Developments in the Law—The Law of Cyberspace

Robert Bartlett

Berkeley Law

Follow this and additional works at: https://scholarship.law.berkeley.edu/facpubs

Part of the Law Commons

Recommended Citation

This Article is brought to you for free and open access by Berkeley Law Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.
"The ability of the World Wide Web to penetrate every home and community across the globe has both positive and negative implications — while it can be an invaluable source of information and means of communication, it can also override community values and standards, subjecting them to whatever more may or may not be found online . . . . [T]he Internet is a challenge to the sovereignty of civilized communities, States, and nations to decide what is appropriate and decent behavior.”


"In a world driven by the flow of information, the interfaces — and the underlying code — that make information visible are becoming enormously powerful social forces. Understanding their strengths and limitations, and even participating in the creation of better tools, should be an important part of being an involved citizen.”

Technorealism Overview (visited April 14, 1999)
<http:www.technorealism.org/overview.html>

"The stuff of a civilization consists largely of its substantive norms. . . . [T]hese informal rules — which have no identifiable author, no apparent date of origin, no certainty of attention from historians — are among the most magnificent of cultural achievements.”

ROBERT C. ELICKISON, ORDER WITHOUT LAW 184 (1991)

"Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. . . . [T]he content on the Internet is as diverse as human thought.”

TABLE OF CONTENTS

I. INTRODUCTION .................................................................................................................. 1577

II. COMMUNITIES VIRTUAL AND REAL: SOCIAL AND POLITICAL DYNAMICS OF LAW IN CYBERSPACE .................................................................................................................. 1586
   A. Community ...................................................................................................................... 1588
   B. "Virtual Communities" .................................................................................................... 1590
      1. The Shape of Online Communities to Date ................................................................. 1590
      2. Possible Future Configurations of Virtual Communities .............................................. 1593
   C. Law and Virtual Communities ......................................................................................... 1596
      1. Community as Common Project — Excluding Unwanted Speech ................................ 1596
         (a) Sexually Explicit Speech .......................................................................................... 1597
         (b) Libel ......................................................................................................................... 1599
         (c) Spam ....................................................................................................................... 1601
      2. Community as Bounded Membership — Excluding Unwanted Members ................. 1603
         (a) ISP Termination ....................................................................................................... 1604
         (b) ISP Discrimination .................................................................................................. 1605
         (c) Anonymity .............................................................................................................. 1607
      3. Community as Sovereignty — Making and Enforcing Rules ....................................... 1608
   D. Conclusion ....................................................................................................................... 1609

III. THE LONG ARM OF CYBER-REACH ............................................................................. 1610
   A. Introduction ..................................................................................................................... 1610
   B. Defamation ...................................................................................................................... 1612
      1. Recent Developments ................................................................................................... 1612
      3. Impact of Cyber-reach on the Constitutional Standards .............................................. 1617
   C. The Right to Speak in Cyberspace ................................................................................. 1622
      1. Recent Developments .................................................................................................. 1622
      2. A Closer Look at the State Action Doctrine ................................................................. 1624
      3. Impact of Cyber-reach on the Right to Speak in Cyberspace ....................................... 1629
   D. Conclusion ....................................................................................................................... 1634

IV. INTERNET REGULATION THROUGH ARCHITECTURAL MODIFICATION: THE PROPERTY RULE STRUCTURE OF CODE SOLUTIONS ................................................................. 1634
   A. Introduction ..................................................................................................................... 1634
   B. Content Control: Enabling the Private Regulation of Decency ...................................... 1637
   C. Privacy Protection: Contracting for a Property Right in Personal Information ............ 1644
   D. Copyright Protection: Balancing Access and Exclusion ............................................... 1649
   E. Conclusion ....................................................................................................................... 1656
V. THE DOMAIN NAME SYSTEM: A CASE STUDY OF THE SIGNIFICANCE OF NORMS TO INTERNET GOVERNANCE .............................................................................................................. 1657
   A. Introduction .............................................................................................................................. 1657
   B. The History and Leadership of the Internet ........................................................................... 1660
   C. Domain Name System Difficulties .......................................................................................... 1662
   D. Proposed Solutions ................................................................................................................. 1665
   E. The Road to ICANN .................................................................................................................. 1671
   F. The Importance of Norms: How to Make ICANN as Successful as Possible .................. 1676
   G. Conclusion .............................................................................................................................. 1680

VI. CYBERSPACE REGULATION AND THE DISCOURSE OF STATE SOVEREIGNTY .................. 1680
   A. The “Sovereign” Discourse ..................................................................................................... 1682
      1. The Realist Conception ........................................................................................................ 1683
      2. The Representational Conception ....................................................................................... 1686
      3. The Postmodern Conception ............................................................................................. 1688
   B. Reassessing Cyberspace, Sovereignty, and the State ........................................................... 1691
   C. The Issue of Personal Jurisdiction ......................................................................................... 1697
      1. Personal Jurisdiction and the Internet .............................................................................. 1697
      2. Reconstructing Personal Jurisdiction in Internet-Related Cases .................................... 1699
   D. Conclusion .............................................................................................................................. 1703
I. INTRODUCTION*

In years to come, historians may refer to 1998 as the year that the Internet solidified itself as an institution within mainstream American culture. Hardly a day passed without the traditional (but not yet irrelevant) media reporting a major Internet story. In May 1998, the Justice Department sued software giant Microsoft, the nation's largest company, for engaging in anticompetitive business practices. The allegations included a claim that Microsoft had attempted to leverage its monopoly over disk operating systems into the market for Internet browsers, computer software that enables users to "surf the Web," or link from one website to another. In September, Independent Counsel Kenneth Starr's report was available online almost immediately after Congress's decision to make the nearly five hundred page document public. Throughout the Monica Lewinsky scandal, which sparked this nation's first presidential impeachment hearing in 130 years, a handful of aggressive Internet news sites consistently "scooped" the traditional press on the latest developments in the investigation. In November, the business community was abuzz at the announcement of a proposed multibillion dollar, three-way alliance of Netscape, America Online, and Sun Microsystems. Meanwhile, sophisticated investors and dilettantes alike spent much of the year betting up the share price of online search engines, online booksellers, and Internet Service Providers (ISPs), many of which had yet to report a profit. Yet a surge in

* The Development authors would like to thank the Harvard Law School faculty for helpful guidance throughout this project, in particular: Lawrence Lessig, Anne-Marie Slaughter, and Jonathan Zittrain.

1 The size of the nation's largest corporations as measured by market capitalization is in constant flux, but recent figures indicate that Microsoft is the nation's largest company, with General Electric a close second. See The 100 Biggest Companies, WALL ST. J., Feb. 25, 1999, at R13.


4 See Amy Harmon, Tangled Web Tangles up the World Wide Web, N.Y. TIMES, Sept. 12, 1998, at AI.

5 See, e.g., James K. Glassman, Matt Drudge, E-Journalist, WASH. POST, June 9, 1998 (celebrating the rise of Matt Drudge, "the notorious Internet journalist who told the world about the liaison between Monica Lewinsky and President Clinton," and observing that the marketplace for news on the Internet poses "a threat to the people with the power today").

6 See Steve Lohr & John Markoff, Deal Is Concluded on Netscape Sale to America Online, N.Y. TIMES, Nov. 25, 1998, at A1 ("By moving quickly toward what both [Netscape and America Online] have recently come to see as the inevitable convergence of technology and media, America Online hopes that it will secure a solid lead in a battle already joined by giants like the Microsoft Corporation and the International Business Machines Corporation to transform the greater part of cyberspace into a vast virtual mall.").

7 See George Anders, Cybersqueeze: Comparison Shopping Is the Web's Virtue — Unless You're a Seller, WALL ST. J., July 23, 1998, at A1 (noting that amid heavy competition, many analysts do not expect Wall Street darling Amazon.com to post an annual profit until 2001); Rob-
sales during the holiday rush hinted at the prospect of future gains. For example, fourth quarter sales figures for Internet bookseller Amazon.com increased fourfold over the same period in 1997. By the end of 1998 there were perhaps two hundred million Internet users worldwide, and many analysts believe that by the year 2002, Internet commerce will account for more than $300 billion of U.S. GDP.

The Internet's tremendous growth must surprise even the most forward-thinking of its founders, who set up the ARPANet as part of a modest communications experiment funded by the federal government in the late 1960s. A principal goal of the ARPANet experiment was to develop a communications loop through which computers in remote locations could share data and "talk" to each other. The architects of the ARPANet envisioned a "decentralized, self-maintaining series of redundant links between computers and computer networks . . . designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war." In the years following the creation of the Internet, numerous fledgling networks with names such as BITNet, CSNet, and Usenet began to dot this new communications landscape. Initially these networks were not compatible and functioned independently. Today's Internet represents the culmination of efforts to link these individual networks into a

---

8 See George Anders, Amazon.com, eBay Post Blazing Growth, WALL ST. J., Jan. 27, 1999, at B6 (reporting that Amazon.com posted a 1998 fourth quarter loss of $46.4 million on revenue of $252.9 million, but that, according to the company's chief financial officer, the Internet bookseller was "profitable" during the December holiday rush).

9 It is impossible to derive a precise figure for the number of Internet users, but two hundred million is a common estimate. See, e.g., Reno v. ACLU, 521 U.S. 844, 850 (1997) (stating that the number of people who use the Internet was expected to reach two hundred million by 1999).

10 See Robert D. Hof, The Net Is Open for Business — Big Time, BUS. WK., Aug. 31, 1998, at 8 (citing predictions by Forrester Research, Inc.). In a later report, Forrester predicted that "global E-commerce revenue would reach $3.2 trillion by 2003, a figure that accounts for almost 5% of all global sales." Linda Himelstein, Robert D. Hof & Geoffrey Smith, Why They're Nuts About the Net, BUS. WK., Nov. 23, 1998, at 52. No one is more aware of this electronic commerce boom than Congress. See, e.g., 144 CONG. REC. S11,503 (daily ed. Oct. 5, 1998) ("I rise today in support of the Internet Tax Freedom Act. In recent years, Internet use has exploded, creating unprecedented opportunities for individuals and businesses. We must not allow a complicated patchwork of taxes to impede future opportunities.") (statement of Sen. Faircloth).


12 For a detailed, technical description of the history of the Internet as seen by some of its founders, see Barry M. Leiner et al., A Brief History of the Internet (visited Apr. 19, 1999) <http://info.isoc.org/internet/history/brief.html> (on file with the Harvard Law School Library).

13 ACLU, 929 F. Supp. at 831. Leiner and his co-authors downplay the defense aspects of the early Internet that are often emphasized by those recounting the early history of the Internet. See Leiner et al., supra note 12.

14 See ACLU, 929 F. Supp. at 832.

15 See Leiner et al., supra note 12.
global communications network of networks. Although the architectural principles underlying what was once called the ARPANet are conceptually similar to those supporting the Internet of today, the number of computers linked through the new medium of communication commonly termed "cyberspace" is exponentially greater.\(^{16}\)

Individuals are able to access the resources available on the Internet by using a computer that is directly\(^{17}\) linked to the Internet or by using a modem that connects a remote user via telephone to a computer that is directly linked to the Internet.\(^{18}\) Although universities, governmental agencies, and corporations often have their own computer networks that are directly connected to the Internet, individuals seeking modem-based access from their homes commonly reach the Internet by subscribing to ISPs, nationwide computer networks that are linked to the Internet.\(^{19}\) Once "on the Net," a user has various communications options, including "one-to-one messaging, . . . real-time communication, . . . [and] remote information retrieval."\(^{20}\) Electronic mail or "e-mail" is perhaps the most popular and well-known form of one-to-one messaging.\(^{21}\) A user can e-mail a message to another user simply by including the other user's e-mail address and then sending the message over the Internet. Once the addressee receives the message, he can open his mail and read its contents much as he would a letter delivered by the postal service. Real-time communication or "chat" allows users to engage in a dialogue over the Internet.\(^{22}\) The communication resembles a telephone conversation, except that rather than speaking, participants communicate by sending written messages that appear almost instantaneously on the recipients' computer screens.\(^{23}\)

The most widely recognized method of remote retrieval of information — "the search for and retrieval of information located on remote computers"\(^{24}\) — is the World Wide Web, which, simply put, "is a series of documents stored in different computers all over the Internet."\(^{25}\) The genius of the World Wide Web lies in its formatting language, 

\(^{16}\) At the end of 1969 there were four host computers connected to the ARPANet. See id. Today the number of hosts exceeds forty million. See Internet Domain Name Survey, January 1999 (visited Apr. 19, 1999) <http://www.nw.com/z/zone/www/report.html> (on file with the Harvard Law School Library).

\(^{17}\) As used here, the term "directly" includes computers linked to computer networks that are in turn connected to the Internet, as well as computers that are themselves connected to the Internet.

\(^{18}\) See ACLU, 929 F. Supp. at 832.

\(^{19}\) See id. at 833.

\(^{20}\) Id. at 834 (categorizing the "most common methods of communication on the Internet").

\(^{21}\) See id.

\(^{22}\) See id. at 835.

\(^{23}\) See id. at 834.

\(^{24}\) Id. at 835.

\(^{25}\) Id. at 836.
called hypertext markup language (HTML), which permits users to move rapidly from one document to another. Each HTML document on the Web has a unique address that corresponds to the computer on which it is stored. If users know the address of a document that they wish to see, they can then access it by typing its address into their Web browser. Users can also move from document to document by “hyperlinking” to other Web material. Typically a hyperlink takes the form of highlighted text describing the contents of another document. If the viewer of one document wants to view the contents of the document described by the link, then she simply “clicks” on the hyperlink, which “transports” the user to the address of the desired document. Because of the tremendous amount of material published in HTML format, the Web now provides educators, students, professionals, entrepreneurs, and ordinary citizens with a powerful tool for the acquisition and dissemination of information. The Web promises to become the public library of the twenty-first century and threatens to make the shopping mall a thing of the past. More than any comparable communications innovation, the Web epitomizes the Information Age.

Nonetheless, not every aspect of the Web and the Internet has been cause for fanfare and jubilation. On the periphery of the dramatic developments celebrated by the popular media, voices of concern and frustration have grown louder as Americans have started to acquire an appreciation for the costs, as well as the benefits, of the information revolution. Although ISPs have largely alleviated the connection bottlenecks that plagued Internet dial-up services as recently as two years ago, customers have recently complained about deluges of irritating — and often offensive — unsolicited e-mail messages, commonly termed “spam.” Online investors, seduced by the prospects of real-time trading and low commissions, have made charges to the SEC of fraud and outright theft. Anxious parents, often far less computer-savvy than their children, have decried the pervasiveness of online pornography and the ease with which predators can contact their children under the new medium’s cloak of anonymity. As companies from every sector of commerce and the federal government itself scramble to prepare for the Year 2000 Problem or “Y2K,” it remains uncertain what

26 See id.
28 See Patrick McGeehan, When Things Go Wrong: What Can You Do If You Have a Grievance About an On-line Trade?, WALL. ST. J., Sept. 8, 1998, at R15 (noting the rising number of complaints about online trading processed by both federal regulators and the National Association of Securities Dealers).
29 See, e.g., Lizette Alvarez, House Passes Bill to Crack Down on Pedophiles Exploiting Internet, N.Y. TIMES, June 12, 1998, at A16 (“Cyberpredators often cruise the Internet in search of lonely, curious or trusting young people.” (quoting Rep. Bill McCollum) (internal quotation marks omitted)).
havoc, if any, the turn-of-the-century computer glitch will wreak on
the Internet.30

Not surprisingly, the growing public awareness of the Internet's
unwieldy and chaotic side has led to calls for regulation and govern-
ance.31 The federal government first took aim at Internet pornogra-
phy by passing the Communications Decency Act of 1996 (CDA).32
Although the government claimed that the law's focus on protecting
minors rendered it fully consistent with the First Amendment,33 the
Supreme Court endorsed the position espoused by the ACLU and
other plaintiffs who had challenged the constitutionality of the stat-
ute.34 At times displaying broad admiration for the chat rooms and
webpages that make up the "vast democratic forums of the Internet,"35
the Court struck down the CDA in a 7–2 decision.36 Stressing that the
nature of the Internet is constantly evolving, at least one commentator
has warned that the ruling's apparent contingency on the state of the
Internet as understood by the justices at the time may make "claims of
victory by the opponents of Internet regulation . . . premature."37 One
lower federal court, however, has already greeted the Child Online

30 See, e.g., Phillip J. Nesser II, The Internet and the Millenium Problem (Year 2000) (visited
Harvard Law School Library) (concluding at this point in his consulting team's review of Internet
protocols that the Y2K problem will not disrupt the functioning of the Internet); see also Barnaby
J. Feder, Fear of the Year 2000 Bug Is a Problem, Too, N.Y. TIMES, Feb 9, 1999, at A1 (discussing
the varying levels of concern about the Y2K problem expressed by Americans).
31 See, e.g., Geeta Anand, Parents Want BPL to Block Porn on Internet, BOSTON GLOBE,
Feb. 12, 1997, at A28 ("City Councilor Maureen E. Feeney (Dorchester), responding to parents'
concerns, plans to ask the Boston City Council today to schedule a hearing on how to regulate
children's Internet access at the [Boston Public Library]."); Karen Kaplan, AOL Drops Plans to
fears that privacy rights are steadily eroding in cyberspace. Mounting public concern helped spur
the Federal Trade Commission to hold hearings in Washington last month to examine whether
government regulation is needed."); Aaron Lucchetti, Plan to Reduce Volatility on Nasdaq Hits
Hurdle, WALL ST. J., Feb. 3, 1999, at C1 (reporting less than unanimous support among traders
for the National Association of Securities Dealers' response to investor complaints about the wild
price volatility of some Internet stocks).
(1996).
33 See Reno v. ACLU, 521 U.S. 844, 864–66 (1997) (discussing and then rejecting the govern-
ment's contention that the CDA was a constitutional exercise of the government's interest in pro-
tecting children from harmful materials).
34 See id. at 861.
35 Id. at 868.
36 See id. at 849.
Protection Act, Congress's attempt to cure the constitutional flaws in the CDA, with skepticism.

Interestingly, just one day after a federal judge in Philadelphia enjoined the enforcement of the Child Online Protection Act, a federal jury in Portland, Oregon, awarded more than $100 million in damages to a group of plaintiffs who alleged that the operators of an anti-abortion website had posted materials that rose to the level of death threats. This distinction between private and public law standards for speech on the Internet is illuminating. It may suggest that the bounds of permissible regulation of Internet speech derive directly from established, real-space First Amendment jurisprudence, under which governmental attempts to regulate speech content are normally subject to strict scrutiny. Aggrieved private parties, however, may pursue each other in actions for libel, defamation, and death threats. But the distinction still leaves open the possibility that legislators will never be able to draft legislation generally applicable to the slippery contours and variegated user-communities of cyberspace without butting up against First Amendment concerns. Nor does it exclude the possibility that private parties accused of cyber-defamation will be able to command a level of constitutional protection that would be unavailable to them in real-space — a scenario that could arise if courts found that cyberspace makes the public-private distinctions hazier than they are in real-space.

