severe constraints on the efficacy of the market to discipline information practices. Individualized negotiation regarding web site information practices is out of the question. Such practices contain numerous variables, including which information is collected, whether it is collected by site advertisers as well as site operators, how the information is used on site, which information, if any, is transferred to third parties, how long information is to be stored, what safeguards are put into place to prevent leakage, and others. As a result, to the extent site operators address information practice issues at all, they generally state their terms in standard, take-it-or-leave-it web access contracts. Of course, Internet users generally have neither the time nor ability critically to examine and compare the privacy protection terms of every web site they visit. Nor would we want them to; a regime in which every new site visit was preceded by considered assessment of privacy terms would significantly burden cyberspace communication.

---

336. *See* Bob Tedeschi, *Targeted Marketing Confronts Privacy Concerns*, N.Y. TIMES ON THE WEB (May 10, 1999) <http://www.nytimes.com/library/tech/99/05/cyber/commerce/10commerce.html> (reporting assessment of electronic commerce industry analyst that "[t]he trend toward capturing and using information is the future of online commerce").

337. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2414 (1996) ("[M]erchants cannot tell which consumers value privacy highly without asking all consumers. Raising the privacy issue may evoke negative reactions in consumers who otherwise would not have thought about the issue.").

338. *See* Kang, *supra* note 317, at 1253 (noting that cyberspace site operators "do not generally provide adequate notice about what information will be collected and how it will be used").

Cyberians and other market proponents have proffered two principal alternatives for overcoming such barriers: delegation and technology.[339] Users could rely on trusted third parties to rate web sites according to the sites' privacy practices.[340] A user's decision whether to visit a site could then take into account the site's privacy rating. In fact, much like content ratings, users could configure their browsers—or service providers could configure their Internet gateways—only to accept sites bearing certain third-party privacy ratings.

Such a regime would depend on the reliability of the third party and its rating system. It also requires cooperation, in the form of accurate reporting of data privacy practices, from those site operators interested in obtaining a rating. Accordingly, such a regime would not solve information asymmetry and collective action problems, but merely push them to another level. Rather than having to assess the information practices of individual web sites, users would have to determine which third parties and rating systems are reliable and have access to accurate reporting. That may be a formidable task.[341] Consider the frequency with which self-serving industry groups masquerade under the banner of such names as "Concerned Citizens for . . . ."[342]

The cyberians' second proffered solution would avoid both transaction costs and third-party agency costs by employing electronic agents rather than human ones. It would rely on the Privacy Preferences Project (P3P) software standard, being developed by the World Wide Web Consortium.[343] Using P3P, Internet users will be able to encode their pri-

339. *See, e.g.*, DYSON, *supra* note 22, at 201.

340. Third party privacy ratings are already in effect. *The New York Times Web Site*, for example, indicates that its information privacy practices meet "TRUSTe" standards. TRUSTe is a nonprofit organization founded by the Electronic Frontier Foundation and the CommerceNet Consortium to help promote consumer trust and confidence in electronic transactions. *See TRUSTe* (visited Jan. 7, 2000) <http://www.truste.org>. The Better Business Bureau's online privacy seal program is BBBOnline. *See BBBOnline* (visited Jan. 5, 2000) <http://www.bbbonline.org>.

341. Indeed, trusted third party reliability has already been called into question. The press has reported that TRUSTe, one of two leading trusted third parties, failed to withdraw its approval seal from the Microsoft web site, or even to conduct an investigation of Microsoft's information practices, despite customer complaints that the Microsoft site was collecting personally identifiable information against customer wishes. Microsoft is one of TRUSTe's principal sponsors. *See* Jeri Clausing, *Privacy Watchdog Declines to Pursue Microsoft, a Backer*, N.Y. TIMES ON THE WEB (Mar. 22, 1999) <http://www.nytimes.com/library/tech/99/03/cyber/articles/23privacy.htm>. TRUSTe reportedly stated that because it was actually Microsoft software in the user's computer, not the web site, that collected user data without the user's agreement, there was no violation of the TRUSTe disclosure guidelines. *See* Microsoft Off TRUSTe's Hook, WIRED NEWS (Mar. 22, 1999, updated Oct. 4, 1999) <http://www.wired.com/news/print_version/chnology/story/18639.html>.

342. In fact, the lobbying organization representing industry in opposing government data privacy regulation calls itself the "Online Privacy Alliance." *See Online Privacy Alliance* (visited Jan. 7, 2000) <http://www.privacyalliance.com>.

343. *See* DYSON, *supra* note 22, at 201-05. The World Wide Web Consortium is a nonprofit institution involved in Internet self-governance. *See World Wide Web Consortium* (visited Jan. 7, 2000) <http://www.w3.org>.

vacy preferences into their browser, and web site operators will be able to include their privacy policies in their site servers.[344] The result will be machine-to-machine communication and, possibly, negotiation, without a person getting involved at either end.[345] For example, I might set my browser to provide that site operators may collect information regarding my site visits and use it to personalize my successive visits, but may not transfer that information to other sites, except for the purpose of offering me books or CDs to my liking at a discount price or unless I am paid $200 in cash. If a site's stated privacy policies meet those specifications, my browser will enter the site. If not, it will either notify me or, more probably, simply bypass that site altogether.

If P3P works as its promoters claim, it might go a long way towards ameliorating Internet users' privacy concerns. But in order for P3P to be effective, a critical mass of users will have to use it. They will also have to insist upon bypassing web sites that either do not encode the site's privacy policies in P3P format or have onerous information practices. Without that critical mass, many commercial web site operators would no doubt prefer to lose the business of isolated P3P-armed customers than put at risk their lucrative trade in user data. Thus, especially given the imperfect substitutability of much Internet content, information asymmetries regarding personal data collection and aggregation, and the likelihood of oligopolistic producer market power as telecommunications mergers proceed apace, Internet users who wish to employ P3P will face a significant collective action problem. Unless a critical mass of additional users also employ P3P, the P3P pioneers will simply shut themselves out of most of the sites they want to visit. As a result, no one will employ P3P unless he can be assured that a critical mass of others will join him.[346]

It seems likely that government regulation requiring or inducing web site operators (and other purveyors of Internet content and services) to implement P3P will be necessary to overcome this collective action problem.[347] Even if P3P encoding is universal, web site operators may still resist

344. Of course, a web site operator might not abide by its stated privacy policy. *See infra* note 348 and accompanying text.

345. *See* BERNERS-LEE, *supra* note 106, at 147.

346. *See* Schwartz, *supra* note 147, at 1695 (referring to such user's "Hobson's choice" between "sacrificing either their privacy or their access to the Internet").

347. One way the state could induce site operators to implement P3P would be to enact default rules requiring a high standard of fair information practices. For a well-reasoned argument favoring such default rules, as well as mandatory rules regarding notice and an individual's right to inspect and correct personal data, see Schwartz, *supra* note 147, at 1670-79. *See also* Kang, *supra* note 317, at 1270 (advocating default rule that "unless the parties agree otherwise, personal data collected in the course of executing a cyberspace transaction can only be used in ways that are functionally necessary to the successful execution of that transaction"). Such default rules would, in effect, give users a property right in their personal information, transferable only through P3P-based transaction. *Cf*. Kenneth C. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, *in* U.S. DEP'T. OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION

user privacy demands. But then users (or more precisely, their browsers) will have at least a greater awareness of site information practices and will be able to engage in transactions to pursue users' privacy preferences.

Government may need to be involved in enforcement as well. There is nothing in P3P technology per se that would prevent a web site from deviating from its stated information practices.[348] Without the possibility of bringing legal action for such fraudulent misrepresentation, users will have to rely on industry self-policing, a notoriously toothless enterprise, or the virtual word of mouth, with all of its questionable veracity. Even aside from imposing sanctions on fraudulent sites, the production and dissemination of reliable information regarding web sites' compliance with their purported information practices is a classic public good. Because state institutions have sufficient impartiality to warrant trust and the authority to require all players to provide accurate information, it would likely fall to them to provide that good.

D. Unequal Access

The liberal democratic state must aim to provide its citizens with at least minimal access to the basic requisites of citizenship. Thus government arguably has an affirmative obligation to provide free and desegregated elementary and secondary education and free legal assistance to indigent criminal defendants, to underwrite the cost of counting ballots, and to forbid the poll tax.[349]

The duty to provide equal access has been particularly important in the area of public discourse and communication. State support for access to information has a long and venerable tradition. It has, indeed, been a basic tenet of our national communications policy to promote "the widest possible dissemination of information from diverse and antagonistic sources."[350] The Framers heavily subsidized the widespread distribution and consumption of the media of their day, constructing public libraries, imposing preferential postal rates and collection practices for newspapers, and maintaining postal roads for both post office and printers' private use.[351] That tradition has carried over into the era of electronic communication. Federal policy and successive pronouncements of the Supreme

---

AGE (1997), *available at* (visited Jan. 7, 2000) <http://www.ntia.doc.gov/reports/privacy/seflreg1.htm#1D> (favoring creation of a property right in personal information, held in the first instance by the individual whom the information is about).

348. Even if such technology is developed in the future, it might be vulnerable to web site operators' counter-technology. Avoiding costly technology wars is arguably one of the reasons for state definition and enforcement of property rights in such instances.

349. *See* Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier* (visited Oct. 17, 1999) <http://www.sjgames.com/ss/tribe.html>.

350. Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 192 (1997).

351. *See* Richard B. Kielbowicz, *The Press, Post Office, and Flow of News in the Early Republic*, 3 J. EARLY REPUBLIC 255, 257-59, 266, 275 (1983).

Court have emphasized the constitutional import of maintaining over-the-air broadcast stations that provide free public access to "a multiplicity of information sources."[352]

In parallel, universal service has served as a fount of telecommunications policy. Through a system of regulated telecommunications-provider monopoly and subscriber cross-subsidy, the government has sought to spread telecommunications to as many citizens as possible at "just, reasonable, and affordable" rates.[353] The goal of universal service has not abated even in our era of increasing telecommunications competition and deregulation. The Telecommunications Act of 1996 sets forth a complex formula for subsidized access to basic telecommunications services for rural areas and low-income consumers.[354]

Universal service has traditionally been limited to basic services, primarily telephony.[355] There is a growing sense, however, that as more and more information and discourse move to cyberspace, access to the Internet will become a prerequisite to full participation in democratic society.[356] Although only a beginning, the Telecommunications Act moves in the direction of including Internet access within the broad ambit of universal service policy goals. The Act maintains substantial subsidies for Internet communication.[357] It also provides for subsidized access to advanced services for schools, hospitals, and libraries.[358] Furthermore, the Act defines the scope of universal service dynamically: "an evolving

352. *Turner Broad.*, 520 U.S. at 226 (Breyer, J., concurring) (quoting Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 663 (1994)).

353. The requirement of "just, reasonable, and affordable" rates, traditionally a requirement of state public utility regulation, was explicitly incorporated into federal law in the Telecommunications Act of 1996. *See* 47 U.S.C. § 254(b)(1) (Supp. III 1997). For a brief, but helpful discussion of universal service policy, including recent applications, see Noam, *supra* note 250, at 958-63. Universal service is central to the telecommunications policies of other liberal states as well. *See id*. at 958.

354. *See* 47 U.S.C. § 254(h)(1)(A) (Supp. III 1997).

355. For a brief historical account of U.S. universal service policy, see Benjamin M. Compaine & Mitchell J. Weinraub, *Universal Access to Online Services: An Examination of the Issue*, 21 TELECOMMUNICATIONS POL'Y 15, 17-19 (1997).

356. *See* ROBERT H. ANDERSON ET AL., UNIVERSAL ACCESS TO E-MAIL: FEASIBILITY AND SOCIETAL IMPLICATIONS (Rand No. MR-650-MF, 1995), *available at* <http://www.rand.org/publications/MR/MR650.pdf> (maintaining that universal access to email is prerequisite to full participation in democratic society); Campbell, *supra* note 250, at 202-03. *But see* Compaine & Weinraub, *supra* note 355, at 31-33 (advising caution in extending universal service to online communication).

357. Internet service providers need neither pay access charges nor contribute to the universal service fund. *See* Bickerstaff, *supra* note 6, at 82-83 (noting these and other subsidies); Weinberg, *supra* note 6, at 225-26, 239 (same). In February 1999, however, the Federal Communications Commission ruled that dial-up Internet calls are interstate in nature and not local. *See* Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, 14 F.C.C.R. 3689 (1999). Although the ruling keeps intact existing reciprocal compensation agreements between telephone companies and Internet service providers, it could ultimately result in the imposition of per call fees on Internet service providers, which would likely be passed on to users.

358. *See* 47 U.S.C. § 254(h) (Supp. III 1997); *see also* Noam, *supra* note 250, at 960-61; Weinberg, *supra* note 6.

level of telecommunications services that the FCC shall establish periodically . . . taking into account advances in telecommunications and information technologies and services."[359]

In fact, cyberspace seems poised to become the principal arena for public discourse, carrying a wealth of information and opinion and bringing rich opportunities for user interaction. As that happens, netizenship may well become a necessary incident of effective citizenship in the liberal state. The question is what would happen in a regime of cyberspace self-governance? A vital part of self-governance is determining who has access to the self-governing community.[360] If netizens bore sole responsibility for determining Internet access, and if the federal government were concomitantly to terminate Internet subsidies, to what extent could we expect netizens to bear the burden of subsidizing access to those who otherwise would be left offline?

At bottom, it seems highly unlikely that netizens would bear such costs. Netizens do benefit from a large network of persons with whom they can communicate.[361] Among other benefits, adding subscribers increases the network's positive utility and spreads the high fixed costs of the network among more users, thus bringing down average costs.

Such network benefits do not continue ad infinitum, however. At some point, adding subscribers places burdens on network communication, whether by causing congestion or by increasing infrastructure costs. At such a point, additional subscribers are high-cost users, and the utility of adding still more members to the network correspondingly diminishes. This point arrives much sooner, of course, if existing subscribers must subsidize new ones. In that event, existing subscribers will have a strong incentive either to refuse to subsidize or to exit the network and establish a new one.[362]

Moreover, those dynamics and that gross disparity in access are likely to occur within cyberspace as well as between the online and offline worlds. The development of new technologies enabling unprecedented high-speed transfer of vast amounts digital information will likely lead to

---

359. 47 U.S.C. § 254(c)(1) (Supp. III 1997). The FCC has yet to expand universal service to Internet access for all citizens, but has supported subsidies for Internet access for schools and libraries. *See* Federal-State Joint Bd. on Universal Serv., 12 F.C.C.R. 87, 226 (Nov. 7, 1996).