The legal debate over the regulation of Internet speech is far from settled, but its layers of complexity shed light on the issues at the heart of the larger discussion about regulation of the Internet and the law of cyberspace. For instance, many commentators who view the Internet

39 See, e.g., ACLU v. Reno, 31 F. Supp. 2d 473, 497 (E.D. Pa. 1999) (granting a preliminary injunction against the enforcement of the Child Online Protection Act on the grounds that the law did not appear to be the least restrictive means of blocking minors' access to indecent material).
40 See id. at 498.
42 For example, after providing a description of the Internet to illustrate how the provisions of the CDA were intended to work, the Court distinguished the situation in Reno from prior cases in which the Court had upheld statutes that targeted speech content. See Reno v. ACLU, 521 U.S. 844, 864-68 (1997). Throughout his opinion for the Court, Justice Stevens relied on long-standing principles of real-space First Amendment law to justify his decision. See, e.g., id. at 868 (noting that although in some cases, the "scarcity" or "invasiveness" of a particular broadcast medium may justify governmental regulation, "[t]hose factors are not present in cyberspace").
43 This statement, of course, greatly oversimplifies a complex area of First Amendment jurisprudence. Part III of this Development examines the nuances of this area in greater detail. See infra Part III.
44 For a thorough discussion of this problem, see infra Part IV.
45 See infra Part III.
as a democratic paradise for the free play of ideas vehemently oppose attempts to apply conventional models of regulation to the Internet.\textsuperscript{46} Others, such as Professor Lawrence Lessig, contend that the law of cyberspace should evolve slowly through a careful application of common law principles, with particular attention paid to the aspects of cyberspace that make Internet transactions unique.\textsuperscript{47} Still others, such as Judge Frank Easterbrook, believe that the task of applying existing law to the Internet is straightforward.\textsuperscript{48} Notwithstanding the intense academic debate, as a practical matter, the sheer size of the Internet — whether measured by its explosively expanding user base, economic significance, or cultural impact — seems to make some form of Internet regulation both unavoidable and desirable.

What exactly one means by "regulation" is far less clear. As discussed above, Congress has already failed in its efforts to protect minors from the rampant availability of pornography on the Internet. Of course, as noted above, this instance of constitutionally flawed lawmaking may have had more to do with the First Amendment values at stake than the uniqueness of cyberspace. The SEC, for instance, may be able to prescribe regulations for the online trading of securities\textsuperscript{49} without similarly running afoul of constitutional rights, because the claim that the constitutional guarantee of speech trumps the government's interest in preventing fraud has never garnered much support.\textsuperscript{50}

Innumerable legal puzzles promise to plague the regulation of online trading and virtually every other cyberspace activity. For instance, how we imagine cyberspace — which, according to one view,


\textsuperscript{47} See, e.g., Lawrence Lessig, Symposium: Emerging Media Technology and the First Amendment: The Path of Cyberlaw, 104 YALE L.J. 1743, 1745 (1995) ("What is special about the common law here is its constructive function. What recommends it is the process that it offers, with its partial answers, to repeated if slightly varied questions, in a range of contexts with a world of different talent and ideals.").

\textsuperscript{48} See Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. CHI. LEGAL F. 207, 208 (1996) (arguing that rather than struggling to develop a body of "cyberlaw," those who wish to bring order to Internet transactions should concentrate on the optimal means of applying existing legal principles to the new medium).

\textsuperscript{49} See, e.g., Charles Gasparino & Michael Schroeder, SEC Steps up Oversight of Online Brokerages, WALL ST. J., Mar. 11, 1999, at C1 ("Last week, the agency introduced a proposed rule that some online brokers believe is aimed squarely at their industry. The SEC proposed that a broker-dealer would violate securities rules if the firm didn't have the 'operational capability' to handle their day-to-day activities.").

\textsuperscript{50} See, e.g., Frederick Schauer, The Speech of Law and the Law of Speech, 49 ARK. L. REV. 687, 690-91 (1997) (characterizing the registration requirements of the Securities Act of 1933 as content-based prior restraints on speech that are not understood as conflicting with the First Amendment).
exists wholly apart from real-space\textsuperscript{51} — will influence the determination of where transactions occur, and therefore affect assertions of jurisdiction. Thus, the SEC may have difficulty justifying a pursuit of the operators of a German website that offers to sell securities that are unregistered for the purposes of the Securities Act of 1933 simply because the website is accessible to investors in the United States. Likewise, free speech issues other than those raised in \textit{Reno v. ACLU} remain unresolved. For example, what if the SEC decided to bring an enforcement action against the German website operators for violating American securities laws? If the accused then accessed a chat room maintained by an ISP and used offensive language to complain about American laws or deluged other ISP customers with harassing e-mails to disseminate similar views, could the ISP pursue a court order enjoining such activity without running afoul of state action concerns? Would it be fully consistent with the First Amendment for the ISP, which is a private company but whose Internet chat rooms arguably constitute public forums, to prevent the offensive speech from reaching other customers through the use of “filtering” technology?

These are but a handful of the manifold questions that confound those who wish to introduce order to the Internet. This Development explores various modes of Internet governance by surveying many of the legal problems created by its growth and describing possible responses to these challenges. Part II of this Development examines the law’s impact on the “virtual community” and, in turn, on real-space life. It begins by briefly discussing the concept of community and its relationship to the law. It then describes some of the online communities observed to date and imagines future online life, in hope of better understanding which, if any, aspects of online life merit the “community” label. In its concluding section, Part II explores various legal issues bearing on online communities. It assembles many of the most important Internet cases to date, both to describe the shape of current doctrine and to demonstrate how concerns of community — both virtual and real — are central to an understanding of the actions of courts and lawmakers. Throughout, Part II argues that lawmakers should make themselves aware of the far-ranging implications that the legal rules under consideration may have on the future of virtual and real community life.

Part III coins the term “cyber-reach” to describe the ability of cyberspace to extend the potential reach of an individual’s voice. Contrary to traditional forms of mass communication, which tend to concentrate communications power in a limited number of hands, anyone with access to the Internet can interact with the rapidly expanding cyberspace audience. Cyber-reach accounts for much of the Internet’s

\textsuperscript{51} See Johnson \& Post, \textit{supra} note 46, at 1378–81.
rapid growth and perhaps holds the promise of the true and meaning-
ful "free trade in ideas" that Justice Holmes imagined eighty years
ago.52 Part III analyzes the potential impact of cyber-reach on Inter-
net defamation law and on the right to speak on "private property" in
cyberspace, concluding that cyber-reach challenges the traditional as-
sumptions that underlie current real-space legal doctrine.

Part IV examines the ways in which the Internet's architectural
code can be rewritten to address cyberspace problems. These "code
solutions" to cyberspace problems are evaluated in terms of Calabresi
and Melamed's property rule paradigm. Part IV analyzes code solu-
tions in three problem contexts: the accessibility of harmful material;
the collection of personal information; and the unauthorized use of in-
tellectual property. Recognizing the inevitability of regulation of the
Internet despite the theoretical appeal of self-governance through code
solutions, Part IV argues that when legislative bodies are considering
regulatory regimes, they should adopt schemes that resemble the prop-
erty rule protection method.

Part V focuses on Internet governance. It uses the controversy sur-
rounding the overhaul of the domain name system as a case study
through which to assess the value of traditional Internet norms to the
future of Internet governance. Part V first traces the evolution of
Internet norms, such as open participation, consensus-building, and
grassroots coordination, from the early history of the Internet through
the development of the domain name system. Second, it discusses the
recent controversy surrounding the domain name system and the vital
role that Internet norms have played in that arena. Part V illustrates
the key functions that norms have served in the construction of a new
regime of domain name governance, and concludes by evaluating the
effectiveness and future role of Internet norms.

This Development concludes with Part VI's analysis of the rela-
tionship between the Internet and the sovereign state. References to
sovereignty, ranging from governments' asserting sovereignty over
transnational Internet activities to libertarian claims that cyberspace
deserves its own "sovereign" status, have become commonplace in
Internet regulation discussions. This Part begins by analyzing the as-
sumptions about state sovereignty that underlie these arguments.
Once examined, these assumptions reveal their inherent indeterminacy,
casting doubt on arguments that seek to develop an Internet regulatory
regime from conceptions of state sovereignty. Part VI therefore sug-
gests an alternative approach for assessing government regulation of
the Internet that provides a clearer picture of the motivation of sover-
eign states to regulate the Internet and the legitimacy of these regula-

tions. Part VI concludes by applying this approach to the current debate about personal jurisdiction in Internet-related cases.

The Internet has rapidly become an influential social, economic, and political force of the modern world. Although it has functioned in one form or another for over thirty years, the law of cyberspace is truly in its infancy. Any attempt to "review" the law of cyberspace is destined to be incomplete, but by capturing and examining the forces that are currently at work, this Development attempts to offer a glimpse of what the law of cyberspace could look like in the future.

II. COMMUNITIES VIRTUAL AND REAL: SOCIAL AND POLITICAL DYNAMICS OF LAW IN CYBERSPACE

The Internet's growth is certain to continue, as the Internet demonstrates that it is no longer a marginal medium, but rather is increasingly relevant to ordinary people in ordinary life — families e-mail to stay in touch, consumers shop on the Web, and citizens inform themselves through online news and information resources. The ability of online users to interact in sophisticated ways, forming "virtual communities," may be what most differentiates the Internet from past developments in communications technology. Internet technology enables people to "meet, and talk, and live in cyberspace in ways not possible in real-space." It permits "many-to-many communication" unattainable with past technologies, which enabled only one-to-one or broadcast communication.


2 See, e.g., Amy Harmon, Guess Who's Going On Line, N.Y. Times, Mar. 26, 1998, at G1 ("The newfound infatuation with E-mail ... is prodding scattered families to reconvene in cyberspace . . . .")


4 Howard Rheingold, The Virtual Community 5 (1993) (defining "virtual communities" as "social aggregations that emerge from the Net when enough people carry on ... public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace").

5 See Lawrence Lessig, The Path of Cyberlaw, 104 Yale L.J. 1743, 1745-46 (1995) [hereinafter Lessig, Path] ("What will be new are the communities that this space will allow, and the constructive . . . possibilities that these communities will bring.").

6 Id. at 1746.

The "virtual community" label, however, has been used loosely by many legal scholars — sometimes describing all users of the Internet⁸ and sometimes characterizing discrete subsets of users.⁹ To better understand the oft-hailed political and social potential of virtual communities,¹⁰ one must analyze what types of "community" life are occurring — and could potentially occur — online.¹¹

How and why does this matter in the eyes of the law? Legal rules — statutes, court decisions, and deference to extra-legal mechanisms such as norms, markets, and programming code¹² — will be crucial in determining what sorts of communities thrive in cyberspace and what sorts of communities do not. Not only will these rules affect people's cyber-lives, but because cyberspace life is becoming more entwined with real-space life, the rules governing virtual communities will also influence our real-space communities. Legislatures and courts have begun to encounter the Internet, as have legal scholars. The perspectives offered by lawmakers, judges, and scholars are all grounded in various premises about online life and its potential for "virtual community."¹³

This Part explores the law's impact on "virtual community" and, in turn, on "real-space" life. Section A briefly discusses the concept of community and its relation to law. Section B then describes some of the online communities seen to date and forecasts future online life, in

---


⁹ See Anne Wells Branscomb, Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces, 104 YALE L.J. 1639, 1640 (1995) (stating that experimental user groups called virtual communities "can be said to occupy separate and diverse cyberspaces").

¹⁰ See, e.g., ESTHER DYSON, RELEASE 2.1, at 46-47 (1998) (discussing the "great Net hope"); MIKE GODWIN, CYBER RIGHTS 15 (1998) (arguing that virtual communities "promise to restore" a "stable sense of community, of place" in America); RHEINGOLD, supra note 4, at 14 (recognizing the Internet's potential to "revitalize the public sphere").

¹¹ The forms of possible online life, as defined by the computer programming code, are many, and not all of them have yet been seen or experienced; no one "inherent" cyberspace community exists. See Lawrence Lessig, The Zones of Cyberspace, 48 STAN. L. REV. 1403, 1408 (1996) [hereinafter Lessig, Zones] (claiming that "cyberspace is socially constructed"). But see GODWIN, supra note 10, at 302 (discussing the "values inherent in the Net"). Moreover, the shape of online community life has already begun to transform. From the early days of interactive, noncommercial, textual exchange, Internet use has moved toward increasingly less interactive, multimedia, commercial intercourse. See Andrew L. Shapiro, The Disappearance of Cyberspace and the Rise of Code, 8 SETON HALL CONST. L.J. 703, 710 (1998) (describing how early, vibrant communities are being supplanted by less creative uses of the Net).

¹² See Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 JURIMETRICS J. 629, 669 (1998) [hereinafter Lessig, Speech] (listing these factors, in addition to law, as factors involved in regulating online speech).

¹³ Many commentators have argued that regardless of how carefully designed Internet legal rules are, they may be irrelevant because they are largely unenforceable, as a result of both jurisdictional and practical constraints. See, e.g., Lessig, Zones, supra note 11, at 1405–06 (discussing the viewpoints of regulation skeptics, including Johnson and Post). However, as Professor Lessig suggests, this skepticism may be overstated, particularly considering the law's potential to regulate programming code. See id.
order to better understand which, if any, aspects of online life merit the "community" label. Finally, section C examines various legal issues bearing upon online communities. This section endeavors to assemble many of the most important Internet cases to date, both to describe the shape of current doctrine and to show how community concerns — both virtual and real — are central to understanding the actions of courts and legislators. Throughout, I argue that lawmakers and policymakers should consider the wide range of existing and potential group life in cyberspace, as well as the implications of legal rules for virtual and real communities.14

A. Community

Many commentators have cited the advent of the Internet and its potential to connect people in new ways as solutions to the problem of declining community in modern America.15 For example, Mike Godwin writes that "virtual communities promise to restore to Americans . . . a stable sense of community, of place."16 Howard Rheingold touts the Internet as "a tool that . . . might help revitalize the public sphere."17 Although technology in general is often cited as a factor contributing to the decline of community,18 the Internet's link to this putative decline remains a major topic of dispute, as commentators consider whether the Internet's ability to enable interactive communication might enhance civic participation and association.19

Defining "community" will help frame the ensuing legal discussion, and will enable an evaluation of whether various forms of virtual life may properly be viewed as community. Many scholars have noted the elusiveness of a definition of "community,"20 a term that is complicated

14 As Professor Lessig has written, "[t]hey are making, not finding, the nature of cyberspace; their decisions are in part responsible for what cyberspace will become." Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY L.J. 869, 904 (1996) [hereinafter Lessig, Reading] (discussing how courts' "findings" about cyberspace impact the shape cyberspace takes).
16 GODWIN, supra note 10, at 15.
17 RHEINGOLD, supra note 4, at 14.
18 See, e.g., DAVID B. WHITTLE, CYBERSPACE: THE HUMAN DIMENSION 287-88 (1997) (suggesting social "disjuncture" due to technology); Putnam, supra note 15, at 75 (describing the role in community's decline played by the increasingly private and individualized leisure fostered by technology); Richard E. Sclove, Making Technology Democratic, in RESISTING THE VIRTUAL LIFE 85, 85 (James Brook & Iain A. Boal eds., 1995) (discussing technology's potential to weaken community interactions). But see BENEDICT ANDERSON, IMAGINED COMMUNITIES 40-49 (1983) (explaining how the rise of print media helped create national community).
19 See, e.g., Putnam, supra note 15, at 76 (expressing interest in the potential for electronic networks either to contribute to or to stem civic decline).
by its central position in the debate between communitarians and liberals.\textsuperscript{21} Nevertheless, many agree that not all voluntary associations of individuals can necessarily be viewed as communities.\textsuperscript{22}

Traditionally, geography has helped to indicate community.\textsuperscript{23} Although geography arguably remains important in defining virtual community,\textsuperscript{24} we are better served in the Internet context by an “experiential” conception of community, rather than a geographic one.\textsuperscript{25} Commentators have used several factors to define community, including: continuity of membership; shared experiences, progress, deliberation, and goals among members; personal investment of members;\textsuperscript{26} established boundaries; and the ability to distinguish members from nonmembers.\textsuperscript{27} For present purposes, three main factors will be used to distinguish “true” communities from other groups: a common purpose or project involving sustained interaction among members; boundaries, with some group control over membership and exit; and a degree of group governance over group norms and behavior.

What is the legal significance of identifying a group as a community? In general, communities generate and perpetuate legal norms.\textsuperscript{28} For example, community norms receive deference when “community standards” are used to determine whether a crime or tort has been committed.\textsuperscript{29} Territorial sovereigns can recognize communities not

\textsuperscript{21} See, e.g., Gregory S. Alexander, Dilemmas of Group Autonomy: Residential Associations and Community, \textit{75 Cornell L. Rev.} \textbf{1}, 17–23 (1989) (summarizing the fundamental debate about the nature of legal rights, duties, and identity). \textit{See generally} Stephen Mulhall & Adam Swift, Liberals and Communitarians (1992) (exploring communitarian and liberal claims). This debate certainly affects an analysis of how virtual communities may or may not mesh with American law and society. As Professor Alexander notes, depending on one’s ideological orientation, the proliferation of voluntary associations (arguably the proper label for emerging virtual “communities”) may or may not enhance true community. See \textit{Alexander, supra} at 23.

\textsuperscript{22} See \textit{Alexander, supra} note 21, at 26–27. This Part formulates a working definition of “community” broad enough to allow those with varying ideologies to make use of the analysis, realizing that one’s fundamental conception of the role and meaning of community will have much to do with one’s understanding of the role and meaning of cyberspace groups.

\textsuperscript{23} See \textit{id.} at 24 (explaining the traditional, territorial conception of community).

\textsuperscript{24} For example, some of the most successful early virtual communities, such as the WELL, had a geographic center (in the WELL’s case, the San Francisco Bay area) and involved community members meeting in real-space. See, e.g., Rheingold, \textit{supra} note 4, at 2 (“The WELL felt like an authentic community to me from the start because it was grounded in my everyday physical world.”).

\textsuperscript{25} See \textit{Alexander, supra} note 21, at 25–26 (discussing an “experiential” conception of community).


\textsuperscript{28} See \textit{Post, supra} note 20, at 476–77.

\textsuperscript{29} This deference can be seen in the legal standards developed for obscenity cases. See, e.g., William S. Byassee, Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community, \textit{30 Wake Forest L. Rev.} \textbf{197}, 207–08 (1995) (discussing the federal obscenity test of local “contemporary community standards” articulated in \textit{Miller v. California}, \textbf{413} U.S. 15 (1973)).
only by leaving these groups alone, but also by enforcing community rules. The law may give communities a sphere of autonomy through the principle of freedom of association, or it may grant communities — such as churches, corporations, and civic associations — the power of self-governance, enforceable in courts of law.