360. As Stephen Holmes aptly puts it: "The core norms of equality before the law and majority rule cannot be put into practice until territorial borders have been firmly established and the question of who is a member of the community has been clearly answered." HOLMES, *supra* note 32, at 100; *see also* OSTROM, *supra* note 122, at 91 (concluding that defining resource boundaries and closing access to outsiders is the first, critical step in organizing for collective action).

361. My discussion here draws upon Noam, *supra* note 250, at 958-59, and Lemley & McGowan, *supra* note 114, at 560.

362. Network benefits may also vary depending on who is being added. "If I decide that I have no interest in communicating with people in East Harlem, then I will conclude that I enjoy no network benefits from their addition." Email from Jonathan Weinberg, Professor of Law, Wayne State University, to author (July 1, 1999).

what Saskia Sassen has labeled "cyber-segmentation." Even beyond unequal conditions for Internet access, "once in cyberspace users will also encounter an unequal geography of access—in this case to certain features, certain sites, and certain high-speed connections."[363] Under such a scenario, those netizens who can afford it and who live in premium telecommunications service areas will have access to high-speed access and high-quality content, including real time video. Others less fortunate will have access only to the Internet more or less as we know it today, except that content providers may increasingly gear their production to the Class A Internet, leaving the Class B Net all the poorer.[364]

In sum, even if we take the cyberian claim for self-governance seriously rather than viewing it as a fairy tale highly dependent on state funding, the claim provides no mechanism for a widespread distribution of citizenship or netizenship incidences. Cyberian democracy would at best be akin to that of the Athenian elite. On distributional grounds alone, it would fall far short of realizing liberal principles.

V
WHY THE STATE?

I have sought to show that a cyberspace unconstrained by the enforcement of liberal principles might more resemble Hobbes' Leviathan than Lockean civil society. But that raises a further intriguing question. Why must the liberal state be the ultimate enforcer of those principles? Why could not netizens create global meta-institutions within cyberspace to elucidate and enforce liberal norms? Perhaps, cyberians might argue, such cyberconstitutionalism could succeed where cyberpopulism, cybersyndicalism, and cyberanarchism could not.

Three possible objections to a cyberconstitutionalist claim come immediately to mind. First, a territorial liberal state cannot afford to allow an unproven cyberspace constitutional authority to be the guardian for liberalism in cyberspace when online activity so profoundly affects and intermeshes with the offline world. Second, because a cyberspace constitutional authority would likely be plagued by the same flaws that, cyberians insist, pervade territorial liberal states, the cyberian claim would gain little from the creation of such an authority. Third, a cyberconstitutional authority, unable to depend on questionable commitment by those it

363. Sassen, *supra* note 201, at 552.

364. Such cyber-segmentation is already a fact. It has been reported that 86% of Internet delivery capacity in the United States is concentrated in the 20 largest cities. In urban areas, moreover, high speed Internet service is largely unavailable to low income neighborhoods. *See* David Lieberman, *America's Digital Divide: On the Wrong Side of the Wires*, USA TODAY, Oct. 11, 1999, at B1; *see also* Bickerstaff, *supra* note 6, at 80 n.474 (citing studies finding that, even by 2002, only 25% of the total U.S. households with an Internet connection will use broadband services).

governs, would ultimately need to rely on a territorial liberal state to enforce the authority's decrees protecting liberalism.

The first objection arises because cyberspace norms and practice can impose significant externalities on the territorial liberal polity. Status discrimination, distortions in the virtual information arena, poor data privacy protection, and unequal access to cyberspace networks all undermine the rights of citizens in the offline world. Indeed, as the Internet assumes an ever greater role in political, cultural, and economic life, it makes increasingly little sense to distinguish such online illiberal phenomena from their offline counterparts. It is thus incumbent on the liberal state to ensure that liberal citizenship rights receive proper protection in cyberspace.

From the viewpoint of the liberal state, there would be no advantage—and considerable disadvantage—in delegating authority to a cyberconstitutional authority to interpret and enforce liberal meta-norms in cyberspace. The liberal state has existed for over 200 years. It has an established tradition of defining and applying liberal principles. The state's elucidation of those principles thus has considerable power in shaping social understandings and norms.[365] State-centered law—both legislation and constitutional adjudication—carries considerable weight in legitimizing certain beliefs and practices and delegitimizing others.[366]

A cyberauthority, in contrast, would have to start from scratch. It might be able to design mechanisms, including fines and suspension from the Internet, to enforce its constitutional proscriptions. But law enforcement power plays only a limited role in the creation, maintenance, and strengthening of norms. Liberal principles, like other norms embodied in formal rules, can affect behavior only if internalized by the population at large. The nascent cyberauthority would stand at a distinct disadvantage as compared to the state in efforts to facilitate this internalization. Even if netizens, who now comprise persons of widely varying backgrounds, attitudes, and interests, could agree on a constitutional structure, that structure would be highly unstable in the face of the frequent and dramatic change that characterizes the Internet. Law and the institutions of the liberal state can draw upon their long history to give them authority when presented with new challenges. Lacking such history, the cyberauthority could not.[367]

The second objection to the establishment of a cyberspace constitutional authority is that it would likely suffer from the very same deficits that, cyberians maintain, plague the territorial liberal state. The Internet Corporation for Assigned Names and Numbers (ICANN), poised to assume control from the United States government over Internet domain

365. *See* CASS R. SUNSTEIN, THE PARTIAL CONSTITUTION 166-67 (1993).
366. *See id.*
367. *See* Lemley, *supra* note 19, at 1269-70; Trachtman, *supra* note 19, at 576.

name administration, is a case in point.[368] ICANN's future power should not be underestimated. No one can establish a publicly accessible web site without an Internet domain name. Accordingly, if ICANN should decide that domain name registrars may (or must) deny registration unless the applicant forswears certain sorts of expression, meets specified criteria of "good standing," or pays a substantial fee, then those who fail to do so will effectively have no presence on the web.[369]

Not surprisingly, then, in what David Post colorfully describes as "Cyberspace's Constitutional Moment," ICANN has become the focal point of intense debate concerning the representation of various Internet constituencies on the Corporation's Board of Directors and about what sorts of checks and balances will be instituted to assure "just governance."[370] In its present configuration, ICANN's bylaws provide for a system of both geographic and interest group representation.[371] There will

---

368. The terms for ICANN's assumption of Internet domain names administration are set forth in a Memorandum of Understanding with the Department of Commerce. *See* Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation For Assigned Names and Numbers (1998), *available at* (visited Jan. 11, 2000) <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm> [hereinafter DOC-ICANN MOU].

369. ICANN's authority over domain name holders will derive indirectly from a chain of top-down contracts. ICANN will enter into contracts with entities that wish to serve as registries for various top level domain names (such as .com, .net, .rec, and the like). Those contracts will likely specify the terms of those entities' contracts with domain name registrars (firms that offer domain name registration services to users). In turn the registry-registrar contracts will likely 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 web sites 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 would ultimately settle on a single set of compatible root servers, and whichever entity controlled those servers would effectively assume ICAAN's power over domain name registration. *See* Jonathan Weinberg, *Internet Governance*, *in* TRANSNATIONAL CYBERSPACE LAW (Makoto Ibusuki ed., forthcoming 2000) (in Japanese), *English translation available at* (visited Sept. 27, 1999) <http://www.law.wayne.edu/weinberg/governance.PDF>.

370. David G. Post, *Cyberspace's Constitutional Moment*, AM. LAW., Nov. 1998, at 117.

371. For example, ICANN's 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.

Bylaws for Internet Corporation for Assigned Names and Numbers, art. V, § 6 (as amended and restated on Oct. 29, 1999), *available at* <http://www.icann.org/general/bylaws.htm> (visited Jan. 7, 2000) [hereinafter ICANN Bylaws]. The Bylaws also call for half of the corporation's Board to be selected by various constituencies. *See* ICANN Bylaws, *supra*, art. V, § 4. Despite this regional and constituency representation, ICANN's Bylaws seems to contemplate a Board of disinterested deliberators, rather than representatives of factions. They require Directors "to act in what they reasonably believe are the best interests of the Corporation and not as representatives of the subordinate

also be established an independent third party review panel, authorized to hear claims that the Board of Directors has "violated the Corporation's articles of incorporation or bylaws."[372] Among the Bylaws are provisions forbidding the corporation from applying its policies "inequitably" or subjecting any party to "disparate treatment unless justified by substantial and reasonable cause."[373] Membership composition and authority has also been a subject of controversy.[374] As those matters now stand, anyone who meets criteria to be set by the Board may register to vote in elections for the At Large Council,[375] which will in turn select half of the Corporation's eighteen directors.[376]

In short, ICANN's governing structure, as that of any more comprehensive cyberspace constitutional authority, will likely fall upon the same axes—and same fault lines—as territorial democracy: citizen versus representative, majority versus minority, special interest versus public interest, legislature versus judiciary. Those tensions cannot fully be resolved. Even at its best, therefore, cyberspace constitutional governance will share what cyberians perceive to be the fundamental flaws of its offline counterpart.

The third objection to a cyberspace constitutional authority is that even if such an authority were a desirable end, it is by no means certain that netizens could establish one without the involvement and backing of the liberal state.[377] A constitutional order is a public good. Such an order is

---

entity that selected them, their employers, or any other organizations or constituencies." ICANN Bylaws, *supra*, art. V, § 8.

For an illuminating public choice account of interest group capture of "private legislatures," such as the American Law Institute and Uniform State Laws, see Alan Schwartz & Robert E. Scott, *The Political Economy of Private Legislatures*, 142 U. PA. L. REV. 595 (1995).

372. ICANN's bylaws provide that the Corporation's "[i]nitial Board shall, following solicitation of input from the Advisory Committee on Independent Review and other interested parties and consideration of all such suggestions, adopt policies and procedures for independent third-party review of Board actions alleged by an affected party to have violated the Corporation's articles of incorporation or bylaws." ICANN Bylaws, *supra* note 371, art. III, § 4(b).

373. ICANN Bylaws, *supra* note 371, art. IV, § 1(c).

374. *See* Jeri Clausing, *Internet Body Feels Democracy's Tug*, N.Y. TIMES, Aug. 30, 1999, at C1 (reporting contentious debate regarding ICANN's membership structure and interest group representation).

375. *See* ICANN Bylaws, *supra* note 371, art. II, §§ 1-6. The At Large Council is to consist of 18 representatives, 2 each selected by the residents of each of the 5 specified geographic regions and 8 selected by the members as a whole. *See id*. art. II, § 7.

376. *See id*. at art. V, § 4.

377. ICANN owes its authority to its agreement with the United States government. *See* DOC-ICANN MOU, *supra* note 368. Moreover, agreements among ICANN, the Department of Commerce, and Network Solutions, Inc. (which acts as the registry for the .com, .net, and .org top level domain names) provide that the Department of Commerce may withdraw its recognition of ICANN by terminating its agreement with ICANN, and that in such event ICANN must assign to the Department any rights that ICANN has in all existing contracts with registries and registrars. *See* ICANN-NSI Registry Agreement ¶ 24 (Nov. 10, 1999), *available at* (visited Jan. 11, 2000) <http://www.icann.org/nsi/nsi-registry-agreement-04nov99.htm#16B>; Amendment 1 to Memorandum of Understanding (MOU) between the Department of Commerce (DOC) and the Internet Corporation

neither self-generating nor self-enforcing.[378] Its creation requires rational bargaining and some means to bind dissenters and holdouts. Even if initial agreement is achieved, the order's continued existence requires a mechanism to insure a high level of commitment in the face of ever-present incentives to defect. Where enforcement power cannot be supplied externally—in this case by the state—a commitment strategy must come from within.[379]

As Elinor Ostrom has shown, self-governing institutions do sometimes arise even without state enforcement.[380] However, a number of variables that are generally crucial to the establishment and maintenance of such institutions are absent in the case of cyberspace. These include a small number of decision makers, a homogeneity of interests, and a history of personal relationship and mutual trust.[381] In the absence of such qualities, a meta cyberauthority is highly unlikely to emerge or succeed.

Cyberians posit that cyberspace can generate emergent governing institutions. They make much of the fact that the Internet is built on a common technical communication protocol, and that informal emergent institutions such as the Internet Engineering Task Force were able to develop that protocol and "somehow [get] hundreds of millions of individuals across the globe to agree on a common syntax for their electronic conversations."[382] But, like other institutions of the early Internet, the Internet Engineering Task Force did consist of a small number of decision makers, with a homogeneity of interests and a personal relationship.[383] And as is evident from the debate regarding ICANN's authority and composite structure, that intimate insider consensus has given way to an interest-group sectarianism as fractious as any real-world politics.[384]

---

for Assigned Names and Numbers (ICANN) ¶ 5 (Nov. 10, 1999), *available at* (visited Jan. 11, 2000) <http://www.icann.org/nsi/amend1-jpamou-04nov99.htm>.

378. *See* COLEMAN, *supra* note 97, at 266-76 (detailing collection action obstacles to the emergence and maintenance of a political body to enforce pre-market cooperative agreements on basic market rules and entitlements); *see also* HOLMES, *supra* note 32, at 100 ("[N]o nation can become liberal unless it is already a nation . . . ."); Brilmayer, *supra* note 64, at 12-16 (arguing that social contract theory necessarily assumes the preexistence of a territorial sovereign); Posner, *supra* note 124, at 137-44 (discussing factors required for group solidarity).

379. *See* COLEMAN, *supra* note 97, at 275-76 (summarizing obstacles to such rational cooperation).

380. *See generally* OSTROM, *supra* note 122 (studying the evolution of nonstate institutions for the management of common pool resources).

381. *See id.* at 184, 188-90 (concluding that these components of social capital are likely crucial to the emergence and stability of self-governing institutions).

382. Post, *supra* note 115, at text following note 26.

383. Similarly, when the Internet was relatively small, the domain name roof servers were informally administered by a single person, Jon Postel, who gained the loyalty and respect of the Internet community. *See* Weinberg, *supra* note 369.

384. *See supra* note 371 and accompanying text; *see also* Clausing, *supra* note 374, at C1 (reporting concerns that ICANN governing bodies contain inadequate representation for individuals and public interest groups).