B. "Virtual Communities"

At this point, the reader may be skeptical about the connection between traditional notions of community and Internet interactions. This skepticism is understandable, particularly because the term "virtual community" is often casually invoked to describe divergent online experiences. Many members of these online groups report, however, that they experience the feeling of being part of a community, and thus we should judge their claims of community membership seriously, as well as anticipate emerging online life that may be even more persuasively described as community.

1. The Shape of Online Communities to Date. — Presently, Internet technology enables several forms of interactive networking among users, including "[t]raditional activities indicative of geographic communities, such as town meetings, exchanging information, discussing problems, coping, and informal chatting." Although these uses may popularly be seen as unusual, they merit exploration not only because they were some of the earliest uses of networked computers, but also because they suggest the possibilities of Internet life beyond the currently more popular cyber-commerce and Web-surfing. Several thorough descriptions of these communities already exist. A brief


31 See Henry H. Perritt, Jr., Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?, 12 BERKELEY TECH. L.J. 413, 451-63 (1997). In many cases, "contract law provides the mechanism for beginning the process of self-governance" because territorial sovereigns enforce these private arrangements. Id. at 476.

32 See Giordano, supra note 27, ¶ 10 ("To the uninitiated, it may seem ironic and even dubious that a sense of community can arise within the sterile environment of a computer network.").

33 See, e.g., RHEINGOLD, supra note 4, at 2.

34 See, e.g., GODWIN, supra note 10, at 23 (urging greater understanding of virtual community life).


36 See Shapiro, supra note 11, at 710.

37 See, e.g., GODWIN, supra note 10, at 5-8; Byassee, supra note 29, at 200-03; Lessig, Path, supra note 5, at 1746-47; Zittrain, supra note 7, at 496-98. See generally RHEINGOLD, supra note 4 (detailing various types of online life).
catalog includes: bulletin board systems,38 conferencing systems,39 Internet Relay Chat,40 Usenet,41 e-mail lists,42 and MUDs/MOOs.43 Access to the Internet and these services44 is provided through commercial Internet Service Providers (ISPs) such as America Online (AOL) or CompuServe that offer a range of member services in addition to Internet access, through network access in universities and workplaces, or through dial-up ISPs.45

The WELL and LambdaMoo provide vivid examples of the capability of online groups to facilitate sustained and meaningful interaction among members. The WELL is a large conferencing system, centered in the San Francisco Bay area.46 Its members have been among the most noted contributors to the literature on virtual communities, recounting experiences of online discussions, jokes, fights, and relationships.47 LambdaMoo became infamous after the oft-cited “Rape in Cyberspace,”48 in which a member of the MOO gained control of another user’s character and forced that character to perform offensive

38 Called BBSs, these are sites onto which users post messages either publicly or privately to other users. See GODWIN, supra note 10, at 7; RHEINGOLD, supra note 4, at 8–9.
39 These systems are high-capacity BBSs, such as the WELL or AOL, which often offer additional services, such as real-time “chatting.” See GODWIN, supra note 10, at 7.
40 Also known as IRC, this program enables groups of people to congregate in “chat rooms” for real-time discussion in text. See RHEINGOLD, supra note 4, at 176–88.
41 Usenet is a large network of newsgroups accessible by the Internet, segregated by topic, onto which anyone can post messages in response to those posted by others, and in which the history of the discussion remains accessible to all who visit. See GODWIN, supra note 10, at 7–8.
42 Often called “listservs,” e-mail lists are mass-mailings sent to other members of a group. Recipients can often respond to the entire group, or without other members knowing, only to particular group members. See David S. Bennahum, The Hot New Medium Is . . . Email, WIRED, Apr. 1998, at 104.
43 These are the abbreviations for “Multi-User Dungeons” and “MUDs object-oriented,” respectively — sophisticated, fictitious, user-created worlds in which players invent roles and interact in a variety of public and private spaces. See GODWIN, supra note 10, at 40; RHEINGOLD, supra note 4, at 145–75.
44 See GODWIN, supra note 10, at 7–8.
45 See BYASSE, supra note 29, at 200.
46 See Katie Hafner, The Epic Saga of The Well, WIRED, May 1997, at 98. The WELL’s geographic center was not originally intended, but as members began to meet in real-space to supplement their online interactions, geographic proximity among members became important. See id.
47 Many writers have extensively chronicled WELL life. See, e.g., GODWIN, supra note 10, at 34–40; RHEINGOLD, supra note 4, at 1–64; Cliff Figallo, The WELL: A Regionally Based On-Line Community on the Internet, in PUBLIC ACCESS TO THE INTERNET 49, 49–61 (Brian Kahin & James Keller eds., 1995); Hafner, supra note 46, at 98. ECHO, a similar system based in New York City, has also received considerable attention. See, e.g., STACY HORN, CYBERVILLE (1998) (providing a window into the online lives of ECHO members).
48 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 293, 295–96 (Mark Stefik ed., 1996); see Giordano, supra note 27, ¶¶ 49–72.
acts, to the outrage of many long-time community participants. Much has been written about how LambdaMOO members responded to the member's transgression of unwritten group norms. Governance of the communities described so far varies— from unwritten norms, to moderation of discussion and regulation of conduct by systems operators (sysops), to formally enforced rules. In addition to different forms of governance, these groups differ in membership size and participation prerequisites. Furthermore, depending on the code used to construct the group, users may or may not be allowed to participate anonymously or pseudonymously or to observe the group's doings without detection. Despite the various configurations, many of these groups' members share a sense that community exists.

Other uses of the Internet arguably create community, although to a lesser degree than the sophisticated arrangements just described. The World Wide Web enables Internet users to access "websites" from computers around the globe. Generally, each site contains a directory of webpages, which frequently possess audiovisual and interactive capabilities and increasingly provide access to chat groups and bulletin boards related to the website's topic. Although many argue that the Web does not provide enough interactivity to establish community, some sites—for example those featuring support groups for issues such as women's health or alcoholism—indicate the Web's community potential. Some commentators suggest that Internet commerce, which has flourished recently, may itself foster community.

49 See Giordano, supra note 27, ¶¶ 60-62 (describing how a character named "Mr. Bungle" infiltrated the MOO, raping one character and forcing another to "enact a ritual of self mutilation").

50 See id. ¶¶ 62-72.

51 See Perritt, supra note 31, at 437-42; Zittrain, supra note 7, at 498-501.

52 See Zittrain, supra note 7, at 501-06.

53 See Perritt, supra note 31, at 449-50.

54 See GODWIN, supra note 10, at 133-37.

55 This practice is called "lurking." See WHITTLE, supra note 18, at 60.

56 Mike Godwin provides a helpful introductory description of the Web. See GODWIN, supra note 10, at 5-9.

57 See, e.g., Falk, supra note 26, at 290.


61 One of the most prominent accounts of the commercial potential of the Internet suggests that commercial intercourse generates community. See JOHN HAGEL III & ARTHUR G. ARMSTRONG, NET GAIN: EXPANDING MARKETS THROUGH VIRTUAL COMMUNITIES at xi (1997) ("Our view is that the profit motive will in fact create new forms of virtual communities whose strong commercial element will enhance and expand the basic requirements of community..."
Additionally, ISPs such as AOL might arguably function as communities, albeit large and diverse ones, as might workplace e-mail networks and community cooperative networks. These arrangements all offer some aspects of community, such as regularity of membership and common experience, although they may lack the robust interaction of the online communities described earlier. Possibly the most significant aspect of these more mainstream uses of the Internet is not their status as alternative communities, but the opportunities they offer for individuals to supplement life in real-space communities.

2. Possible Future Configurations of Virtual Communities. — As technologies advance, programming code has great potential to provide users with any kind of Internet community they desire. Thus, some commentators have cautioned against assuming a fixed "nature" of the Internet or virtual communities, lest judges and lawmakers "perceive the new technology in that early, clumsy form, which then becomes their image of its nature, possibilities, and use." Judges and others referring to the nascent Internet have celebrated its open, decentralized structure, but such descriptions are "not to say ... how cyberspace has to be." Before discussing the law's role in shaping these communities, it will be useful to explore how technology, markets, and other extra-legal forces may potentially shape the evolving cyberspace. In this regard, three issues factor most importantly in the evolution of virtual communities: how public and private spaces in cyberspace are designated; to what degree the online experience is tailored to individual preferences; and how the Internet meshes with other technologies.

— trust and commitment to each other.); see also Dyson, supra note 10, at 57–61 ("Many markets are communities, not just mechanisms for setting prices.").


See, e.g., Doheny-Farina, supra note 62, at 37; Laura J. Gurak, Persuasion and Privacy in Cyberspace 132 (1997); Whittle, supra note 18, at 411.

Cf, e.g., Shapiro, supra note 11, at 714–15 (anticipating a blending of life in real-space and cyberspace); Jon Katz, The Digital Citizen, Wired, Dec. 1997, at 68 (observing that the online world features many of the "real" world's most active citizens).

See infra p. 1635.

See, e.g., Branscomb, supra note 9, at 1678–79 (cautioning against making such assumptions about cyberspace).


See, e.g., ACLU v. Reno, 929 F. Supp. 824, 881 (E.D. Pa. 1996) (Dalzell, J., concurring) ("[The Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country — and indeed the world — has yet seen."); aff'd, 521 U.S. 844 (1997); Godwin, supra note 10, at 302.

Lessig, Reading, supra note 14, at 888. Lessig notes that "cyberspace has no permanent nature, save the nature of a place of unlimited plasticity." Id.
One of the most challenging current questions is the distinction between public and private on the Internet. As Web access becomes increasingly "channeled" through commercial "portals" and "mega-sites," the question arises whether public, open spaces on the Internet are being compromised. Although in large part technology and market forces currently drive which areas in cyberspace are publicly accessible and which are not, legal and normative debates exist as well. In one view, the Internet should remain a model of diverse and open access, decentralization, and public intercourse — a model possibly enhanced by the explicit designation of certain areas as "public forums." Another view holds that economic markets and emerging technology will properly enable sophisticated proprietary control, meaning that users will mainly gain access to cyberspace through private providers. An intermediate position suggests the possibility of zoning — designating some spaces on the Internet as publicly accessible, while allowing other spaces to remain privately controlled.

Divergent views about the meaning of community are central to the public-private debate. For example, those who see community as a medium for deliberation argue for government intervention to preserve the Internet as a space for public access and for debate about issues of public interest. Such public access advocates posit that for the

---

70 The Internet began as a government entity for defense research, and one key question is who will administer it in the future. See infra pp. 1657-58, 1660.


72 See, e.g., Jim Evans, Portals Open Doors to Convergence at CES, CNN ONLINE (Jan. 8, 1999) <http://www.cnn.com/TECH/computing/990108/portal.ces.idg/index.html> (on file with the Harvard Law School Library) (describing how "[the portals firmly believe that theirs is the content medium of the future, and it has only just begun"); see also Andrew L. Shapiro, New Voices in Cyberspace, THE NATION, June 8, 1998, at 36, 36-37 (discussing Microsoft Internet software, by which Microsoft can "simply steer [users] — subtly but strongly — where it wants them to go").

73 In constitutional law, a "designated public forum" is an area under government control provided for expressive purposes and thus subject to First Amendment protections. Many authors have advocated designating all or part of the Internet as a public forum. See, e.g., Steven G. Gey, Reopening the Public Forum — From Sidewalks to Cyberspace, 58 OHIO ST. L.J. 1535, 1618-34 (1998) (calling for a reworking of the public forum doctrine using Justice Kennedy’s functional approach and for extending coverage to the Internet); David J. Goldstone, A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech, 69 U. COLO. L. REV. 1, 9-10 (1998) (advocating treating dissimilar spaces on the Internet differently, and designating some as public forums); Robert Kline, Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet, 6 CORNELL J.L. & PUB. POL’Y 23, 57-58 (1996) (describing the Internet as a public forum — "an open meeting place for all members of the public where ideas are exchanged, issues are debated, and self expression flourishes").

74 See, e.g., Lessig, Reading, supra note 14, at 892-93 (describing the prevailing trend toward zoning).

75 See Lessig, Zones, supra note 11, at 1410-11 (discussing the potential for the Internet to prevent deliberation); Cass R. Sunstein, The First Amendment in Cyberspace, 104 YALE L.J. 1757, 1785-86 (1995) (same); Andrew L. Shapiro, Keeping On-Line Speech Free: Street Corners in Cy-
Internet "to produce attention to public issues, and exposure to diverse views, a market system may well be inadequate." However, for those who see community as a collection of people satisfying private preferences, government designation of public spaces may not only be undesirable, but may also threaten individual freedom.

Technology and market forces are also transforming how tailored an individual's Internet experience will be — a transformation that concerns the issue of "filtering." Some writers have noted that in real-space we must see and experience things not of our choosing, in contrast to the world of programming code, in which near-perfect filtering of content may soon be possible. A perfectly tailored Internet experience has been celebrated by both civil libertarians and entrepreneurs because it may allow a new wave of personal control over information and experience. However, some commentators urge a deeper assessment of the consequences of the ability to "select out of the world[s]" we do not prefer, arguing that complete consumer sovereignty may have negative consequences for democratic and communitarian aspirations.

---

78 See Pool, supra note 67, at 224–25, 250. Pool examines the regulatory response to communications technologies since the printing press and concludes that historically, when new communications technologies were introduced, "regulation seemed to be a technical necessity." Id. at 1. Consequently, "[a]s new technologies have acquired the functions of the press, they have not acquired the rights of the press." Id. at 250. For Pool, "[n]etworked computers will be the printing presses of the twenty-first century" and must therefore remain "free of public control." Id. at 224–25.
79 See infra pp. 1595–96.
80 See Lawrence Lessig, The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation, 5 COMM.LAW CONSPECTUS 181, 189–90 (1997) [hereinafter Lessig, Constitution]. Filtering technology is currently rough-edged and may exclude information that the consumer actually wants. However, some writers, such as Lessig, argue that even a "perfect" filter may still be dangerous because it allows people to tune out too much. See Lessig, Zones, supra note 11, at 1410.
82 See Chip Bayers, The Promise of One to One (A Love Story), WIRED, May 1998, at 130, 186 (discussing the hope for tailored commerce).
83 Lessig, Zones, supra note 11, at 1410.
84 See, e.g., Sunstein, supra note 75, at 1788.
The Internet's links to other technologies will also be critical in shaping future configurations of virtual communities. Web television and Internet videophones are already available, and as the Internet becomes more integrated into familiar technologies, it will begin to seem less separate from our daily lives. As "the mystery of cyberspace" fades, it will become less convincing to call cyberspace "there" and real-space "here." However, as the Internet becomes more a part of the life we already know, we may be inclined to turn away from the sorts of virtual communities made possible by the Internet. Such "extraordinary blindness to this potential" would be disappointing, but seems all too possible as life on the Internet increasingly mimics life in real-space.

Not only will the resolution of these three issues — public-private spaces, filtering, and integration with real-space — shape virtual community life, but their texture may in large part depend upon how programming code and Internet users are regulated by law. Although markets and programming code have so far been largely responsible for the texture of these issues, that does not mean that law cannot or should not play a role. To the contrary, law can regulate the Internet, thereby shaping its communities and expressing our collective values. Section C analyzes how law has already begun to mold virtual communities. Using a framework based upon the definition of community proposed earlier, section C examines three main areas in which law has played a role — defining the substance of virtual communities, determining the membership of these communities, and delineating the scope of these communities' powers of self-governance.

C. Law and Virtual Communities

1. Community as Common Project — Excluding Unwanted Speech. In defining "community," one key element is a sense of common purpose among the community's members. The amount of

86 See, e.g., Matt Richtel, Videophone Call-Ins On a Cable TV Channel, N.Y. TIMES, Oct. 22, 1998, at G3 (describing a cable television channel that urges viewers to call in with Internet-based videophones).
87 See Charles McGrath, The Internet's Arrested Development, N.Y. TIMES, Dec. 8, 1996, § 6, at 80 (looking forward to "when the Net becomes invisible and we can finally stop talking about it").
88 Shapiro, supra note 11, at 710.
89 Shapiro argues that this distinction is already erroneous. See id. at 718.
90 Lessig, Path, supra note 5, at 1747.
91 See Lessig, Constitution, supra note 80, at 191.
92 See Lessig, Reading, supra note 14, at 909 ("These are our democratic choices, and real choices they are."); Giordano, supra note 27, ¶¶ 74-75 (arguing that law defines significant aspects of communities); see also infra pp. 1695-97.
freedom people have to shape speech in virtual communities will be crucial to the types of "community" that emerge. As Philip Giordano notes, "limitations on speech are essential to the formation and individuality of virtual communities" because rules about group discussion "are tools that the players use to realize the kind of community with which they wish to identify." Regulation of the scope of speech in virtual communities implicates constitutional principles of freedom of speech and association. These principles have arisen in cases concerning sexually explicit speech, libelous speech, and "spam" (cyber "junkmail") on the Internet. These cases reveal the potential impact of cyber-speech regulation on the shape of online community life. Although these cases indicate that legal rules permitting suppression of unwanted speech may best enable "true" communities to form, the desirability of such communities must always be weighed against their potential to exclude disfavored views, which may or may not be welcome in alternate online forums.

(a) Sexually Explicit Speech. — The cases and legislation addressing sexually explicit speech on the Internet raise two issues that bear significantly on the status and shape of virtual communities: the role of local community standards in obscenity law and the role of user-controlled filters in controlling access to sexually explicit speech that is not otherwise barred as obscene.

Although the Supreme Court struck down Congress's attempt to regulate indecent speech on the Internet through the Communications Decency Act (CDA) as violative of the First Amendment, some Internet obscenity prosecutions have succeeded, despite their apparent conflict with the "local community standards" test applied in federal obscenity cases. The most significant of these prosecutions is United States v. Thomas, in which the Sixth Circuit rejected a "community

---

93 Giordano, supra note 27, ¶ 31.
94 Id. ¶ 69.
95 See id. ¶ 30.
98 The Court announced this standard in Miller v. California, 413 U.S. 15, 30-34 (1973), in response to the confusion generated by Roth v. United States, 354 U.S. 476 (1957), which many had interpreted as mandating that courts should determine a national obscenity standard. See Byassee, supra note 29, at 207-08.
99 74 F.3d 701 (6th Cir. 1996).
of cyberspace" standard\textsuperscript{100} and applied the "local community standards" test to the prosecution of two individuals who had made allegedly obscene material available through an out-of-state computer bulletin board.\textsuperscript{101}

At stake was an understanding of exactly where the effects of this obscenity were felt\textsuperscript{102} — in the local community, as suggested by the court's rationale, or merely in cyberspace, as the defendants argued.\textsuperscript{103} Although proponents of a separate cyberspace standard make a good case that the local community is barely affected by access to obscenity fully restricted to the home,\textsuperscript{104} the Thomas court's reluctance to accept a cyberspace community standard as an alternative is also understandable.\textsuperscript{105} As articulated to date, such a standard is not particularly workable or compelling, in large part because calling the millions of users of cyberspace a "community" contradicts common experience, even though discrete subsets of Internet users may have convincing community claims. Nevertheless, continued judicial reliance upon "local community standards" may itself lead to an intolerable result, as this test gives liability-wary bulletin board operators a strong incentive to tailor their offerings to the jurisdiction with the broadest definition of obscenity, potentially resulting in an alarming retreat to a national obscenity standard.\textsuperscript{106} As more cases arise, well-defined and identifiable virtual community standards, as opposed to Thomas's shallow invocation of the Internet community at large, should be advocated. Courts are more likely to take sophisticated, discrete Internet communities seriously if they distinguish the claims of such communities from

\textsuperscript{100} See id. at 711--12. Several commentators advocate a "community of cyberspace" standard. See Byassee, supra note 29, at 209--10; Rebecca Dawn Kaplan, Cyber-Smut: Regulating Obscenity on the Internet, 9 STAN. L. & POL'Y REV. 189, 194 (1998) (proposing the use of Internet surveys as evidence of community standards in cyberspace); Egan, supra note 35, at 147 (proposing that judges instruct juries to apply the obscenity standard of the cyberspace community). But see Timothy S.T. Bass, Comment, Obscenity in Cyberspace: Some Reasons for Retaining the Local Community Standard, 1996 U. CHI. LEGAL F. 471, 472 (arguing in favor of the current standard).