Cyberspace does contain one sort of social glue that might substitute for other commitment-enhancing variables found in smaller institutions. That is network benefits.[385] An Internet user wants the technical capability to communicate with everyone else on the Internet. A user, or group of users, who dissents by developing and using a different communications protocol will be unable to communicate with anyone else, and thus will forfeit substantial network benefits. As a result, even someone who fervently believes that she has invented a better protocol is likely to stick with the standard.

But network benefits may well prove insufficient to secure commitment to a complex constitutional regime. For one, the dissenter loses network benefits only upon removal from the network. While dissent from the standard communications protocol automatically removes the dissenter from the network, dissent from other policy would not. Network benefits will thus help to secure commitment only if the cyberauthority is able and willing to invoke the extreme sanction of suspension or expulsion from the principal cyberspace network in order to enforce compliance. In addition, the desire to remain on the network and the costs of establishing a competing network will not necessarily trump all reasons for dissent. The proliferation of filtering systems to block access to vast numbers of sites carrying what the filterer believes is objectionable content is evidence that network benefits may give way, at least in part, before other goals and concerns. It is doubtful, therefore, that network benefits would be sufficient to prevent secession from an overarching cyberauthority, especially over hotly contested political and social issues such as those mediated by political liberalism. A cyberspace constitutional authority, in sum, would ultimately be thrown back upon the liberal state for the enforcement of basic citizenship rights.

Cyberconstitutionalism thus fails on three counts to rescue the cyberian claim for cyberspace self-governance. First, the liberal state would likely be a more effective guarantor of liberal rights, both online and off, than would a new, independent cyberspace authority. Second, cyberconstitutionalism would likely resemble the "top-down" rule and interest group politics of the territorial liberal state, not the "bottom-up" ordering cyberians envision. Third, given insurmountable collective action problems, a cyberauthority is highly unlikely to emerge without the backing of the territorial liberal state.

385. *See supra* text accompanying notes 114, 175.

VI
THE CYBERIANS' INTERNATIONAL CLAIMS

I have thus far measured the cyberians' political claims against the benchmark of the territorial liberal democratic state. But the cyberians' argument has an international dimension as well. Cyberians assert what I will call "international claims," which parallel their claims of liberal perfection and community autonomy. In so doing, cyberians rightly emphasize cyberspace's global character, underscoring the transnational nature of both Internet communication and government efforts to regulate cyberspace activity. Cyberspace self-governance, they insist, is not merely a claim for autonomy against the domestic governmental institutions of Internet users' own countries. It is also a claim against foreign governments and international bodies that might seek to interfere with cyberspace activity. Seen in that light, to compare the cyberian vision solely with the domestic institutions of the liberal democratic nation-state, as I have done thus far, misses part of what the cyberian political claim is all about. This Part seeks to fill that gap.

Cyberians assert that cyberspace should be treated as a separate, self-governing jurisdiction in the international as well as domestic arena.[386] In support of this argument, they present two sorts of claims that draw upon liberal democratic theory. The first is directed against foreign government interference. Cyberians contend that a nation-state's imposition of jurisdiction over Internet users not physically present within the nation-state runs contrary to the principle of government by consent of the governed.[387] The second international claim is directed against the regulation of cyberspace by international organizations, including United Nations agencies and other arbitral and regulatory bodies that spawn from multilateral treaties. Cyberians assert that the liberal and democratic deficit that plagues even nominally liberal democratic domestic governments is exacerbated in international organs, where regulators are even farther removed from those they would regulate.[388]

A careful and complete consideration of the cyberians' international claims would require at least another full article. Here I will present only a very brief account of these claims. Likewise, I will offer only summary, tentative arguments in response, what I hope will be the rudiments of future exploration.

A. Foreign Government Interference

Consider the following hypothetical scenario:

---

386. *See, e.g.*, Johnson & Post, *Law and Borders*, *supra* note 2, at 1378-80.

387. *See generally* Johnson & Post, *Law and Borders*, *supra* note 2; Post, *supra* note 20.

388. *See* Johnson & Post, *supra* note 28, at 70-73.

> *Neo-Nazis living in Texas set up a web site on a server in their home state. The web site contains the content you might expect: racist and anti-Semitic diatribes, tributes to Hitler, and photos of Nazi memorabilia. The site professes to be open only to white Aryans, and prospective visitors are presented with a dialogue box requiring them to swear that they meet that requirement before being admitted to the site. Aside from that purported restriction, the site is accessible to any Internet user anywhere in the world, including Germany.*
>
> *Neo-Nazi speech of the type appearing on the web site is a crime under German law, as in many Western democracies.*[389] *A German prosecutor brings an indictment against the Texas neo-Nazis.*[390] *He contends that, because the site is accessible to those physically present in Germany, the site operators have violated German law forbidding neo-Nazi speech and fall within the jurisdiction of Germany's criminal courts.*[391]

Cyberians would argue that prosecuting foreign web site operators for violation of domestic law violates the liberal democratic principle of government by consent of the governed. In their view, Germany could not legitimately assert its criminal laws over the Texas neo-Nazis because the Texans have neither played any role in the laws' formulation nor consented to be bound by them. For cyberians, moreover, the example of the Texans illustrates why cyberspace should be treated as a separate, self-governing

---

389. Germany's Basic Law and criminal code provide German courts broad discretion to restrict neo-Nazi propaganda. *See* Eric Stein, *History Against Free Speech: The New German Law Against the "Auschwitz"—and Other—"Lies,"* 85 MICH. L. REV. 277, 286-322 (1986) (providing a translation and analysis of relevant parts of the German criminal code); David E. Weiss, *Striking a Difficult Balance: Combatting the Threat of Neo-Nazism in Germany While Preserving Individual Liberties*, 27 VAND. J. TRANSNAT'L L. 899, 928 (1994). Germany's Information and Communication Services Act, enacted in 1997, extends Germany's longstanding prohibition of neo-Nazi propaganda to Internet speech, providing that, in certain instances, Internet service providers can be held criminally liable for the dissemination of neo-Nazi speech on their networks. Informations-und Kommunikationsdienste-Gesetz, available in English translation at *Federal Act Establishing the General Conditions for Information and Communication Services: Information and Communication Services Act* (visited Jan. 7, 2000) <http://www.iid.de/rahmen/iukdge.html>. The Act is discussed in 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. R. 765, 792-95 (1998). Germany is far from alone in its efforts to proscribe neo-Nazi activity. *See* Kathleen E. Mahoney, *Hate Speech: Affirmation or Contradiction of Freedom of Expression*, 1996 U. ILL. L. REV. 789, 803 (1996) (noting that Austria, Belgium, Hungary, Italy, the Netherlands, Romania, Russia, and Switzerland have enacted laws to restrict hate propaganda).

390. On a number of occasions, German prosecutors have investigated Internet service providers because providers' German subscribers could access foreign neo-Nazi sites on the World Wide Web. *See* John F. McGuire, Note, *When Speech Is Heard Around the World: Internet Content Regulation in the United States and Germany*, 74 N.Y.U. L. REV. 750, 770 (1999).

391. This is merely a hypothetical. I am not aware of any case in which German authorities have sought to prosecute a foreign web site operator (as opposed to an Internet service provider) for violation of German law forbidding neo-Nazi speech, and I do not know whether German law could reasonably be construed to apply to a foreign web site operator.

jurisdiction. Given web sites' global accessibility, numerous web site operators regularly run afoul of foreign laws of which the operator is wholly unaware, enacted by a country that the operator has never visited.[392]

The cyberian argument comprises two basic propositions. The first is that Germany cannot properly legislate or otherwise prescribe law that applies to the Texans when the Texans have had no role in the law's formulation.[393] The second is that Germany cannot legitimately subject the Texans to the jurisdiction of a German court absent their physical presence in that country.[394] Both propositions are fundamentally incorrect as a matter of positive international law.[395] But the cyberian claim is not that Germany's actions violate international law. They argue rather that Germany's attempt to prescribe and adjudicate its law contravenes liberal democratic principles. It is to that theoretical point which I will now turn.

The cyberians' first proposition relates to a state's authority to enact laws applicable to conduct outside the state's territory. Cyberians challenge the legitimacy of state legislation affecting nonresident foreign nationals who have had no part in that country's political process. Such legislation, cyberians maintain, runs contrary to the principle of "government by the consent of the governed." As David Johnson and David Post contend, the consent principle "implies that those subject to a set of laws must have a role in their formulation."[396] However, Internet users generally have no right to vote or otherwise participate in the democratic process in countries in which they neither reside nor hold citizenship. Accordingly, as in our scenario concerning the Texas neo-Nazis, foreign law—even law enacted

---

392. *See* Johnson & Post, *Law and Borders*, *supra* note 2, at 1379-80.

393. For a definition of a state's jurisdiction to prescribe law, see RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(a) (1987) [hereinafter RESTATEMENT (THIRD) OF FOREIGN RELATIONS].

394. *See id.* § 401(b) (defining jurisdiction to adjudicate).

395. *See* Goldsmith, *supra* note 19, at 1240-44. Under international law, Germany has a right to prohibit the Texans' speech if the Texans can be said to have communicated their speech within German territory or, possibly, even if the Texans' speech is deemed to occur entirely in Texas but nevertheless has substantial effect within Germany. *See* 1 SIR ROBERT JENNINGS & SIR ARTHUR WATTS, OPPENHEIM'S INTERNATIONAL LAW 460, 472-76 (9th ed. 1992) (stating that customary international law allows a state to assert jurisdiction over offenses having their culmination in the state even if not begun there and, more controversially, over conduct taking place abroad that has substantial effects within the state); *see also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS, *supra* note 393, § 402(1)(c) (concluding that unless "unreasonable," a state has jurisdiction to prescribe law with respect to "conduct outside its territory that has or is intended to have substantial effect within its territory"). Under international law, Germany's right to subject the Texans to the jurisdiction of its courts is essentially coterminous with its right to prescribe law. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 313 (5th ed. 1998) (footnote omitted) (concluding that there is "no essential distinction between the legal bases for and limits upon" legislative and personal jurisdiction).

396. Johnson & Post, *Law and Borders*, *supra* note 2, at 1370; *see also* Post, *supra* note 20, at 542 ("However difficult it may be to argue that individuals or groups have consented to the application of a territorial state's exercise of power over them, it is far more difficult to make that argument in the context of the exercise of state *power against those who have no part in constituting the state's authority.*").

through local democratic process and otherwise comporting with liberal principles[397]—does not in any way reflect such Internet users' consent.[398]

The problem with this argument is that the Internet users' consent makes up only one side of the liberal democracy equation. Germany's exercise of legislative authority with respect to the Texans exemplifies a common irreconcilable conflict between realizing the democratic will of one country's citizens and imposing law on nonresident foreigners without their consent. The Texas web site, although physically located outside Germany, serves to disseminate neo-Nazi speech within Germany. At the same time, Germany's citizens, we may assume, have democratically chosen to prohibit the dissemination of neo-Nazi speech in their country. Indeed, German law combating neo-Nazism lies at the heart of Germany's postwar constitutionalism, born out of the trauma of that country's totalitarian past and designed to forge a "militant democracy," a liberal state capable of resisting those who would attack the constitutional order and foment ethnic hatred.[399]

Consequently, to deny Germans the possibility of applying their law to the web site operators would frustrate their fundamental expression of democratic self-rule. To be certain, Germany's effort to further its political ethos in the face of foreigners' Internet speech has spillover effects far beyond Germany's borders. But in our increasingly interconnected world (offline as well as online), many local ordinances have spillover effects in other countries.[400] To focus only on whether foreign residents have consented to those effects is to ignore the legislating country side of the liberal democracy equation. When, as in this case, foreign resident conduct has substantial effect within the legislating country and runs strongly against that country's fundamental public policy, the prescriptive outcome of the

---

397. Equating liberalism with the Internet slogan, "information wants to be free," cyberians might assert that any state-imposed constraint on speech, including the German prohibition of neo-Nazi expression, necessarily contravenes liberal principles. *See* John Perry Barlow, *The Framework for Economy of Ideas: Rethinking Patents and Copyrights in the Digital Age*, WIRED, Mar. 1994, at 83, 89 (crediting "information wants to be free" slogan to Stewart Brand); Barlow, *supra* note 1 (declaring that in cyberspace "all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits") While such an insistence on the primacy of free speech may be a tenable position, it does not comport with international understandings of liberal rights, at least as codified in human rights treaties. For example, the International Covenant on Civil and Political Rights, to which 144 countries are party, provides that "[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law." International Covenant on Civil and Political Rights, Dec. 19, 1966, 6 I.L.M. 368. For information regarding countries' signing, ratification, and accession to the treaty, see United Nations Treaty Collection, International Covenant on Civil and Political Rights (visited Jan. 4, 2000) <http://www.un.org/Depts/Treaty/final/ts2/newfiles/part_boo/iv_boo/iv_4.html>.

398. *See* Johnson & Post, *Law and Borders*, *supra* note 2, at 1370, 1375-76.

399. *See* Friedrich Kübler, *How Much Freedom for Racist Speech?: Transnational Aspects of a Conflict of Human Rights*, 27 HOFSTRA L. REV. 335, 336-37 (1998); Stein, *supra* note 389, at 278-79.

400. *See* Goldsmith, *supra* note 19, at 1240-42 (arguing that asserting prescriptive jurisdiction over cyberspace activity falls well within accepted principles of international law).

legislating country's democratic process should prevail. Accordingly, even though the Texas neo-Nazis have played no part in formulating Germany's law, its extraterritorial application still comports with liberal principles.[401]

The cyberians' second proposition questions a state's adjudicatory authority. It asserts that a state may not legitimately subject to its judicial process foreign nationals not physically present in that country's territory. Cyberians would contend in this regard that in addition to having no role in the formulation of the German prohibition, the Texas neo-Nazis have not consented to be bound by it. Johnson and Post concede that a person who physically enters a country's territory is generally deemed to consent to be bound by that country's laws.[402] But, they argue, cyberspace is different, and the difference derives from notice. Physical boundaries generally have "signposts that provide warning that we will be required, after crossing, to abide by different rules."[403] Cyberspace, on the other hand, lacks such signposts. "The Net enables transactions between people who do not know, and in many cases cannot know, each other's physical location."[404] The Texas neo-Nazis, in sum, might well not know or have any reason to know that people are visiting their site while sitting in front of computers in Germany. And even if they do know, the nature of Internet communication is such that information is available simultaneously everywhere, and thus not cannot really be said to exist in any particular physical location.[405]

The cyberians' second proposition is vulnerable on a number of counts. For one, as Jack Goldsmith and others have pointed out, cyberspace's global reach means that web site operators should reasonably

---

401. A hypothetical consent argument might support Germany's extraterritorial legislative authority argument as well. Customary international law generally permits a nation to extend its law to extraterritorial activity with substantial domestic effects. *See* Goldsmith, *supra* note 19, at 1208. The United States, acting through its various government officials, follows customary international law regarding a nation's extraterritorial legislative (or "prescriptive") authority. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS, *supra* note 393, § 402(1)(c). Accordingly, one could plausibly argue that the Texas neo-Nazis have indirectly, through their elected representatives (as well as non-elected officials appointed by those representatives), "consented" to Germany's legislative authority.