\textsuperscript{101} See Thomas, 74 F.3d at 705--06, 711--12 (noting that in this case the bulletin board operator had established methods to determine the location of individuals downloading materials, as well as actual knowledge of where the information was sent).

\textsuperscript{102} Cf. Branscomb, supra note 9, at 1653 (linking the question of which jurisdictional rules should apply to where the detrimental consequences of Internet use occurred).

\textsuperscript{103} See Byassee, supra note 29, at 209--10 ("[C]omputer users — or at least those individuals who use their computers to join the cyberspace community — no longer participate as members of the local community in significant ways in which VCR owners or adult bookstores still must participate.").

\textsuperscript{104} Cf. Stanley v. Georgia, 394 U.S. 557, 558--59 (1969) (holding that possession of obscene materials in one's home is protected by the First Amendment).

\textsuperscript{105} See Byassee, supra note 29, at 210 (noting that the precise formulation of such a broadly-framed standard may "prove to be . . . elusive").

the less defensible claims invoking the "cyberspace community" as a whole.107

Sexually explicit speech also implicates the issue of filtering,108 most visibly on publicly accessible machines. Two cases have arisen concerning the installation of filters on Internet terminals in public libraries,109 with the first case, Mainstream Loudoun v. Board of Trustees, decided by the Eastern District of Virginia, holding that such content-based blocking by libraries violates the First Amendment.110 Although the Eastern District noted that public libraries are free to avoid the blocking problem by not providing Internet access at all,111 this is hardly a plausible long-term strategy in light of the growing importance of Internet resources and the current federal "E-rate" program, which aims to connect American schools and libraries to the Internet.112 Yet courts must consider local concerns about maintaining community standards and bolstering community identity, particularly because the public viewing involved in the library cases is more clearly a matter of local concern than the private viewing at issue in the Thomas case. Ultimately, courts must strike a balance between the expression of local community norms and the provision of widespread public access to the Internet. However, these values need not be mutually exclusive, as Mainstream Loudoun seems to suggest.

(b) Libel. — The management of libelous speech on the Internet is another issue affecting virtual communities and their potential to con-

---

107 Additionally, to retain control over these prosecutions, local communities must continue to make convincing arguments about local harms, particularly because dormant commerce clause concerns have already led two jurisdictions to constrain state attempts to regulate Internet indecency. See ACLU v. Johnson, 4 F. Supp. 2d 1029, 1034 (D.N.M. 1998); American Libraries Ass'n v. Pataki, 966 F. Supp. 160, 183–84 (S.D.N.Y. 1997).

108 The Supreme Court highlighted the alternative of user-controlled filters in its rejection of the CDA's indecency provision. See Reno v. ACLU, 521 U.S. 844, 877 (1997). As discussed above, private filtering by Internet users has generated debate; some authors lament that the current imperfect filters will unduly limit the speech that reaches both children and adults. See, e.g., Jonathan Weinberg, Rating the Net, 19 HASTINGS COMM. & ENT. L.J. 453, 477–81 (1997).


110 See Mainstream Loudoun, 2 F. Supp. 2d at 795, 797.

111 See id. at 795–96.

control the content of speech within their borders.\textsuperscript{113} Most pertinent to virtual communities is the question whether to hold ISPs liable for the harmful or libelous speech of their members. The nature of ISP liability will shape the tenor and content of speech by members, as well as the means used by ISPs to regulate member speech. Mandating ISP liability (or liability for sysops, the moderators of ISP postings) threatens "to drive the amateur sysop to extinction and thereby to destroy what's left of online community."\textsuperscript{114} Yet permitting rampant libel on the Internet might itself destroy community.

The first cases addressing ISP liability generated conflicting results. The court in \textit{Cubby, Inc. v. CompuServe, Inc.}\textsuperscript{115} did not hold the ISP liable for a defamatory statement posted on its server,\textsuperscript{116} whereas the court in \textit{Stratton Oakmont, Inc. v. Prodigy Services}\textsuperscript{117} reached the opposite conclusion.\textsuperscript{118} In 1996, the CDA overruled \textit{Stratton Oakmont}; section 230 granted broad immunity from liability to ISPs that merely carried content generated by others.\textsuperscript{119} Section 230's power was confirmed by \textit{Zeran v. America Online, Inc.},\textsuperscript{120} in which the Fourth Circuit rejected a challenge to an ISP's immunity. The \textit{Zeran} court cited Congress's apparent rationale for granting such immunity: "[T]o maintain the robust nature of Internet communication"\textsuperscript{121} and to prevent ISPs from "severely restrict[ing] the number and type of messages posted" out of fear of liability.\textsuperscript{122} In 1998, \textit{Blumenthal v. Drudge}\textsuperscript{123} extended \textit{Zeran}, holding that, absent a showing of ISP control, even an ISP that pays a member for certain postings is immune from tort liability for the poster's libel.\textsuperscript{124}

Although the \textit{Zeran} and \textit{Blumenthal} courts exhibited an understanding of the potential chilling effects on speech in ISP communities that would occur if ISPs were held liable for members' postings, these rulings have left Internet libel victims without much recourse.\textsuperscript{125} These courts recognized that cyberspace is not really a separate realm

\textsuperscript{113} Elsewhere in this Development, Internet libel is considered in greater detail than in this Part's community-framed discussion. See infra pp. 1612-22.

\textsuperscript{114} Zittrain, supra note 7, at 496.


\textsuperscript{116} See id. at 144.


\textsuperscript{118} See id. at *77.


\textsuperscript{120} 129 F.3d 327 (4th Cir. 1997).

\textsuperscript{121} Id. at 330.

\textsuperscript{122} Id. at 331.


\textsuperscript{124} See id. at 47, 49-50.

— that conduct "there" has real-world effects "here" — and they were admittedly largely bound by Congress's express directive of immunity. Nevertheless, even if widespread ISP liability would result in ISPs "scrambling to hide behind contracts, waivers, monitoring of all content, and censorship of messages before posting," an online world increasingly tied to our real-space lives and increasingly populated by new users less respectful of online norms of civility may be too complex for a blanket rule of ISP immunity to make sense. As courts continue to decide how to treat ISPs, distinctions must be drawn among the variety of moderated groups on the Internet, and attention must be paid to the actual effects of regulation upon ISP policy and behavior.

(c) Spam. — "Spam" is the common term for unwanted e-mail and mainly refers to commercial solicitations. Spam has provoked outrage — users express frustration at its volume and its frequently fraudulent nature, while ISPs cite the time and money spent accommodating and removing spam from ISP servers. ISPs have begun aggressive anti-spam litigation, which has been notably successful. At stake is whether e-mail networks are considered public or private domains, and thus if a First Amendment right to send e-mail to these domains exists, or whether such unwanted e-mail is more properly considered a trespass. Courts and policymakers must carefully consider the implications of extending anti-spam efforts beyond the unso-

126 See Blumenthal, 992 F. Supp. at 49.
127 Branscomb, supra note 9, at 1671.
129 See Loundy, supra note 119, at 1082–1085 (suggesting possible analytical analogies to ISPs, including press, disseminators, common carriers, traditional mail routers, public forums, bulletin boards, and broadcasters).
130 See, e.g., Carroll, supra note 71, § 1.
132 See Daniel P. Dern, Postage Due on Junk E-mail — Spam Costs Internet Millions Every Month, INTERNETWEEK (May 4, 1998) <http://www.techweb.com/se/directlink.cgi?INW99805 04Soo3o> (on file with the Harvard Law School Library). Significantly, much of the spam that has been attacked to date has been fraudulent in nature. Some spammers promote fraudulent products, others forge return addresses to evade ISP filtering devices, and still others "hack" into an ISP's server to gather a list of e-mail addresses to target. See, e.g., Janet Kornblum, AOL Sues Junk Emailler, CNET News (Oct. 20, 1997) <http://www.news.com/News/Item/0,4,15436,00. html> (on file with the Harvard Law School Library) (describing suit in which AOL alleged that Prime Data committed computer crimes to gain access to the AOL network); Joe Nickell, Juno Jumps on Spammers, WIRED NEWS (Nov. 25, 1997) <http://www.wired.com/news/business/story/ 8788.html> (on file with the Harvard Law School Library) (mentioning forged return addresses).
licitated, often fraudulent commercial mailings that have been the subject of most spam cases to date.\(^\text{134}\)

In *Cyber Promotions, Inc. v. America Online, Inc.*\(^\text{135}\) a federal district court held that AOL's e-mail server was not a public forum for First Amendment purposes,\(^\text{136}\) deeming that "in the absence of State action, [AOL] has the right to prevent unsolicited e-mail solicitations from reaching its subscribers."\(^\text{137}\) Soon afterward, the fight against spam was further fueled by *CompuServe, Inc. v. Cyber Promotions, Inc.*,\(^\text{138}\) in which a federal district court sustained an ISP's claim of trespass against a spammer who continued to send bulk, unsolicited commercial e-mail to the ISP's members after "repeated demands to cease and desist."\(^\text{139}\) On the coattails of this litigation, lawmakers have begun to consider a variety of anti-spam measures, which range from advocating an outright ban on unsolicited commercial e-mail to mandating the labeling of such messages.\(^\text{140}\)

Although these efforts at suppressing spam are understandable — particularly considering the fraudulent practices of many commercial spammers — caution is in order, lest these early cases more generally dictate the First Amendment's treatment of e-mail. Cases concerning the blocking of *noncommercial* e-mail by arguably *public* access providers are now arising, and ISPs continue to argue that the principles established in the commercial spam cases should apply to noncommercial.

\(^{134}\) See Goldstone, *supra* note 73, at 63–65, 70 (discussing the implications of the initial, rather unsympathetic, commercial spam cases for future cases involving noncommercial speech).


\(^{136}\) See *id.* at 442.

\(^{137}\) *Id.* at 437. The court also held that AOL's server was not a public forum under the Pennsylvania constitution. See *id.* at 446.


\(^{139}\) *Id.* at 1017. The court found that the ISP server was not analogous to either a public forum or a public utility. See *id.* at 1025–26. The *CompuServe* court's reasoning has subsequently been followed by another federal district court. See America Online v. IMS, 24 F. Supp. 2d 548, 550–52 (E.D. Va. 1998) (holding a bulk commercial e-mailer liable for trespass to chattels and violation of the Lanham Trademark Act for falsifying return addresses).

cial e-mail as well.\textsuperscript{141} As applied in the cases to date, the trespass rationale — which focuses on the cost to the ISP of the extra demands placed on its server — would appear to apply to noncommercial e-mail.\textsuperscript{142} Yet the First Amendment interests raised by noncommercial speech significantly differ from those raised by commercial speech;\textsuperscript{143} courts must fully consider the merits of the public forum analysis before rejecting arguments that assert a First Amendment right for non-commercial speakers to send e-mail to proprietary servers.\textsuperscript{144} Particularly if there continue to be no “sidewalks” for protestors in front of ISP “property” in cyberspace, a rote application of trespass and First Amendment doctrines to noncommercial e-mail may cause an improper translation of our society’s principles of free speech and association to cyberspace.\textsuperscript{145} Abdicating cyberspace to proprietary interests — and rejecting the existence of public forums in cyberspace — may pose too great a threat to free speech, as courts continue to hold that private ISPs can “with complete impunity forbid or delete” certain topics from their servers.\textsuperscript{146}

2. Community as Bounded Membership — Excluding Unwanted Members. — In addition to control over content, another element critical to defining community involves membership boundaries — the ability of community members to include or exclude members, to distinguish members from nonmembers, and to keep private the actions of group members. The Internet’s current open architecture seems quite inclusive. However, if the “zoning” of cyberspace continues its drift toward proprietary organization, with control transferring to private interests that are free to exclude whomever they choose, the need for a more rigorous examination of private membership policies may arise. If online forums are competing for members, speakers excluded from one forum will readily find another;\textsuperscript{147} however, it is unclear that


\textsuperscript{144} Cf. Goldstone, \textit{supra} note 73, at 63–65, 70 (suggesting caution when denying First Amendment protections to commercial e-mailers).

\textsuperscript{145} See Shapiro, \textit{supra} note 75, at 14 (arguing for the need for public forums in cyberspace).


\textsuperscript{147} Cf. Vicki Been, \textit{“Exit” as a Constraint on Land Use Exactions: Rethinking the Unconstitutional Conditions Doctrine}, 91 COLUM. L. REV. 473, 506–07, 517 (1991) (discussing the theory of
such competition exists. As in the previous subsection, three doctrinal areas will be analyzed: ISP member termination, ISP discrimination in membership, and the legality of member anonymity. Throughout, one must keep in mind the differences between code and real-space architectures with respect to their abilities to exclude perfectly — once access is denied in cyberspace, there is not even a sidewalk upon which to stand.

(a) ISP Termination. — ISP member termination concerns "[w]hether virtual communities are justified in excluding undesirable." Some commentators have begun to advise ISPs to stave off government regulation by creating broad contractual "acceptable use" policies with members, in order to ensure ISP authority to terminate unruly members. Authors have noted the power of sysops to banish members and have also discussed how virtual communities such as LambdaMoo and the WELL have removed unruly members in the absence of formal policies. If courts continue to define these providers as private actors, as opposed to state-sponsored public forums or utilities, membership policies will presumably be upheld without a more probing due process review.

To date, only a few court cases have addressed member termination. The most prominent case, Cyber Promotions v. Apex, involved an ISP's summary termination of an alleged spammer. Because the contract between the ISP and the member provided for notice prior to termination, the court granted the member injunctive relief, reasoning that "the fact that Cyber is an unpopular citizen of the Internet does not mean that Cyber is not entitled to have its contracts enforced in a court of law." However, no court has yet found a default ISP duty competitive federalism and Tiebout's work suggesting that local geographic communities compete for residents).

148 Branscomb, supra note 9, at 1662.
150 See Johnson & Post, supra note 8, at 1388; Shapiro, supra note 75, at 11 (describing termination of Prodigy protesters).
151 See, e.g., Dibbell, supra note 48, at 300–08 (LambdaMoo); Hafner, supra note 46, at 121–22 (the WELL).
152 See Perritt, supra note 31, at 449–50 (discussing the use of trespass theory to enforce member termination contracts).
to provide notice or a hearing to terminated members.\textsuperscript{155} When such cases arise in the future, courts will need to decide how vigorously to enforce “acceptable use” policies, as well as what standards to apply to ISP termination in the absence of such policies.

If the public access model of the Internet grows, courts may begin to classify public providers as state actors and consequently hold them to a higher procedural standard for membership termination. However, if the private model continues to gain strength and if access to the Internet simultaneously becomes more vital, courts and lawmakers will need to consider whether Internet access rights to “private” services exist and whether state action should be imputed to these services.\textsuperscript{156}

In addition to the state action issue, when confronting cases of ISP termination, courts may need to consider users’ unique attachment to their ISP-granted usernames and addresses. These online “identities” are usually not portable or replicable across ISPs. Thus, when a member is terminated, she loses not only access to the Internet through a particular provider, but also the use of her developed identity.\textsuperscript{157} Whether users will be granted any sort of property interest in these “identities” remains to be determined.

(b) ISP Discrimination. — The ability of ISPs and other Internet groups to discriminate in choosing their members will also influence the shape and feel of virtual communities. To date, these considerations have only slightly emerged, and understandably so — without knowing what parts of the Internet are “public” or “private,” the applicability of state and federal antidiscrimination laws remains uncertain.\textsuperscript{158} However, the experiences of some women on the Internet have

\textsuperscript{155} See Kaplan, supra note 154.

\textsuperscript{156} See generally Goldstone, supra note 73 (explaining the feasibility of designating Internet providers as state actors or as public forums).

\textsuperscript{157} Cf. Lessig, Zones, supra note 11, at 1410 n.26 (noting that one must develop “a certain social capital to function well” in cyberspace and that “[e]xit, or banishment, is the forfeiting of that social capital”); Peter Wayner, Lost in Cyberspace: How to Hold on to Your Address, N.Y. TIMES, Jan. 28, 1999, at E9 (discussing the difficulty and cost of altering e-mail addresses when companies providing addresses change).

\textsuperscript{158} See Branscomb, supra note 9, at 1654–55. The public-private issue has arisen in the area of discrimination against the disabled. Many early online interactions had a liberating potential for disabled people, because early text-based formats lent themselves to translation for the blind and deaf. See Sreenath Sreenivasan, Blind Users Add Access on the Web, N.Y. TIMES, Dec. 2, 1996, at D7. However, as sites became more interactive and graphical, the disabled became less able to navigate them. See Michael Moeller, Disabling Web Barriers, PC WEEK ONLINE (May 12, 1998) <http://www.zdnet.com/pcweek/reviews/0s11/11twinai.html> (on file with the Harvard Law School Library); see generally Debra Nussbaum, Bringing the Visual World of the Web to the Blind, N.Y. TIMES, Mar. 26, 1998, at G8 (describing efforts to make the Internet “more accessible to blind, deaf and disabled users”). The Department of Justice has issued a statement that the Americans With Disabilities Act (ADA) will cover government entities on the Internet, as well as those serv-
already generated antidiscrimination concerns. As one author has explained, "[w]omen are quickly learning that many places on the Internet are . . . uncomfortable . . . for them."¹⁵⁹ This discomfort stems not simply from the presence of sexually explicit materials online, but rather extends to a wide array of interactive experiences.¹⁶⁰ Ironically, such discomfort arises despite the frequently cited potential of the Internet to equalize interaction between the sexes.¹⁶¹

One notable claim of discrimination involved a group of women who raised a Title IX challenge to single-sex online discussion groups established for a course at Santa Rosa College, a California public school.¹⁶² Single-sex forums had been present on the Internet prior to this case,¹⁶³ but the Santa Rosa situation was different: government "sponsorship" of the groups triggered Title IX. Female Santa Rosa students had initially asked for their own group,¹⁶⁴ but derogatory and sexist remarks about certain female students began to appear on a subsequently formed men's group. The Department of Education launched an inquiry that resulted in the disbanding of the groups, although no litigation ensued.¹⁶⁵ The Department's action "for the most part dismayed Netizens," not only because of the novel assertion of federal government authority to modify discussion groups, but also because the "decision left open the question of whether the government can use Title IX to intervene in other parts of cyberspace."¹⁶⁶ Whether protections of intimate association are transgressed by government action of this sort is a question that will need to be more fully considered in future cases — ones in which courts are required to reach the merits, as they were not in the Santa Rosa situation.¹⁶⁷ A recognition of the effects of discriminatory conduct — both in cyberspace and real-space — must not be lost, however, amidst the loudly voiced fears of government overregulation of online groups.¹⁶⁸

nces deemed to be "public accommodations." See Moeller, supra. How this will be enforced and which Internet entities will be labeled "public accommodations" remains to be determined.
¹⁵⁹ Cheris Kramarae, Technology Policy, Gender, and Cyberspace, 4 DUKE J. GENDER L. & POL. 149, 152 (1997).
¹⁶⁰ See id. at 151–54; Giordano, supra note 27, ¶ 37.
¹⁶¹ See, e.g., Whittle, supra note 18, at 272 (discussing the potential for gender equalization online); cf. Roger O. Crockett, Invisible — And Loving It, BUSINESS WEEK, Oct. 5, 1998, at 124 (describing how minority entrepreneurs find the Internet a haven from real-space discrimination).
¹⁶² See GODWIN, supra note 10, at 103; Branscomb, supra note 9, at 1654–55, 1673; Giordano, supra note 27, ¶¶ 41–45.
¹⁶³ See, e.g., Giordano, supra note 27, ¶ 39 (outlining the success of single-sex discussion groups on the WELL).
¹⁶⁴ See GODWIN, supra note 10, at 103.
¹⁶⁵ See Giordano, supra note 27, ¶ 43.
¹⁶⁶ Id., ¶ 44.
¹⁶⁷ See, e.g., Branscomb, supra note 9, at 1673.
¹⁶⁸ See GODWIN, supra note 10, at 114 (foreshadowing the effects of strong government regulation). Godwin's observation that "online forums, when left to speak in freedom, tend to become
(c) Anonymity. — A final issue of community membership control concerns the right of group members to remain anonymous both within and without a given online community. Authors exploring this topic express divergent beliefs about whether anonymity or pseudonymity in online groups — something much more possible in cyberspace than in real-space — engenders or inhibits community formation. The views lawmakers and judges adopt toward anonymity and pseudonymity will affect the legal treatment of these concepts, particularly concerning whether claims of a "right to anonymously communicate" implicate only speech interests or associational interests as well. No right to non-detection — which permits true anonymity — has ever existed in real-space; rather, real-space constraints have allowed a certain degree of non-detection. Whether this degree of possible anonymity will be transferred into cyberspace, or whether programming code will be encouraged to permit perfect detection of individuals' actions, remains an open question.

ACLU v. Miller is the most prominent judicial treatment of anonymous Internet communication. In Miller, a federal district court struck down, on First Amendment grounds, a Georgia law prohibiting all electronic communications that did not truthfully identify the sender. In reaching its decision, the court relied upon Supreme Court precedent recognizing a right to distribute pamphlets anonymously. However, although the Miller outcome is protective of anonymous speech, one commentator has warned that focusing on speech rights — as did the Miller court — may prevent courts from fully exploring the associational rights implicated by anonymous online communication. Future courts must be mindful of the potential of such communication to foster intimate relationships and associations.

more tolerant places over time" is questionable, although his concerns about state intervention are generally well-voiced. Id.

169 Compare Giordano, supra note 27, ¶¶ 11–13 (citing the beneficial effects of anonymity and identity creation on community formation), with Dyson, supra note 10, at 64–65 (arguing that real community requires identity over time, which is impossible with anonymity). See also Sherry Turkle, Life on the Screen: Identity in the Age of the Internet 177–269 (1995) (discussing the ramifications for personal identity of interacting via constructed online identities).

170 See Tien, supra note 30, at 122 (advocating a freedom of association rationale for anonymity protection).

171 See Lessig, Reading, supra note 14, at 876–82.


173 See id. at 1233.


175 See id. at 122, 176 ("Because social interaction on the Internet provides great potential for self-definition through association, protection of online anonymity is also justified by recognized rights of association .... Anonymity is linked to speech as association because the ability to bound groups fosters expression and intimacy ...."). Another anonymity issue certain to become more prominent involves "anonymous remailers" — Internet entities that agree to reroute com-
Many commentators have cautioned against targeting anonymity, but the diversity of suggested approaches indicates that a careful consideration of anonymity’s actual role in creating or hindering “community” — in a variety of contexts — is vital. The law’s treatment of anonymity will largely determine what types of interactions thrive on the Internet and whether the Net’s potential for permitting a heightened degree of anonymity is realized. Courts must decide whether cyberspace anonymity will resemble real-space anonymity; in so doing, courts must consider whether the degree of anonymity currently possible in real-space is merely happenstance, or whether it is a considered balance that endures because of its consonance with our legal and constitutional values.

3. Community as Sovereignty — Making and Enforcing Rules. — The degree of sovereignty and autonomy granted to various online groups constitutes the final legal dimension vital to the shape of present and potential online communities. This subsection considers the delegation to these communities of not only rule-making, but also rule-enforcing powers. Whether Internet communities, like other recognized autonomous groups in society, will be accorded a degree of autonomous governance depends upon how separately society allows these communities to exist and the degree to which real-space life is considered to be affected by Internet relationships.

Several authors have argued that Internet communities need to exercise powers of self-governance in order to thrive. Many Internet self-governance advocates point to the success to date of governance through shared group norms, as opposed to legalistic rules, but at the same time, they recognize that such norms may be jeopardized by the


177 Sovereignty is more fully discussed elsewhere in this Development. See infra Part VI.

178 See Perritt, supra note 31, at 451-63 (discussing possible analogies to other self-governing, autonomous communities).

179 See, e.g., DYSON, supra note 10, at 52-57 (arguing that communities must set their own rules to thrive); Byassee, supra note 29, at 219 (claiming that self-governance enhances the practical possibility of controlling online behavior); Johnson & Post, supra note 8, at 1391-93 (advocating the delegation of governance to online communities because of community members’ “interest in assuring the growth and health of their shared enterprise”); Perritt, supra note 31, at 419-25 (citing practical reasons, beyond fostering community, for delegating governance); Giordano, supra note 27, ¶ 8 (noting that self-governance cements virtual communities).
rapidly expanding membership of Internet communities.\textsuperscript{180} Although self-governance appears to work best when virtual communities already possess sophisticated group norms, permitting self-government initially may grant virtual communities the freedom and autonomy needed to establish these norms.\textsuperscript{181} As some have cautioned, however, "[h]ighly public cyberspaces may have powerful real world effects."\textsuperscript{182} Whether the law delegates powers of governance to online communities — through recognition of "Virtual Magistrate" decisions,\textsuperscript{183} for example — will not only depend upon how public and private spaces are legally designated on the Internet, but also upon how lawmakers and judges view the relationship between virtual life and real life. As with all of the legal questions addressed in this Part, how courts and legislatures answer these questions will necessarily be both descriptive and constitutive: not only will they describe the cyberspace we currently know, but they will also forge cyberspace's future shape, functions, and meanings.\textsuperscript{184}

\textbf{D. Conclusion}

We have only begun to encounter the communities that cyberspace makes possible and to apply our legal principles and rules to the unique situations created by Internet-enabled interactions. Legal rules will certainly affect which communities thrive and which fail, as well as how these communities will impact and become part of our real-space lives. As courts and legislatures begin to address these issues, an open mind and a spirit of experimentation will be crucial,\textsuperscript{185} lest we freeze the development of cyberspace and virtual communities. "What the Net will become is still, in large part, up to us"\textsuperscript{186} — lawyers, judges, scholars, policymakers, and citizens alike. Sensible and thoughtful regulation of cyberspace — and its wide variety of group interactions — cannot proceed without careful attention to the Internet's nexus with community life, both virtual and real.

\textsuperscript{180} See Henry H. Perritt, Jr., Dispute Resolution in Electronic Network Communities, 38 Vill. L. Rev. 349, 400 (1993) (arguing that the need for law is greater once groups enlarge and norms erode).

\textsuperscript{181} See \textit{id.}; see also infra pp. 1678–80.

\textsuperscript{182} Gosnell, \textit{supra} note 128, at 422.


\textsuperscript{184} See Lessig, \textit{Reading}, \textit{supra} note 14, at 904.

\textsuperscript{185} See Lessig, \textit{Path}, \textit{supra} note 5, at 1752–53.

\textsuperscript{186} Rheingold, \textit{supra} note 4, at 310.
III. THE LONG ARM OF CYBER-REACH

A. Introduction

One of the most striking aspects of cyberspace is that it "provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions." This characteristic sharply contrasts with traditional forms of mass communication, such as television, radio, newspapers, and magazines, which require significant start-up and operating costs and therefore tend to concentrate communications power in a limited number of hands. Anyone with access to the Internet, however, can communicate and interact with a vast and rapidly expanding cyberspace audience. As the Supreme Court opined in its recent landmark decision, *Reno v. ACLU*, the Internet enables any person with a phone line to "become a pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." Indeed, the Internet is "a unique and wholly new medium of worldwide human communication" that contains content "as diverse as human thought." The term "cyber-reach" can be used to describe cyberspace's ability to extend the reach of an individual's voice. Cyber-reach makes the Internet unique, accounts for much of its explosive growth and popularity, and perhaps holds the promise of a true and meaningful "free trade in ideas" that Justice Holmes imagined eighty years ago. Thus,

1. ACLU v. Reno, 929 F. Supp. 824, 843 (E.D. Pa. 1996). In its findings of fact, the district court grouped the most common methods of Internet communication into six categories: one-to-one messaging, such as e-mail sent to one particular address; one-to-many messaging, such as e-mail sent to a group of addresses, or a listserv; many-to-many messaging, such as a newsgroup or bulletin board; real-time communication, such as Internet chat that enables individuals to engage in immediate dialog; real-time remote computer utilization, which for example would allow a user to access a library's online card catalog; and remote information retrieval, which primarily entails browsing the World Wide Web for information. See *id.* at 834–36.

2. In the words of the Supreme Court, "[a]ny person or organization with a computer connected to the Internet can 'publish' information." *Reno v. ACLU*, 521 U.S. 844, 853 (1997). Indeed, Web publishing is so simple and accessible "that thousands of individual users and small community organizations are using the Web to publish their own personal 'home pages.'" *Reno*, 929 F. Supp. at 837. Many commercial Internet Service Providers (ISPs), such as America Online, allow subscribers to create webpages free of charge. See *id.* at 843. The ease of Web publishing, coupled with its ability to reach a large audience, has fueled the astounding growth of the World Wide Web, which is estimated to contain over 320 million webpages. See Steve Lawrence & C. Lee Giles, *Searching the World Wide Web*, 280 Sci. 98, 100 (1998). In addition, any Internet user can post a message to one of thousands of newsgroups and bulletin boards and thus reach a potentially worldwide audience. Moreover, many commercial ISPs provide subscribers access to internal bulletin boards and discussion areas.

4. *Id.* at 870.
5. *Id.* at 850 (quoting *Reno*, 929 F. Supp. at 844) (internal quotation marks omitted).
6. *Id.* at 870 (quoting *Reno*, 929 F. Supp. at 842) (internal quotation marks omitted).
7. In his famous dissent in *Abrams v. United States*, Justice Holmes addressed the ultimate constitutional importance of the free trade in ideas:
cyber-reach makes cyberspace "different" enough from physical space that we should consider how this difference may justify modifying existing legal rules that were designed without cyberspace in mind. This Part does not consider whether this "difference" is so great that cyberspace cannot be governed by traditional legal machinery. Rather, assuming that cyberspace can be regulated and shaped in traditional ways, this Part explores what difference cyber-reach should make to legal analysis.

Although cyber-reach potentially can impact the entire legal regime of cyberspace, this Part assesses its impact on two areas of the law that have an extensive doctrinal background in physical space and have also already begun to develop a body of cyberspace case law, which is certain to multiply in the near future. Section B considers the law of Internet defamation and argues that cyber-reach could have constitutional implications for state defamation law. Section C explores the conflict between Internet speakers and private censors, with reference to the state action doctrine, and argues that cyber-reach may challenge traditional notions of a private property owner's right to censor or silence speech. The common thread that runs through these analyses is that the potential benefits that cyber-reach holds for the public will only be fully realized if our legal regime recognizes the impact that cyber-reach has on traditional assumptions underlying current legal doctrine.

But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas, — that the best test of truth is the power of the thought to get itself accepted in the competition of the market; and that truth is the only ground upon which their wishes safely can be carried out.

Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting). Critics have consistently attacked this "marketplace" theory of the First Amendment as inconsistent with economic and practical reality, because most marketplaces of mass speech, such as television or newspapers, are dominated by a few wealthy voices. See, e.g., Owen M. Fiss, Free Speech and Social Structure, 71 IOWA L. REV. 1405, 1410-15 (1986). In contrast, in his supporting opinion in Reno, District Judge Dalzell observed that the Internet is the most participatory marketplace of mass speech that the world has yet seen. See Reno, 929 F. Supp. at 881 (opinion of Dalzell, J.); see also Eugene Volokh, Cheap Speech and What It Will Do, 104 YALE L.J. 1805, 1833-43 (1995) (predicting that the information superhighway will both democratize and diversify the information marketplace).

8 This is an interesting and important topic of debate in its own right. One leading cyber-space commentator has noted that the idea that cyberspace would be largely immune from regulation was once so accepted by Internet enthusiasts that it became a cliché. See James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 66 U. CIN. L. REV. 177, 178 (1997). Perhaps the leading skeptics of traditional legal regulation in cyberspace are Johnson and Post. See David R. Johnson & David Post, Law andBorders — The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367, 1367 (1996). For a sharp criticism of Johnson and Post, see Jack L. Goldsmith, Against Cyberanarchy, 65 U. CHI. L. REV. 1199, 1199–1201 (1998). See also infra Part VI (analyzing sovereignty and jurisdictional issues in cyberspace).
B. Defamation

i. Recent Developments. — Early Internet defamation litigation focused on whether Internet Service Providers (ISPs) that enable a third party to post a defamatory statement about the plaintiff on the Internet should be considered publishers or mere distributors of defamatory material. Under state law, publishers are generally held liable for defamatory statements, while distributors such as bookstores and libraries are liable only if they knew or had reason to know of the defamatory statements at issue. Cubby, Inc. v. CompuServe Inc. was the first major case to address this question, when a federal district court held that defendant CompuServe, at the time one of the nation’s largest ISPs, was a mere distributor of alleged defamatory statements posted to one of its electronic forums. The court noted that CompuServe had delegated responsibility for reviewing the contents of the forum to an independent contractor and had no opportunity to review the forum’s contents prior to publication online. The

---

9 Defamation is broadly defined as any communication that "tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him," RESTATEMENT (SECOND) OF TORTS § 559 (1977), but truth is a defense to liability, see id. § 581A. Defamation occurs in two forms: libel and slander. Libel generally covers written or printed defamation, while slander generally covers oral defamation, but the distinction is not always easy to make. See id. § 568 cmt. b. Although the modern practice has been to combine libel and slander under the common tort of defamation, the legal distinction between them remains important because state law traditionally requires slander plaintiffs, but not libel plaintiffs, to prove financial loss in order to recover damages. See id. §§ 569, 575. Most commentators agree that defamation on the Internet is best classified as libel, principally because an electronic message can always be printed. See, e.g., Terri A. Cutrera, Computer Networks, Libel and the First Amendment, 11 COMPUTER/L.J. 555, 562 (1992); David J. Loundy, E-Law 4: Computer Information Systems Law and System Operator Liability, 21 SEATTLE U. L. REV. 1075, 1106-07 (1998). However, no judicial opinion has squarely addressed whether online speech is libel or slander, and the answer may vary according to jurisdiction. See R. James George, Jr. & James A. Hemphill, Defamation Liability and the Internet, 507 PLU/PAT 691, 708 (1998). To the extent that the libel/slander distinction is based on the assumption that libel is more likely to reach a wide audience, cyber-reach also suggests that Internet defamation should be considered libel.

10 See, e.g., Cianci v. New Times Publ’g Co., 639 F.2d 54, 61 (2d Cir. 1980).

11 See, e.g., Auvil v. CBS "60 Minutes," 800 F. Supp. 928, 931-32 (E.D. Wash. 1992). Several commentators have also suggested that under certain circumstances, ISPs might be considered common carriers, which enjoy even greater protection from defamation liability than distributors. See, e.g., Cutrera, supra note 9, at 566-68; Loundy, supra note 9, at 1090-92; Edward A. Cavazos, Note, Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability For a New Technology, 12 REV. LITIG. 231, 237-40 (1992). However, because communications common carriers have historically held a monopoly in a given locality, common carrier status for ISPs, which have proliferated with abandon, is a rather poor fit. See I. Trotter Hardy, The Proper Legal Regime For "Cyberspace", 55 U. PITT. L. REV. 993, 1004 (1994). Furthermore, at least one federal court has rejected the common carrier analogy in the copyright context. See Religious Tech. Ctr. v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1369 n.12 (N.D. Ca. 1995).


13 See id. at 140-41.

14 See id. at 137.
opinion was especially solicitous of the role that ISPs were playing in the "information industry revolution" and did not want to establish a rule of liability that would impose an undue burden on the free flow of information.\footnote{Id. at 140.} Four years later, however, in \textit{Stratton Oakmont, Inc. v. Prodigy Services Co.},\footnote{1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).} a New York state trial court ruled that defendant Prodigy, another large ISP, was a publisher of alleged defamatory statements on one of its electronic bulletin boards.\footnote{See id. at *1.} The court took pains to explain that it was in "full agreement" with the \textit{Cubby} decision,\footnote{Id. at *5.} but held that Prodigy's own policies of regulating the content of its bulletin boards mandated the finding that it was a publisher.\footnote{See id.}

In 1996, Congress passed legislation that immunized ISPs from publisher liability for information provided by third parties, effectively overturning \textit{Stratton Oakmont}.\footnote{"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1) (Supp. II 1996). An "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." \textit{Id.} § 230(e)(3).} Notably, the legislation did not explicitly exempt ISPs from distributor liability, and its specific reference to "publisher or speaker" is evidence that Congress intended to leave distributor liability intact. Nevertheless, in the first case to test the legislation, \textit{Zeran v. America Online, Inc.},\footnote{129 F.3d 327 (4th Cir. 1997).} the Fourth Circuit held that § 230 immunized defendant America Online (AOL) from both publisher and distributor liability for alleged defamatory statements on its electronic bulletin boards.\footnote{See id. at 330-33.} The court based its holding on a questionable interpretation of the word "publisher," stating that "distributor" was merely a subset of the word "publisher."\footnote{Id. at 332.} This broad interpretation of § 230 was further extended last year in \textit{Blumenthal v. Drudge},\footnote{Id. at 330-33.} when a federal district court held that AOL was immunized from liability for alleged defamatory statements in the Drudge Report,\footnote{For a more detailed criticism of the \textit{Zeran} court's verbal gymnastics, see David R. Sheridan, \textit{Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet}, 61 ALB. L. REV. 147, 168-72 (1997).} an online gossip column that AOL provided to its subscribers.\footnote{992 F. Supp. 44 (D.D.C. 1998).} AOL was arguably responsible for the Drudge Report and was not simply a conduit for "another information content provider," which would bring it under the protective umbrella of § 230. AOL had con-
tracted with and paid Matt Drudge to provide his column, had aggressively promoted it, had the right to control its content. Nevertheless, although expressing sympathy for the plaintiffs’ position, the court concluded that its hands were tied by § 230 and that AOL was thus immune from suit. Other recent cases have solidified the trend toward granting ISPs broad immunity under § 230.