402. *See* Johnson & Post, *Law and Borders*, *supra* note 2, at 1370. The accepted understanding of transient jurisdiction comports with that of John Locke, who posited that by walking upon a country's highways a person tacitly accepts an obligation to obey that country's government. *See* JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT, §§ 119-21. Like others, Johnson and Post question the legitimacy of basing consent on mere physical presence, emphasizing that such consent has "a strong fictional element." Johnson & Post, *Law and Borders*, *supra* note 2, at 1398; *see also* Brilmayer, *supra* note 64, at 5 ("State reliance on consent inferred from someone merely remaining in the state is particularly unrealistic. An individual's unwillingness to incur the extraordinary costs of leaving his or her birthplace should not be treated as a consensual undertaking to obey state authority.").

403. Johnson & Post, *Law and Borders*, *supra* note 2, at 1370.

404. *Id*. at 1371.

405. *See id*. at 1375.

foresee the territorial ramifications of their activity.[406] To use Professor Goldsmith's example:

> A manufacturer that pollutes in one state is not immune from the antipollution laws of other states where the pollution causes harm just because it cannot predict which way the wind blows. Similarly, a cyberspace content provider cannot necessarily claim ignorance about the geographical flow of information as a defense to the application of the law of the place where the information appears.[407]

Nor, as Professor Goldsmith also discusses, would the Texas web site operators necessarily face a Hobson's choice of either complying with Germany's law or withdrawing from the web altogether.[408] By employing filtering technology, they could block access to those with German Internet addresses (although Germans who sought access through anonymous remailers could probably sidestep such controls),[409] or they could simply condition access on telephonic or facsimile proof of geographic location.[410] In addition, the Texas neo-Nazis could effectively avoid Germany's efforts to enforce its law by keeping themselves and their assets out of German territory.[411] In sum, Germany's application and enforcement of its law against the Texas web site operators would appear to comport with liberal principles, just as they would accord with international law and practice regarding extraterritorial jurisdiction.[412]

Yet underlying the cyberians' international claims is a more profound attack on Germany's efforts to prescribe, adjudicate, and enforce its law. To one degree or another, cyberians call into question not only the extraterritorial reach of Germany's law, but also the fundamental sovereign authority of Germany and other nation-states. They see in cyberspace a challenge to the nation-state's liberal credentials and continued efficacy. For cyberians, cyberspace is a realm in which individuals actually consent to the rules that govern them because they can always leave rule regimes they find repugnant. In contrast, citizens' consent to nation-state law "has a strong fictional element" because no one chooses where to be born and most can ill-afford to move to another country.[413] True consensual

406. *See* Goldsmith, *supra* note 19, at 1243-44; *see also* 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, 160 (1997) (discussing reasonable foreseeability in context of claims for copyright infringement).

407. Goldsmith, *supra* note 19, at 1244.

408. *See id.* at 1226-30, 1244.

409. *See* W. John MacMullen, *Anonymity, Privacy, and Security*, *in* INTERNET ISSUES AND APPLICATIONS, 1997-1998, at 67, 75-79 (Bert J. Dempsey & Paul Jones eds., 1998) (describing remailing technology).

410. *See* Goldsmith, *supra* note 19, at 1226-30, 1244.

411. *See id.* at 1219-21.

412. For a cogent argument that extraterritorial jurisdiction as applied to cyberspace activity comports, at least in principle, with international law and practice, see *id.* at 1239-44.

413. Johnson & Post, *Law and Borders*, *supra* note 2, at 1398-99.

self-government can thus best be realized by sharply reducing the province of nation-state law, by dispersing sovereignty among a "multiplicity of communities and political bodies," of which cyberspace networks and fora will play a central part.[414]

This is not the place to commence a discussion of the future of the nation-state in an age of global communication and increasing economic interdependence. As numerous commentators have argued,[415] however, I will contend that, at least for the foreseeable future, a global regime of semi-autonomous liberal nation-states represents the best means for fostering liberal rights and institutions. People live fundamentally in a territorially-based social and political culture. Cyberians may anticipate "the gradual displacement of the so-called natural world by the digitized fabricated creations of humans."[416] But such virtual world hegemony, together with its related notion of a transcendent cyberspace culture, "seems dangerously naïve in the face of people's frequent, intense attachment to their locality as the appropriate forum for self-assertion and democratic association."[417] Concomitantly, territorial nation-states remain essential guarantors of security, productive economic arrangements, health services, and other safety nets upon which a stable liberal order depends.[418] Moreover, international relations theorists increasingly view the activist liberal state as a springboard for protecting human rights worldwide, prompting calls for, among other measures, global jurisdiction for national

---

414. *Id*. at 1398 (quoting Michael J. Sandel, *America's Search for a New Public Philosophy*, ATLANTIC MONTHLY, Mar. 1996, at 57, 73-74); *cf*. DAVIDSON & REES-MOGG, *supra* note 15, at 117, 178-207, 301-03 (characterizing the coming "Information Age" as that of the "sovereign individual" and an age in which the nation-state will be reduced to its true role of "predatory institution," selling territorial protection services, with cyberspace occupying the realm of productive human endeavor).

415. *See, e.g*., Brillmayer, *supra* note 64, at 57; Louis Henkin, *That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera*, 68 FORDHAM L. REV. 1, 7 (1999); Michael Reisman, *Designing and Managing the Future of the State*, 8 EUR. J. INT'L L. 409, 416 (1997); *see also* DAVID HELD, DEMOCRACY AND THE GLOBAL ORDER 233-37 (1995) (viewing the nation-state as one among many overlapping centers for collective self-rule within an overarching framework of global democratic law); John Rawls, *The Law of Peoples*, *in* ON HUMAN RIGHTS: THE OXFORD AMNESTY LECTURES 1993, 41 (Stephen Shute & Susan Hurley eds., 1993) (contending that persons in the original position would choose to live in a world comprising territorial nation-states that respect basic human rights).

416. CURTIS E.A. KARNOW, FUTURE CODES: ESSAYS IN ADVANCED COMPUTER TECHNOLOGY AND THE LAW 35 (1997). Karnow's book is critically reviewed in Christopher M. Kelly, *The Cyberspace Separatism Fallacy*, 34 TEX. INT'L L.J. 413 (1999).