One consequence of this trend is that defamation plaintiffs likely will begin turning their attention toward recovering damages from those who originally post defamatory material, rather than from the ISPs that merely serve as intermediaries. Of course, it is not surprising that plaintiffs have thus far focused their attention on the comparatively deep-pocketed corporate ISPs, but with this route to recovery effectively barred by § 230, plaintiffs may have little choice but to pursue the original defamer or to take no legal action at all. Even the Zeran court was careful to state that its holding would not allow the original culpable party to escape liability. As a practical matter, some commentators have expressed doubt that limiting liability to the original defamer can provide an adequate remedy to defamation plaintiffs, primarily because cyberspace affords potential defendants a degree of anonymity. Although cyberspace anonymity can make a plaintiff’s task more difficult, it does not make it impossible in every case.

27 In fact, the money that Drudge received from AOL was his sole source of income. See id.
28 See id. at 51.
29 See id.
30 See id. at 52–53.
34 The universe of potential defamers generally can be divided into two groups: “calculated” defamers who might hide their identity behind an anonymous re-mailer or a fraudulent account, and others who choose to engage in controversial speech without taking any overt precautions to maintain anonymity. Although precise quantification is impossible, clearly many (perhaps even most) potential defamation defendants fall into the latter category. Furthermore, the use of

Once the inevitable lawsuits against the originators of defamatory material find their way to the courts, judicial attention must shift to the proper constitutional limits on state defamation liability. To date, this topic has taken a back seat to the challenge of determining the fate of ISPs, but it raises an interesting set of First Amendment questions. Before we can assess the potential impact of cyber-reach, we must have a clear understanding of these constitutional limits. Unfortunately, this task is complicated by both the confusing nature of defamation law\(^\text{35}\) and the Supreme Court’s often perplexing efforts at establishing minimum constitutional standards for state defamation law.\(^\text{36}\)

Prior to 1964, defamation was generally treated as a strict liability tort.\(^\text{37}\) The Supreme Court first endowed defamation with First Amendment protection in its landmark decision, New York Times Co. v. Sullivan,\(^\text{38}\) which established a minimum constitutional fault standard of “actual malice” in order for a public official to recover damages under state defamation law against critics of his official conduct.\(^\text{39}\) Subsequent cases have extended this holding to the broader category of public figures.\(^\text{40}\) A decade after New York Times, in Gertz v. Robert Welch, Inc.,\(^\text{41}\) the Court examined the limits the Constitution imposes on defamation suits brought by private figures and concluded that negligence, rather than actual malice, was the appropriate minimum fault standard.\(^\text{42}\) The Court justified this reduced fault standard by reasoning that the state has a greater interest in compensating private individuals for harms inflicted on them by defamatory falsehoods than it has in the case of public figures.\(^\text{43}\) Private individuals are more vulnerable to injury because they do not enjoy significant access to the anonymous re-mailers has come under attack. See supra Part II, note 175. Even in the case of a fraudulent account, it is conceivable that a determined plaintiff might pursue a negligence claim against an ISP that failed to follow responsible sign-up procedures.


\(^{36}\) See id. at 1522.


\(^{38}\) 376 U.S. 254 (1964).

\(^{39}\) Id. at 279–80. The Court defined “actual malice” as “knowledge that [the defamatory falsehood] was false or ... reckless disregard of whether it was false or not.” Id. at 280. The Court’s holding was designed to preserve “uninhibited, robust, and wide-open” debate on public issues. Id. at 270. Without such a high fault standard, “would-be critics of official conduct [might] be deterred from voicing their criticism” for fear of possible legal liability. Id. at 279.


\(^{41}\) 418 U.S. 323 (1974).

\(^{42}\) See id. at 347.

\(^{43}\) See id. at 343–46.
“channels of effective communication” and thus cannot realistically counter false statements in the media.\textsuperscript{44} In addition, private individuals are more deserving of recovery because they have not “voluntarily exposed themselves to increased risk of injury from defamatory falsehood[s]” by assuming an influential role in society.\textsuperscript{45} Therefore, after \textit{Gertz}, it appeared that the dichotomy between public and private figure plaintiffs would determine the level of constitutional protection for defamatory speech.

However, in \textit{Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.},\textsuperscript{46} the Court added another dichotomy to the analysis by distinguishing between private and public speech. The Court explained that reduced constitutional protection would attach to speech that did not involve a matter of public concern.\textsuperscript{47} Although the \textit{Dun & Bradstreet} holding is quite narrow,\textsuperscript{48} a majority of the Court strongly indicated that the states were free to impose strict liability in defamation actions brought by private figures involving speech of purely private concern.\textsuperscript{49} Moreover, the Court's analysis suggested that the constitutional fault rule established for public figures in \textit{New York Times} might not apply to purely private speech. Taken together, the Court's decisions establish that two dichotomies — public versus private figure plaintiff, and public versus private speech — shape constitutional protections for defamation.\textsuperscript{50} Unfortunately, the decisions do not offer much guidance on distinguishing between public and private figures, or between public and private speech. To determine public figure status, \textit{Gertz} ex-
plained that an individual may achieve such pervasive fame or notori-
ety that he becomes a public figure in all contexts, but that the most
common scenario occurs when an individual voluntarily injects him-
self or is drawn into a particular public controversy and thus becomes
a public figure for a limited range of issues. To distinguish public
from private speech, Dun & Bradstreet merely stated that courts
should examine the content, form, and context of the speech.

3. Impact of Cyber-reach on the Constitutional Standards. — The
emergence of cyberspace as a new locus for defamation does not mean
that Internet defamation is an entirely “new” legal issue that necessar-
ily requires radical changes in constitutional doctrine. However, ex-
isting standards of liability should not merely be cut from physical
space and pasted onto cyberspace, either. One leading commentator
has observed that “[s]ome cyberspace issues seem wholly unremark-
able,” and that in the case of Internet defamation, “the fact that a
communication [is] an electronic mail message on the Internet . . .
makes little difference to the legal outcome.” The interesting ques-
tions raised by Internet defamation “have nothing to do with the fact
that the message [is] sent by e-mail.” This type of reasoning —
although refreshing because it resists the urge to overstate the difference
between cyberspace and real-space — fails to appreciate how cyber-
reach changes the defamation landscape. Internet defamation is still
defamation, but its dynamics differ because of the speech-enabling
characteristics of cyberspace. Even assuming at the outset that Inter-
net defamation exhibits no difference in kind from real-space defama-
tion, it clearly manifests a difference in degree. And in general, differ-
ences of degree may have constitutional implications.

Given the wide availability of Internet communication and its par-
ticipatory nature, it seems inevitable that many future defamation
plaintiffs will be private individuals rather than public figures, at least
according to traditional modes of classification. Assuming that poten-
tially defamatory speech is of public concern, these plaintiffs would be
subject to the Gertz rule and would have to demonstrate negligence in
order to recover damages under state defamation law. However, sev-
eral commentators have proposed that under certain circumstances,
cyber-reach dictates that the appropriate level of fault in such cases should be elevated to actual malice. The thrust of their arguments is that the policy rationales underlying the Gertz distinction — that private individuals do not have the ability to counter defamatory speech and have not voluntarily exposed themselves to the risk of defamatory falsehoods — no longer apply in cyberspace, where everyone is on equal footing.

This is an intriguing argument at first glance, but upon closer inspection it has serious flaws. First, as other commentators have noted, the argument tends to overstate the capacity of a defamed person to reply in cyberspace. The only possible way to neutralize the first prong of the Gertz rationale would be through quick and easy access to the same forum in which the original defamation had occurred, not merely through access to the Internet in general. Second, the argument tends to discount the importance of the second prong of the Gertz rationale. The Gertz Court explained that voluntary exposure to public scrutiny was a more important justification for the distinction between public and private figure plaintiffs than the ability to reply to defamatory falsehoods. Clearly, even vigorous and frequent participation in online discussions does not grant an individual such pervasive fame or notoriety that he should be considered a public figure in all contexts, but whether such an individual might be considered a public figure in the narrow context of online discussion is a closer call.

56 See, e.g., Cutrera, supra note 9, at 570 (arguing for an actual malice standard when plaintiffs who are defamed on a computer bulletin board have access to the bulletin board); Bruce W. Sanford & Michael J. Lorenger, Teaching an Old Dog New Tricks: The First Amendment in an Online World, 28 CONN. L. REV. 1137, 1157–58 (1996) (suggesting an actual malice standard for plaintiffs who participate in online debate with respect to defamatory statements stemming from such debate). These commentators discuss the appropriate liability standard for ISPs rather than the original defamer, but the same reasoning applies regardless of the defendant's status. Cf. Dun & Bradstreet, 472 U.S. at 783–84 (Brennan, J., dissenting) (rejecting the media/nonmedia distinction for defamation defendants).

57 See, e.g., Robert M. O'Neil, The Drudge Case: A Look at Issues in Cyberspace Defamation, 73 WASH. L. REV. 623, 632–33 (1998); Hadley, supra note 33, at 493–98. Hadley convincingly argues that "the ability to reply in cyberspace, just like in the real world, depends not just on one's access to the Internet, but also on the ability and willingness of others to access one's reply." Id. at 492. For example, a private individual defamed by the Drudge Report could conceivably set up his own webpage to counter the defamatory falsehoods, but he would likely receive few visitors to the site. See id. at 494; see also O'Neil, supra, at 632. Similarly, a plaintiff defamed via e-mail would lack the ability to reply unless he could access the original e-mail distribution list, which might not be of much help, because of the ease with which the original recipients can forward the defamatory statements to others. See Hadley, supra note 33, at 494–95. Even in the narrow context of electronic bulletin boards, where presumably the same people who read a defamatory statement could also read a reply, the reply might not be effective unless it is immediate and the original defamatory statements are not copied from the bulletin board and disseminated elsewhere. See id. at 496; see also Zeran v. America Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997) (noting that defamatory statements on AOL bulletin boards were discovered and broadcast by a radio station).

Although the Court’s methodology is not entirely clear,\textsuperscript{59} the Court is obviously reluctant to define public figures broadly.\textsuperscript{60} The common thread through the Court’s reasoning is that public figure status requires a plaintiff to thrust himself to the forefront of a public controversy.\textsuperscript{61} Given the sheer number of speakers in cyberspace, all taking advantage of their cyber-reach, it is not easy for any individual to distinguish himself as being at the forefront of a public controversy. Certainly, the act of posting messages to one of literally thousands of online bulletin boards comes nowhere near the definition. Therefore, the suggestion that the \textit{Gertz} standard of negligence liability should be abandoned in favor of a more expansive application of the actual malice rule in cyberspace is tenuous at best.

An alternative way that cyber-reach might affect constitutional protections in cyberspace is by influencing the distinction between public and private speech. If a private figure plaintiff is defamed by speech of public concern, he has the burden of demonstrating negligence in accord with \textit{Gertz}, but if the speech is purely private, then state defamation law may impose strict liability on the speaker.\textsuperscript{62} Consequently, those accused of uttering defamatory falsehoods in cyberspace will no doubt frequently argue that their speech involves a matter of public, and not merely private, concern. The Court’s vague instruction that courts should distinguish between public and private speech based on the speech’s “content, form, and context”\textsuperscript{63} provides the sole direction for this determination. This open-ended inquiry offers little concrete guidance, can lead to inconsistent results, and has been criticized as an ultimately unworkable standard.\textsuperscript{64}

\textsuperscript{59} As one federal court has colorfully observed, trying to determine whether a particular plaintiff is a public or private figure “is much like trying to nail a jellyfish to the wall.” Rosanova v. Playboy Enters., Inc., 411 F. Supp. 440, 443 (S.D. Ga. 1976).

\textsuperscript{60} \textit{Gertz} was a prominent attorney who was defamed in connection with his role in representing the family of a young boy slain by a Chicago policeman, yet the Court considered him a private individual. \textit{See Gertz}, 418 U.S. at 325–26, 351–52. The Court has even rejected public figure status for a participant in a well-publicized divorce proceeding involving one of America’s wealthiest industrial families, who voluntarily held press conferences during the proceedings. \textit{See Time}, Inc. v. Firestone, 424 U.S. 448, 453–55 (1976).

\textsuperscript{61} \textit{Gertz} was a prominent attorney who was defamed in connection with his role in representing the family of a young boy slain by a Chicago policeman, yet the Court considered him a private individual. \textit{See Gertz}, 418 U.S. at 325–26, 351–52. The Court has even rejected public figure status for a participant in a well-publicized divorce proceeding involving one of America’s wealthiest industrial families, who voluntarily held press conferences during the proceedings. \textit{See Time}, Inc. v. Firestone, 424 U.S. 448, 453–55 (1976).

\textsuperscript{62} \textit{Gertz} was a prominent attorney who was defamed in connection with his role in representing the family of a young boy slain by a Chicago policeman, yet the Court considered him a private individual. \textit{See Gertz}, 418 U.S. at 325–26, 351–52. The Court has even rejected public figure status for a participant in a well-publicized divorce proceeding involving one of America’s wealthiest industrial families, who voluntarily held press conferences during the proceedings. \textit{See Time}, Inc. v. Firestone, 424 U.S. 448, 453–55 (1976).


Regardless of these doctrinal uncertainties, cyber-reach drastically affects both the form and context of speech. In Reno, the Court recognized that Internet speech can take the form of being broadcast to a potential audience of millions; furthermore, it can occur in the context of an online, interactive discussion with a nationwide, or even worldwide, assembly of speakers. Although simply having a bigger audience obviously does not change the content of fixed words, content is only one of three factors to consider. Moreover, in determining that the speech at issue was not of public concern, the Dun & Bradstreet plurality emphasized that the speech was restricted to a small audience. Although it seems sensible that simply taking private speech and posting it on the Internet does not magically transform it into speech of public concern, the communicative power of cyber-reach challenges conventional assumptions about public and private speech by bringing traditionally private speech into the realm of public debate, arguably justifying a more expansive definition of speech of public concern.

Cyber-reach argues most powerfully in favor of a change in the constitutional landscape in the case of a private individual suing over defamatory speech of no public concern. According to Dun & Bradstreet, the states appear free to impose liability without fault. Even if public concern is defined expansively in cyberspace, much Internet speech is so free-wheeling and diverse that it still is not likely to fit the definition. Yet as the Court observed in Reno, diversity is the very strength of Internet speech. Thus, the Court’s approach to cyberspace seems to counsel against a regime that could chill Internet speakers who might choose silence rather than risk strict liability for

---

66 See Dun & Bradstreet, 472 U.S. at 762 ("[S]ince the credit report was made available to only five subscribers, who, under the terms of the subscription agreement, could not disseminate it further, it cannot be said that the report involves any strong interest in the free flow of . . . information." (quoting Virginia Pharmacy Bd. v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 764 (1976)) (internal quotation marks omitted)).
67 See Hadley, supra note 33, at 500 (noting that "much of the speech on the Internet is miles from the public controversies" triggering heightened constitutional protection); cf. Snead v. Redland Aggregates Ltd., 998 F.2d 1325, 1330 (5th Cir. 1993) ("A speaker cannot turn his speech into a matter of public concern simply by issuing a press release.").
68 See supra p. 1616. Indeed, several lower courts have interpreted Dun & Bradstreet in this manner. See, e.g., Snead, 998 F.2d at 1333-34; Mutafis v. Erie Ins. Exch., 775 F.2d 593, 594-95 (4th Cir. 1985).
69 The Court’s opinion is littered with approving references to the diverse content of the Internet: cyberspace is a “vast democratic forum[],” Reno, 521 U.S. at 868, that is “open to all comers,” id. at 880, and serves as a “vast platform from which to address and hear from a worldwide audience of millions,” id. at 853. It has created a “new marketplace of ideas,” id. at 853, and a “dynamic, multifaceted category of communication,” id. at 870, with “content [that] is as diverse as human thought,” id. (quoting ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996)) (internal quotation marks omitted).
70 It is important to recognize exactly what this would mean: neither actual belief in the speech’s truth nor reasonable efforts to ascertain the truth would preclude liability.
their utterances — an effect that is multiplied by the uncertainty of determining what constitutes a matter of public concern. Prior to the explosive growth of cyberspace, several commentators argued against a return to strict liability for defamatory falsehoods based on the chilling effect that it could have on protected speech.\(^1\) Their reasoning has now attained even greater force in the context of cyberspace, in which literally everyone can act as a publisher of information.

Leaving aside the lessons of *Reno*, there is room within the Court's decision in *Dun & Bradstreet* to reject strict liability in cyberspace. The three-justice plurality in *Dun & Bradstreet* did not offer an extensive justification for not "constitutionaliz[ing] the entire common law of libel,"\(^2\) except to say that speech on matters of no public concern was not of central First Amendment importance.\(^3\) In his concurrence, Chief Justice Burger was similarly reticent.\(^4\) However, Justice White, the crucial fifth justice supporting the possibility of strict liability for defamatory speech of no public concern, went into more detail in his concurrence. He theorized that in balancing the First Amendment interest against the legitimate state interest in compensating defamation victims for reputational harm, the scales tip in favor of the state because imposing strict liability would not intimidate the powerful media into silence.\(^5\) Justice White's reasoning closely mirrored his dissent in *Gertz*, which painted a picture of Goliath publishers benefiting at the expense of David plaintiffs.\(^6\) Yet cyber-reach turns Justice White's reasoning into an anachronism: in the context of cyberspace, the Davids are not simply plaintiffs, but also the principal speakers. In other words, strict liability in cyberspace would not chiefly punish the publishing Goliaths of the world, but instead would punish or silence the Davids that Justice White solicitously defended. Consequently, it is highly doubtful that the states should possess the constitutional authority to impose strict liability for defamatory speech in cyberspace.

\(^1\) See, e.g., Smolla, *supra* note 35, at 1561; Taylor, *supra* note 64, at 181–83. Other commentators have also noted that strict liability for defamatory speech would contradict other Court decisions that seem to establish that strict liability has no place in First Amendment law. See, e.g., Loftus E. Becker, Jr., *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 CONN. L. REV. 203, 233–35 (1989).


\(^3\) See id. at 758–60.

\(^4\) See *id.* at 763–64 (Burger, C.J., concurring in the judgment).

\(^5\) Justice White acknowledged that the driving force behind both *New York Times* and *Gertz* was protecting the press from intimidating damages liability, but stated that he believed the Court had engaged in "severe overkill," *id.* at 771 (White, J., concurring in the judgment), chiefly because "other commercial enterprises in this country . . . must pay for the damage they cause as a cost of doing business," *id.* at 772. He doubted "the easy assumption that the common-law rules would muzzle the press," *id.*, which "as successful and powerful as it is," would not "be intimidated into withholding news that by decent journalistic standards it believes to be true," *id.* at 774.

on issues of no public concern. And as a policy matter, granting some form of constitutional protection to the entire common law of libel should encourage the sort of robust communication that has been the hallmark of Internet speech.

C. The Right to Speak in Cyberspace

1. Recent Developments. — Discussion of the right to speak in cyberspace has thus far been dominated by litigation pitting commercial advertisers against ISPs. Advertisers have argued that they have a First Amendment right to send unsolicited e-mail to ISP subscribers, and the ISPs have countered that they have a right to block this "spam"77 from reaching their members. The first case to address this issue was Cyber Promotions, Inc. v. America Online, Inc.,78 in which a federal district court held that because America Online was a purely private actor and not a state actor, it could use self-help remedies to block Cyber Promotions's e-mail advertisements without implicating the First Amendment.79 One year later, in CompuServe Inc. v. Cyber Promotions, Inc.,80 another federal district court took this rationale a step further, holding that Cyber Promotions's delivery of unwanted e-mail to CompuServe's subscribers was a trespass to chattels under state law,81 and that CompuServe was entitled to injunctive relief to protect its property, without implicating state action.82 Recently, other courts have seized upon CompuServe's trespass to chattels theory in order to grant ISPs relief against commercial spammers.83

A pending case that has attracted significant media interest84 and that could have an important long-term impact on the relationship between speech and property rights in cyberspace is Intel Corp. v. Hamidi.85 Intel brought suit against a disgruntled former employee, Ken Hamidi, alleging trespass to chattels and seeking to enjoin him from sending mass distributed e-mails to Intel employees at their

77 "Spam" is a pejorative term that describes unwanted e-mail, which usually consists of "junk" commercial solicitations. Spam is also discussed in detail above in Part II. See supra pp. 1601-03.
79 See id. at 456.
81 See id. at 1021-25.
82 See id. at 1026-28.
Hamidi, the spokesman for FACE Intel, a nonprofit organization of former and current Intel employees, sent the e-mails as part of his ongoing campaign to inform Intel employees about what he considers to be Intel’s abusive and discriminatory employment practices. In November 1998, California Superior Court Judge Lewis granted Intel a preliminary injunction. Intel filed a motion for summary judgment, arguing that Hamidi does not have a First Amendment right to express his views on Intel’s private e-mail system; Hamidi countered that whether he has committed a trespass is a triable issue of fact. On April 16, 1999, Judge Lewis issued a preliminary ruling denying Intel’s motion for summary judgment.

Although Intel raises some of the same concerns as commercial spamming cases such as CompuServe, it is a case of first impression because the challenged speech is not commercial spam, but instead is speech of public concern that lies at the heart of First Amendment protection. Before reaching the merits of Hamidi’s speech, however,

86 See id.
87 See Mendels, supra note 84. A copy of Hamidi’s most recent e-mail message to Intel employees is available on the FACE Intel website. See FACE Intel’s September 2, 98 E-mail Message and Intel’s Internal Reactions (visited Apr. 19, 1999) <http://www.faceintel.com/septemberemail.htm> (on file with the Harvard Law School Library).
92 Although commercial speech is not entirely removed from First Amendment protection, the Supreme Court has made it clear that such speech occupies a “subordinate position in the scale of First Amendment values.” Ohrallik v. Ohio State Bar Ass’n, 436 U.S. 447, 456 (1978).
93 See, e.g., Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–59 (1985) (“It is speech on matters of public concern that is at the heart of the First Amendment’s protection.” (quoting First Nat’l Bank of Boston v. Bellotti, 435 U.S. 765, 776 (1978)) (internal quotation marks omitted)); NAACP v. Claiborne Hardware Co., 458 U.S. 886, 913 (1982) (recognizing that expression on public issues “has always rested on the highest rung of the hierarchy of First Amendment values” (quoting Carey v. Brown, 447 U.S. 455, 467 (1980)) (internal quotation marks omitted)). Although we have already seen that there is no clear line between public and private speech, see supra pp. 1619–20, the form, content, and context of Hamidi’s speech suggest that it is speech of public concern. First, because it is in the form of mass distributed e-mails, Hamidi’s speech targets a large audience and is therefore unlike typical private speech. See, e.g., Dun & Bradstreet, 472 U.S. at 762; Connick v. Myers, 461 U.S. 138, 141 (1983); see also supra p. 1620. Second, the public has an interest in the content of Hamidi’s speech, because employment discrimination is clearly a topic of public concern. Furthermore, portions of Hamidi’s most recent e-mail message also address proposed federal legislation, see FACE Intel’s September 2, 98 E-mail Message and Intel’s Internal Reactions (visited Apr. 19, 1999) <http://www.faceintel.com/septem
the court must engage the threshold issue of state action. Because the First Amendment acts as a shield against state—not private—conduct, private actors are generally free to censor speech with impunity.\textsuperscript{94} Initially, Intel appears to be the quintessential private actor, and therefore its silencing of Hamidi's speech should not raise any constitutional concerns. However, the case is problematic because Intel is not merely exercising its own right to censor speech, but instead is asking the state, via a court-administered injunction enforcing state trespass law, to act as the censor. This is a crucial distinction\textsuperscript{95} that is worthy of further analysis because of its potential impact on the free speech landscape in cyberspace.

2. A Closer Look at the State Action Doctrine. — Determining when the conduct of private actors implicates state action is one of the great conundrums of constitutional law, and perhaps no area of constitutional law has been more heavily criticized for its incoherence.\textsuperscript{96} Although some commentators consider the state action doctrine so bankrupt that it should be completely abolished,\textsuperscript{97} this doctrine serves an important liberty interest by limiting the reach of legal and judicial power.\textsuperscript{98} As the Court has explained, whether the doctrine is good or

\textsuperscript{94} The Supreme Court has often highlighted this dichotomy between state and private action by stating that the Constitution erects no shield against merely private conduct, "however discriminatory or wrongful." Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974) (quoting Shelley v. Kraemer, 334 U.S. 3, 13 (1948)) (internal quotation marks omitted).

\textsuperscript{95} Unfortunately, this was a distinction that the court failed to make in CompuServe. In granting an injunction, the court simply stated, without elaboration, that "the mere judicial enforcement of neutral trespass laws by the private owner of property does not alone render it a state actor." CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1026 (S.D. Ohio 1997) (citing RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW § 16.3 (2d ed. 1992)). The Rotunda and Nowak treatise, however, fails to cite a single case in support of its assumption that judicial enforcement of trespass law does not trigger state action. In addition, the treatise's discussion of state action is conspicuously flawed because it fails to address any of the cases, such as New York Times, in which the Court has held that the mere judicial enforcement of trespass law does not trigger state action. In an influential article, Professor Charles Black described the doctrine as a "conceptual disaster area." Charles L. Black, Jr., The Supreme Court, 1966 Term—Foreword: "State Action," Equal Protection, and California's Proposition 14, 81 HARV. L. REV. 69, 95 (1967). Many subsequent commentators have expressed similar frustration. See, e.g., Erwin Chemerinsky, Rethinking State Action, 86 NW. U. L. REV. 503, 503–05 (1983); Henry J. Friendly, The Public-Private Penumbra—Fourteen Years Later, 130 U. PA. L. REV. 1289, 1290–91 (1982); Alan R. Madry, Private Accountability and the Fourteenth Amendment; State Action, Federalism and Congress, 59 MO. L. REV. 499, 500 (1994).

\textsuperscript{97} See, e.g., Chemerinsky, supra note 96, at 505–06.

bad policy, the state action requirement is a "fundamental fact of our political order."99 This section's purpose is not to outline a normative view of state action, but instead to demonstrate that within the Court's current state action doctrine, the judicial enforcement of trespass laws in order to censor Internet speech constitutes state action. Of course, this conclusion does not necessarily mean that every example of this type of state action amounts to an unconstitutional deprivation of First Amendment rights,100 but it does mean that the threshold question of whether state action exists must be answered in the affirmative.101

The starting point for the proposition that judicial enforcement of trespass law constitutes state action is Shelley v. Kraemer,102 in which the Court held that simply granting judicial enforcement of a private restrictive racial covenant implicated state action.103 Although the Court has not given Shelley an expansive reading104 and many com-

99 Id. at 937.
100 As Justice Rehnquist has succinctly stated, "[e]ven if there is 'state action,' the ultimate inquiry ... is, of course, whether that action constitutes a denial or deprivation by the State of rights that the [Constitution] protects." Flagg Bros. v. Brooks, 436 U.S. 149, 155 n.4 (1978).
101 How this threshold question should be answered in the absence of judicial action is beyond the scope of this section, but its resolution will greatly impact freedom of speech in cyberspace. Some cyberlaw commentators, principally Professor Lawrence Lessig, have theorized that the dominant force that will shape behavior in cyberspace will be technological code, rather than traditional legal regulation. See, e.g., Lawrence Lessig, The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation, 5 COMMLAW CONSPectUS 181, 183-84 (1997). The potentially disturbing corollary to this thesis is that constitutional rights in cyberspace could be left to the vagaries of private code. See id. at 191. For example, a property owner in cyberspace who is armed with powerful blocking software need not rely upon trespass law to exclude unwanted speech; therefore, no hypothetical First Amendment claim against the property owner — no matter how compelling — could ever surmount the state action hurdle. See Lawrence Lessig, The Zones of Cyberspace, 48 STAN. L. REV. 1403, 1408 (1996). Thus, lawmakers should focus their energies on influencing the development of cyberspace code in order to preserve our legal values in cyberspace. See, e.g., Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 JURIMETRICS J. 629, 669-70 (1998). Analogously, in our example, one could argue that the courts should not allow the vagaries of code to determine the existence or nonexistence of state action, but should rather look exclusively to the underlying speech and property rights at issue to determine the proper constitutional accommodation. Cf. Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY L.J. 869, 908 (1996); Cass R. Sunstein, The First Amendment in Cyberspace, 104 YALE L.J. 1757, 1804 (1995). Because it would require such a large deviation from current doctrine, however, it seems highly unlikely that in the foreseeable future a court would find state action in the case of a purely private actor using self-help remedies to block unwanted speech. See Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 456 (E.D. Pa. 1996). For a more detailed analysis of code-based regulation of cyberspace, see discussion below in Part IV.
102 334 U.S. 1 (1948).
103 See id. at 20. The Court explained that "[t]he short of the matter is that ... it has been the consistent ruling of this Court that the action of the States ... includes action of state courts and state judicial officials," id. at 18, and furthermore that "[w]e have no doubt that there has been state action in [this case] in the full and complete sense of the phrase," id. at 19.
104 Only once has the Court explicitly relied on the Shelley theory that a plaintiff's conduct constitutes state action merely because the state affords him judicial relief. See Barrows v. Jackson, 346 U.S. 249, 254 (1953). On other occasions, the Court could have relied on Shelley but chose other theories of state action instead. For example, in a series of sit-in cases in the 1960s,
mentators view the case with skepticism, the Court has never repudiated Shelley's essential holding and has in fact cited the case approvingly for the conclusion that invoking the authority of state courts qualifies as state action.

Nevertheless, given the uncertainty surrounding the decision, Shelley alone is arguably a slim reed on which to rest a finding of state action. But Internet speakers facing court-enforced censorship need not rely exclusively on Shelley. For instance, the Court has often held that mere judicial enforcement of substantive state law amounts to state action. \textit{New York Times Co. v. Sullivan} provides a clear example of this rule. In \textit{New York Times}, the only state action was judicial enforcement of state libel law in the context of a civil action between private parties, yet the Court quickly disposed of the state action issue by announcing that "[t]he test is not the form in which state power has been applied but, whatever the form, whether such the Court overturned trespassing convictions but did not cite Shelley. \textit{See}, e.g., Bell v. Maryland, 378 U.S. 216 (1964); Robinson v. Florida, 378 U.S. 153 (1964); Lombard v. Louisiana, 373 U.S. 267 (1963); Peterson v. City of Greenville, 373 U.S. 244 (1963).

Commentators' chief criticism of Shelley is that if any decision by a state court qualifies as state action, then ultimately all private actions must comply with the Constitution, rendering the Court's state action doctrine meaningless. This criticism is based on the theory that anyone whose rights are violated could file suit in state court, and the court's dismissal of the case would qualify as state action sustaining the infringement of the right. \textit{See}, e.g., Chemerinsky, \textit{supra} note 96, at 525-26. However, this is not a fair reading of Shelley's holding, but instead is an attempt to stretch it to its logical absurdity. Nothing in Shelley even remotely suggests that the denial of judicial relief constitutes state action. On the contrary, state action was based on "the active intervention of the state courts, supported by the full panoply of state power." Shelley, 334 U.S. at 19. The Court explained that Shelley was not a case in which "the States have merely abstained from action, leaving private individuals free to impose such discriminations as they see fit." \textit{Id.} Rather, the state had made available "the full coercive power of government." \textit{Id.} In other contexts, the Court has reiterated that the denial of judicial relief by itself is not state action. \textit{See}, \textit{e.g.}, \textit{Flagg Bros.}, 436 U.S. at 165.

\textit{See}, \textit{e.g.}, Palmer v. Sidoti, 466 U.S. 429, 432 n.1 (1984) (citing Shelley for the proposition that "[t]he actions of state courts and judicial officers in their official capacity have long been held to be state action governed by the [Constitution]"); \textit{Flagg Bros.}, 436 U.S. at 160 n.10 (citing Shelley in support of the proposition that invoking the authority of a state court to seize and impound property constitutes state action). In addition, relying solely upon Shelley, the Court has held that the mere application of sanctions by a state regulatory agency — which is arguably much less coercive than a court-ordered injunction — triggers state action. \textit{See} \textit{Moose Lodge No. 107 v. Irvis}, 407 U.S. 163, 178-79 (1972). More recently, however, the Court in \textit{dicta} cautioned against "reliance upon an extension" of Shelley, which it described as a "volatile case," but did not directly address the merits of the Shelley holding. \textit{Bray v. Alexandria Women's Health Clinic}, 506 U.S. 263, 282 n.14 (1993).

The most direct way for the Court to call Shelley into question would be to grant judicial relief in a case, while maintaining that there has been no state action. Yet in the fifty-one years since the Shelley decision, the Court apparently has never done this. The closest it came was in 1987, in \textit{San Francisco Arts & Athletics, Inc. v. USOC}, 483 U.S. 532 (1987), in which the Court granted the U.S. Olympic Committee an injunction yet held that the case did not involve government action. \textit{See id}. at 542-47. The Court expressly reserved judgment, however, on whether the injunction itself could be considered government action, because the parties had not properly raised the issue within their questions presented to the Court. \textit{See id}. at 547 n.30.

power has in fact been exercised.\footnote{108} The Court has reaffirmed this rule not only in subsequent libel actions,\footnote{109} but also in other contexts dealing with laws that do not bear directly on free speech.\footnote{110} Perhaps because of the Court's matter-of-fact treatment of state action in these cases, their import is often lost on lower courts addressing the state action doctrine,\footnote{111} but at least a handful of lower courts have grasped the significance of \textit{New York Times}.\footnote{112} Still, many courts insist that judicial enforcement of trespass law in the face of a First Amendment challenge does not constitute state action.\footnote{113} The only plausible rationale for this conclusion is that neutrally applied trespass laws are not specifically directed at speech, but instead affect speech only incidentally or indirectly.\footnote{114} In other words, trespass law is aimed at the activity of all trespassers, including — but

\begin{itemize}
  \item Id. at 265. For support, the \textit{New York Times} Court cited \textit{Ex Parte Virginia}, 100 U.S. 339 (1879), in which the Court stated that "[a] State acts by its legislative, its executive, or its judicial authorities," \textit{id.} at 347, and \textit{AFL v. Swing}, 312 U.S. 321 (1941), in which state action consisted of a judicial grant of a permanent injunction against labor picketing, \textit{see id.} at 325–26.
  \item \textit{See}, e.g., Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767, 777 (1989) (finding that the First Amendment is implicated by a private party's libel suit because of "the need to encourage debate on public issues").
  \item For example, the Court has found state action in the judicial enforcement of state common law tort liability for malicious interference with plaintiffs' businesses. \textit{See} NAACP v. Claiborne Hardware Co., 458 U.S. 886, 916 n.31 (1982) ("Although this is a civil lawsuit between private parties, the application of state rules of law by the Mississippi state courts in a manner alleged to restrict First Amendment freedoms constitutes 'state action' under the [Constitution]."). Perhaps the strongest statement of this rule occurs in \textit{Cohen v. Cowles Media Co.}, 501 U.S. 663 (1991), in which the Court held that enforcement of state promissory estoppel law constituted state action: "... These legal obligations would be enforced through the official power of the Minnesota courts. Under our cases, that is enough to constitute "state action" for the purposes of the [Constitution]."
\end{itemize}

\textit{Id.} at 668 (citations omitted).

111 Commentators are sometimes just as guilty as the courts in overlooking the significance of \textit{New York Times} to the state action question. For example, in the lengthy discussion of state action in their constitutional law treatise, Professors Rotunda and Nowak fail to mention \textit{New York Times}. \textit{See} ROTUNDA & NOWAK, supra note 95, \S\S 16.1–16.5.

112 \textit{See}, e.g., Paul v. Watchtower Bible & Tract Soc'y of N.Y., Inc., 819 F.2d 875, 880 (9th Cir. 1987) ("State laws whether statutory or common law, including tort rules, constitute state action."); Edwards v. Habib, 397 F.2d 687, 691 (D.C. Cir. 1968) ("There can now be no doubt that the application by the judiciary of the state's common law, even in a lawsuit between private parties, may constitute state action which must conform to the constitutional strictures which constrain the government."); see also Lloyd Corp. v. Whiffen, 750 F.2d 1157, 1159–60 (Or. Ct. App. 1988) (observing that if the state applies constitutional constraints to private libel suits, then state action must be present when a court enjoins a trespass), \textit{aff'd} on other grounds, 773 F.2d 1294 (Or. 1989).


not limited to — those who speak. The obvious doctrinal problem with this argument is that the Court has held that state action exists even when state courts enforce laws that do not specifically target speech. Perhaps just as importantly, cyber-reach challenges traditional assumptions about the purpose of purportedly neutral trespass laws. In real-space it is a safe assumption that trespass law is primarily used to prohibit others from physically interfering with one’s property, while silencing unwanted speech is only an incidental or indirect effect. It appears that the opposite is true in cyberspace: as the recent increase in litigation indicates, plaintiffs are aggressively using the theory of electronic trespass to block unwanted speech, while preventing a physical invasion unrelated to the content of the trespasser’s speech is at best an incidental purpose of the application of trespass law, if it is a purpose at all. Should the courts continue to prove receptive to the theory of electronic trespass, this trend of censoring unwanted speech will no doubt accelerate in the future, because almost every conceivable “trespass” in cyberspace carries a message.