417. HELD, *supra* note 415, at 230 (referring to the naivety of notions of global culture and world government).

418. *See* Reisman, *supra* note 415, at 416; *see also* HOLMES, *supra* note 32, at 39, 100-01 (contending that liberalism has always presupposed and depended upon a strong territorially-bound state to enforce individual rights and guarantee individual security); LESSIG, *supra* note 12, at 3-4 (noting that, as has been acutely apparent in post-Communist Central and Eastern Europe, the absence of a strong state that both enforces and abides by the rule of law spawns hooliganism and civil strife, not libertarian utopia).

courts to prosecute human rights violations.[419] Such factors point toward a regime of what Brian Barry terms "cosmopolitan nationalism,"[420] a system of national institutions that constitute the principle (though certainly not exclusive) locus for implementing and adapting universal liberal principles.[421]

In sum, contrary to the cyberians' international claim, liberal principles may, in appropriate circumstances, support a democratic nation's extraterritorial application of its laws to foreign Internet users. The desire to further liberal principles also cautions against a cyberian position that would too quickly jettison the territorial liberal democratic nation-state.

B. International Organizations

Given what they perceive to be the practical difficulties of nation-state regulation of the global Internet, cyberians foresee, with considerable foreboding, a move towards cyberspace regulation by international treaty and international organizations.[422] Such a regime, they argue, would present in magnified form the failings of "top-down" nation-state administration. International regulators would be far removed from those they are seeking to regulate. Democratic institutions, which according to cyberians, stray far from the liberal democratic ideal at the national level would face insurmountable obstacles in the international arena. International regulatory bodies would both be unaccountable to their broad constituencies and subject to capture at the hands of organized, well-heeled factions.[423]

The cyberians' fear is not entirely unfounded. International treaties and organizations have been proffered as vehicles for Internet regulation in a number of instances.[424] Moreover, as many commentators have noted,

---

419. *See* Steven R. Ratner & Anne-Marie Slaughter, *Appraising the Methods of International Law: A Prospectus for Readers*, 93 AM. J. INT'L L. 291, 297-98 (1999) (noting trend toward recognizing and invoking universal jurisdiction for national courts to prosecute human rights violations).

420. Brian Barry, *Statism and Nationalism: A Cosmopolitan Critique*, *in* GLOBAL JUSTICE 12, 53-60 (Ian Shapiro & Lea Brilmayer eds., 1999).

421. *See id.* at 54 (discussing Jürgen Habermas' proposed "patriotism of the Constitution," a "patriotism [for Germans] based on loyalty to the universalistic political principles of liberty and democracy embodied in the constitution of the Federal Republic of Germany").

422. *See, e.g.*, Johnson & Post, *supra* note 28, at 70-73.

423. *See id.* at 72-73.

424. For example, prior to the creation of ICANN, the World Intellectual Property Organization (WIPO), a special agency of the United Nations, had sought to take a portion of Internet domain name administration under its wing. *See* Joseph P. Liu, *Legitimacy and Authority in Internet Coordination: A Domain Name Case Study*, 74 IND. L.J. 587, 601 (1999) (describing International Ad Hoc Committee formed by the WIPO and other organizations in 1996 to propose solutions to conflicts between trademarks and Internet domain names). The WIPO is still involved in making recommendations to ICANN regarding how to handle trademark-domain-name conflicts. *See* WORLD INTELLECTUAL PROPERTY ORGANIZATION, FINAL REPORT OF THE WIPO INTERNET DOMAIN NAME PROCESS (Apr. 30, 1999), *available at* (visited Jan. 7, 2000) <http://ecommerce.wipoint/domains/process/eng/final_report.html>.

rule through international organization does tend to suffer from a democratic deficit.[425]

Nevertheless, the cyberian juxtaposition of cyberspace self-governance to top-down regulation by international organs largely presents a false dichotomy. International law making and enforcement involve a wide variety of actors. Some are international agencies. But national institutions and nongovernmental organizations have come to play a significant role in this area as well. Indeed, as Anne-Marie Slaughter has observed, "today transgovernmentalism [cooperative regulation by national governmental institutions] is rapidly becoming the most widespread and effective mode of international governance."[426] This trend draws momentum from the Internet, which enhances possibilities for information sharing between, oversight by, and cooperation among lawmakers and regulators of different countries. National democratic institutions are bolstered in the process.[427] Moreover, not all international organs can be counted as democratic liabilities. Many serve, indeed, to enforce nation-state compliance with human rights treaties and to promote the transparency and accountability of domestic regulatory procedures.[428]

In sum, while cyberian concerns regarding a democratic deficit in certain international bodies may be justified, one cannot extrapolate from those instances to all "international" regulation of cyberspace activity. In many cases, we can assume, international—or transgovernmental—Internet regulation will further, not obstruct, liberal democratic principles.

CONCLUSION

Cyberians hail cyberspace as the pinnacle of "bottom-up" governance. Digital communication and data storage, they argue, enable us to overcome

---

425. *See, e.g.*, A. Michael Froomkin, *Of Governments and Governance*, 14 BERKELEY TECH. L.J. 617, 625-29 (discussing democratic deficit in treaty-making and decision making of the World Intellectual Property Organization); Peter L. Lindseth, *Democratic Legitimacy and the Administrative Character of Supranationalism: The Example of the European Community*, 99 COLUM. L. REV. 628, 633-42 (1999) (discussing the democratic deficit in European Community administrative institutions).

426. Anne-Marie Slaughter, *The Real New World Order*, 76 FOREIGN AFF. 183 (1997); *see also* Harold Hongju Koh, *How Is International Human Rights Law Enforced?*, 74 IND. L.J. 1397 (1999) (emphasizing the centrality of nation-state internationalization of international human rights norms and domestic judicial enforcement of those norms to international human rights regime).

427. *See* Henry H. Perritt, Jr., *Cyberspace and State Sovereignty*, 3 J. INT'L LEG. STUD. 155, 181-97 (1997) (discussing the Internet's potential role in the development of international and transgovernmental institutions, lending force to democratization and the rule of law).

428. *See* Patricia Isela Hansen, *Transparency, Standards of Review, and the Use of Trade Measures to Protect the Global Environment*, 39 VA. J. INT'L L. 1017, 1058-66 (1999) (favoring an approach to World Trade Organization dispute resolution that would encourage transparency in national regulatory procedures affecting international trade); Laurence R. Helfer & Anne-Marie Slaughter, *Toward a Theory of Effective Supranational Adjudication*, 107 YALE L.J. 273, 293-97, 337-85 (1997) (discussing European Court of Human Rights and United Nations Human Rights Committee).

geographical and cost barriers to disintermediated rule making. The virtual fora, networks, and rule regimes of cyberspace bring to fruition understandings and hopes of decentralized, extra-legal norm creation. They serve as a shining example of all that "private ordering" can be.

If so, we need to take a cold, hard look at some of the incongruities and limitations of private ordering. An untrammeled cyberspace would ultimately be inimical to liberal democratic principles. It would free majorities to trample upon minorities and would serve as a breeding ground for invidious status discrimination, narrowcasting and mainstreaming content selection, systematic invasions of privacy, and gross inequalities in the distribution of basic requisites for netizenship and citizenship in the information age.

It is thus incumbent upon the liberal state selectively to regulate cyberspace. Virtual association should enjoy considerable deference, no less—but no more—than its offline counterpart. But the most egregious illiberal practices and norms of the virtual world demand the cautious, but resolute intervention of international institutions and the territorial liberal state.