Finally, no discussion of the enforcement of trespass law as state action would be complete without an analysis of the series of Supreme Court cases in which private property owners have sought to exclude unwelcome speakers. These cases establish that, even when the public is invited onto private property, the property owner normally can enforce state trespass laws to exclude speakers without violating the Constitution. Unfortunately, rather than illuminating the state action question, these cases tend to amplify the confusion. They are sometimes understood to mean that private property owners who enforce state trespass law are not state actors, but this is a decidedly curious interpretation in light of the conspicuous lack of state action.

115 See supra note 110.
116 See supra p. 1622.
118 Under current law, a shopping center owner’s private property rights trump a speaker’s First Amendment rights, see Hudgens, 424 U.S. at 520–21, but speakers may enjoy a right to speak on shopping center property if the relevant state constitution grants more expansive rights of expression than the federal Constitution, see Pruneyard, 447 U.S. at 88. In addition, speakers have a right to speak on the property of a private, company-owned town. See Marsh, 326 U.S. at 509–10.
discussion in the cases. A more sensible interpretation of the cases is that the Court presumes the threshold existence of state action, thereby allowing itself to engage in a substantive balancing of competing rights.

3. Impact of Cyber-reach on the Right to Speak in Cyberspace. — Returning to Intel v. Hamidi, the preceding discussion of state action demonstrates that an injunction against Hamidi would constitute state action that must conform to constitutional standards. Nevertheless, it is tempting to conclude that because the Court has held that the rights of private property owners generally trump the federal constitutional rights of speakers, Intel should prevail. Such a hasty conclusion, however, would be erroneous for two reasons. First, the case is being

120 Neither Marsh nor Logan Valley mentioned the words "state action" or "state actor" at all; judicial enforcement of state trespass law was presumed to be state action. See Logan Valley, 391 U.S. at 319 ("The State may not delegate the power, through the use of its trespass laws, wholly to exclude those members of the public wishing to exercise their First Amendment rights …."); Marsh, 326 U.S. at 508 ("A state statute, as the one here involved … clearly violates the … Constitution."). Lloyd Corp., however, did mention state action, stating that "it must be remembered that the First and Fourteenth Amendments safeguard the rights of free speech and assembly by limitations on state action, not on action by the owner of private property used nondiscriminatorily for private purposes only." Lloyd Corp., 407 U.S. at 567. But this is a puzzling reference for several reasons. First, the Court did not mention state action anywhere else in the opinion. If the case truly hinged on the existence or nonexistence of state action, presumably the words "state action" or "state actor" would have appeared in the holding. Second, in the opinion's conclusion, the Court acknowledged that the relevant inquiry was not whether state action exists, but rather how to balance the competing rights in the case properly. See id. at 570 ("There may be situations where accommodations between [property rights and First Amendment rights], and the drawing of lines to assure due protection of both, are not easy. But on the facts presented in this case, the answer is clear."). Third, in subsequent cases discussing the Lloyd Corp. holding, the Court has never mentioned the words "state action" or "state actor." See, e.g., Pruneyard, 447 U.S. at 80-81; Hudgens, 424 U.S. at 520-21. Finally, Hudgens alludes to state action only in passing, see Hudgens, 424 U.S. at 513, and Pruneyard does not mention state action at all.

121 Marsh makes the most explicit statement about this balancing of competing rights. See Marsh, 326 U.S. at 509 ("When we balance the Constitutional rights of owners of property against those of the people to enjoy freedom of press and religion, as we must here, we remain mindful of the fact that the latter occupy a preferred position."). But as the most recent case pitting private property owners against speakers, Pruneyard is the best guide to the Court's methodology and puts to rest any confusion that Lloyd Corp.'s reference to state action may have caused. If the shopping center owner in Lloyd Corp. were not a state actor, then there is no reason to believe that the shopping center owner in Pruneyard would be a state actor, either. Therefore, it would be impossible for the owner in Pruneyard to violate a speaker's right of free expression, regardless whether the speaker asserted federal or state constitutional rights. Yet the Court in Pruneyard clearly did not view Lloyd Corp. in this light. As already noted, "state action" or "state actor" was never mentioned in Pruneyard; instead, the Court engaged the merits of the competing rights in the case, upholding the California Supreme Court's decision that the state constitution gave the student leafleters in the case a right of free expression on the shopping center's private property. See Pruneyard, 447 U.S. at 88. Pruneyard thus confirms that in cases matching private property owners against speakers, state action is assumed, and the relevant inquiry is the proper balancing of competing rights. See Paul Brest, State Action and Liberal Theory: A Case Note on Flagg Brothers v. Brooks, 130 U. Pa. L. Rev. 1296, 1321 (1982) (noting that the state action in Pruneyard "was nothing more than a state property rule").

122 See supra p. 1628.
litigated in California, where Hamidi enjoys more expansive rights of free expression under the California state constitution than he does under the federal Constitution. Indeed, one lesson of *Pruneyard* is that in California, a speaker generally occupies a preferred position over a private property owner when such property has been opened to the public.\(^\text{123}\)

More fundamentally, cyber-reach suggests that Hamidi also has a federal First Amendment right to disseminate his electronic messages to Intel employees.\(^\text{124}\) Cyber-reach enables Hamidi to send his messages from one forum, the Internet, to another forum, Intel's proprietary computer system. The fact that this case involves two different forums — rather than just one — distinguishes it from real-space cases pitting private property owners against speakers. For instance, in the series of cases from *Marsh v. Alabama* to *Pruneyard Shopping Center v. Robins*, the Court balanced the litigants' competing speech and property rights while considering the nature of the single forum in which the dispute occurred.\(^\text{125}\) Here, the *Intel* court must balance Hamidi's speech rights and Intel's property rights while considering the effect the decision will have on both the Internet and on Intel's computer system. Consequently, the unthinking application of real-space analogies can be misleading if it fails to account for the novel characteristics of cyber-reach.\(^\text{126}\)

\(^{123}\) See *Pruneyard*, 447 U.S. at 88.

\(^{124}\) From Hamidi's perspective, it is fortuitous that he can take advantage of the increased speech protections of the California state constitution. However, because the dynamics of cyber-reach are not limited to cases arising in California courts, the remainder of the analysis will focus on Hamidi's federal constitutional rights.

\(^{125}\) See supra pp. 1628-29 and note 121.

\(^{126}\) For example, in its Motion for Summary Judgment, Intel cites a number of cases involving a single forum for the proposition that "California law does not extend [speech] rights . . . to a forum where the property owner does not open up his property to the public in general." Plaintiff's Motion for Summary Judgment, Intel Corp. v. Hamidi, No. 98AS05067 (Cal. Super. Ct. Dec. 9, 1998) (motion available at <http://www.faceintel.com/summaryjudgment.htm>) (on file with the Harvard Law School Library). Not only are these cases of limited value because they involve only one forum, but also Intel's assertion that it has not opened up its computer system to the "public in general" strains credulity. By voluntarily connecting its computer system to the Internet, Intel obviously wants to take advantage of the tremendous communicative power of cyberspace. Because of this decision, Intel is now at least a passive participant in the "new marketplace of ideas," *Reno v. ACLU*, 521 U.S. 844, 885 (1997), and cannot expect to control every message that crosses the border from cyberspace into its employees' e-mail inboxes. Not only is this technologically impossible (as the *Intel* litigation aptly demonstrates), but Intel's own policies permit "reasonable personal use" of the Internet, which presumably includes receiving unsolicited e-mails. See Plaintiff's Motion for Summary Judgment, Intel Corp. v. Hamidi, No. 98AS05067 (Cal. Super. Ct. Dec. 9, 1998) (motion available at <http://www.faceintel.com/summaryjudgment.htm>) (on file with the Harvard Law School Library).
The best real-space analogy\textsuperscript{127} for the Intel case is that Hamidi is standing on a speaker’s platform in the middle of a public park,\textsuperscript{128} pointing his megaphone in the direction of Intel’s private property, and Intel wants the court to force Hamidi to take his megaphone and his message elsewhere. This analogy illuminates several key aspects of the case. First, Hamidi’s speech is not originating on Intel’s property, but instead arrives there as its final destination. Second, an injunction against Hamidi’s speech not only would remove his message from Intel’s property, but also would restrict his right to broadcast his message from his speaker’s platform. Third, Intel is not trying to silence Hamidi altogether, but rather wants him to disseminate his message in a different manner.\textsuperscript{129} This analogy is also helpful in determining the...

\textsuperscript{127} When a case of first impression reaches the courts, much of the battle often focuses around which new analogy the court should adopt to resolve the case. For example, in Cyber Promotions, Inc. v. America Online, Inc., AOL convinced the court that AOL’s private computer system was: akin to a private resort swimming pool that has a “channel” leading to the “ocean” that is the Internet. AOL has permitted persons swimming in its “pool” to transmit messages to and receive messages from the Internet ocean. AOL has, however, taken steps to prevent sharks such as Cyber from entering AOL’s pool from the Internet ocean. At no time has AOL contended that it controls communications over the Internet ocean, but only that it controls its own private channel.

\textsuperscript{128} Several commentators have suggested that cyberspace should be considered a public forum, such as a public street, park, or sidewalk, where the Court under its public forum doctrine applies strict scrutiny to content-based restrictions on expressive activity. See, e.g., Steven G. Gey, Reopening the Public Forum — From Sidewalks to Cyberspace, 58 OHIO ST. L.J. 1535, 1610–19 (1998); Robert Kline, Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet, 6 CORNELL J.L. & PUB. POL’Y 23, 56–60 (1996). The problem with this argument is that cyberspace is not publicly owned in any traditional sense, thus it cannot fit squarely into the Court’s public forum jurisprudence. This is only a minor objection, however, because the Court’s opinion in Reno v. ACLU strongly suggests that speech in cyberspace is entitled to the same level of protection as public forum speech. See supra p. 1610; supra note 69; see also Gey, supra, at 1611 (noting that the Reno majority treated the Internet as a public forum without making the designation explicit).

\textsuperscript{129} Intel might try to analogize its requested injunction to a constitutionally permissible time, place, or manner regulation of protected speech. However, time, place, or manner restrictions only pass constitutional muster if they are content-neutral. See, e.g., Ward v. Rock Against Ra-
ultimate question in the case, which is how to balance the litigants' competing interests properly.

On one side of the scale, Hamidi appears to possess a strong First Amendment interest in being permitted to send his messages without court interference. As already noted, his e-mails fall within the definition of speech of public concern, which the First Amendment is designed to protect. In addition, because his messages originate in cyberspace, Intel's content-based restriction on Hamidi's speech is subject to strict scrutiny in accordance with Reno. Furthermore, Hamidi's messages are tailored for Intel employees; cyber-reach enables him to disseminate the messages via e-mail in the most effective and efficient method possible. In fact, Hamidi is simply playing the role of a cyberspace "town crier" or "pamphleteer" that the Court exalted in Reno. Intel might respond that alternative avenues of communication exist through which Hamidi could broadcast his message, such as the FACE Intel webpage. However, the Court specifically rejected that argument in Reno, observing that content-based speech restrictions in cyberspace cannot be justified by the suggestion that the speaker can disseminate his message elsewhere on the Internet.

On the other side of the scale, Intel's legal interest in protecting its private property by censoring Hamidi's speech is not particularly compelling. As a general matter, there is arguably less justification for enforcing purportedly neutral trespass laws against speakers in cyberspace than in real-space, because the primary purpose of enforcing trespass law in cyberspace seems to be the censorship of unwanted speech. This argument is buttressed by the fact that Hamidi has used Intel's employee e-mail inboxes for their express purpose —

cism, 491 U.S. 781, 791 (1989); Heffron v. Int'l Soc'y for Krishna Consciousness, 452 U.S. 640, 647-48 (1981). Clearly, Intel's attempt to censor Hamidi's speech must be classified as a content-based speech restriction. As noted previously, Intel permits its employees to receive unsolicited e-mail, see supra note 126, and Hamidi's messages have not burdened Intel's computer system, see supra note 127. Therefore, Intel cannot argue that censoring Hamidi would be consistent with any content-neutral company policy.

130 See supra p. 1623 and note 93.
131 See supra note 128.
133 This was the primary argument that led the Court to rule in favor of the private property owner in Lloyd Corp. See Lloyd Corp. v. Tanner, 407 U.S. 551, 567 (1972) ("It would be an unwarranted infringement of property rights to require [the property owner] to yield to the exercise of First Amendment rights under circumstances where adequate alternative avenues of communication exist.").
134 See Reno, 521 U.S. at 880 ("[O]ne is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place." (quoting Schneider v. New Jersey, 308 U.S. 147, 163 (1939)) (internal quotation marks omitted)).
135 See supra p. 1628.
communication. Moreover, Hamidi's messages have not disrupted the proper functioning of Intel's computer system. Finally, Pruneyard forecloses the possibility that Intel could raise a valid Fifth Amendment takings challenge or its own First Amendment challenge to Hamidi's speech.

Ultimately, Intel wants to enjoy all the benefits of Internet communication without having to shoulder any of its burdens. Benefits rarely come without costs — and if Intel believes that the benefits derived from connecting its computer system to the Internet are outweighed by the costs of tolerating free expression, then Intel should employ its own self-help measures to counter unwanted speech rather than ask the state to countenance censorship. Indeed, it is ironic that a technological giant such as Intel, which has helped to usher in and has greatly benefited from the cyberspace age, now expects the state to protect it from a creature of its own making. The irony is only heightened by Intel's adversary, a poorly financed army of one. As a policy matter, Intel might argue that a decision in favor of Hamidi would set a bad precedent because it would open the floodgates for others, including commercial spammers, to inundate private computer systems with

136 As already discussed, Intel cannot plausibly claim that its employee e-mail inboxes are not open to the public, see supra note 126, nor can it claim that the purpose of its e-mail system is not communication. Intel might try to narrow the definition of "communication" by arguing that the only purpose of its e-mail system is business-related communication, not communication in general. However, this is belied by Intel's own company policies, which permit reasonable personal use of the Internet. See id. Furthermore, although Intel obviously disapproves of the content of Hamidi's messages, the messages would still fall under the more narrow definition of "communication," because they are specifically directed at Intel's business practices.

137 See supra note 127. Intel claims, however, that Hamidi's messages are disruptive because they harm employee productivity — specifically, employees spend time "contact[ing] computer systems support personnel questioning why they are receiving unrequested e-mails and asking to be blocked from further e-mails." Plaintiff's Motion for Summary Judgment, Intel Corp. v. Hamidi, No. 98AS05067 (Cal. Super. Ct. Dec. 9, 1998) (motion available at <http://www.faceintel.com/summaryjudgment.htm>) (on file with the Harvard Law School Library). This is not a particularly troubling claim, however, because Hamidi's messages allow the recipient to remove himself from future e-mailings by requesting that his name be deleted from the distribution list. See FACE Intel's September 2, 98 E-mail Message and Intel's Internal Reactions (visited Apr. 19, 1999) <http://www.faceintel.com/septemberemail.htm> (on file with the Harvard Law School Library). Hamidi claims that he has received only 450 requests for deletion and that he has deleted those recipients. See Defendant's Memorandum of Points and Authorities in Opposition to Motion for Preliminary Injunction, Intel Corp. v. Hamidi, No. 98AS05067 (Cal. Super. Ct. Nov. 12, 1998) (memorandum available at <http://www.faceintel.com/opposeinjunction.htm>) (on file with the Harvard Law School Library). More fundamentally, requiring an employee simply to erase the unwanted message — which takes only a single mouse click or keystroke — is an acceptable burden to bear in the interests of free speech. Cf. Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 72 (1983) (striking down prohibition on unsolicited mailing of contraceptive advertisements, based on the logic that "the short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned" (quoting Lamont v. Commissioner of Motor Vehicles, 266 F. Supp. 880, 883 (S.D.N.Y. 1967)) (internal quotation marks omitted)).

mass e-mailings. This argument, however, is meritless. The logic of a decision in favor of Hamidi would not apply to commercial spammers, but instead would be based on a careful balancing of the competing rights in Hamidi's case. Furthermore, by no means would a ruling against Intel "imply that those who wish to disseminate ideas have free rein"; rather, Hamidi's expressive activity would continue to be bound by the requirement that it not unduly interfere with the business functions of Intel's computer system.

D. Conclusion

As courts encounter the inevitable flood of future Internet litigation, they should carefully scrutinize the underlying foundations of existing legal doctrine and ask whether cyber-reach uproots, or at least weakens, those foundations. Sometimes the answer will be yes, as in the analysis of the constitutional limits of state defamation liability and the right to speak in cyberspace. At other times, the answer will be no. However, the courts should not engage this question in a cursory fashion that either assumes that real-space doctrine should be grafted wholesale onto cyberspace, or just as erroneously, assumes that cyberspace should not be bound by existing rules. The only way that judicial decisions will have lasting legitimacy is if courts approach this threshold question with an open and inquisitive mind. Furthermore, by recognizing the impact that cyber-reach can have on traditional assumptions underlying legal doctrine, courts will help ensure that the "new marketplace of ideas" achieves its full potential as we enter the new millennium.

IV. INTERNET REGULATION THROUGH ARCHITECTURAL MODIFICATION: THE PROPERTY RULE STRUCTURE OF CODE SOLUTIONS

A. Introduction

"Cyberspace" refers to the interconnection of many computers worldwide. Computers are nothing more than machines that read and carry out instructions or "code." Some kinds of code direct computers' most basic functions; some enable the processing of words, music, or visual images; and some facilitate the interconnection of com-

---


140 Cf. Pruneyard, 447 U.S. at 83 (noting that "[t]here is nothing to suggest that preventing [the shopping center owner] from prohibiting [leafletting] will unreasonably impair the value or use of [the] property as a shopping center").


1 The term was invented by William Gibson. See WILLIAM GIBSON, NEUROMANCER 4 (1984).

2 I use the term "code" generally to refer to the instructions executed by computers. Code may be represented in various forms, including holes in a punch-card, wiring on a chip, or a sequence of ones and zeros.
puters. Thus, in many respects, cyberspace is reducible to code — it is the interconnection, through code, of machines that read and manipulate code, thereby enabling the exchange of code. Code defines the architecture of cyberspace.\(^3\)

Real-space is often contrasted with cyberspace.\(^4\) The fundamental difference between the two is that the architecture of cyberspace is open and malleable.\(^5\) Anyone who understands how to read and write code is capable of rewriting the instructions that define the possible. This has led to the swift and steady evolution of cyberspace.\(^6\) Compared to the highly malleable architecture of cyberspace, the architecture of real-space is closed.

There are problems in cyberspace: children access harmful material; organizations collect personal information without the knowledge of the individuals from whom it is taken; and people use intellectual property in unauthorized ways.\(^7\) As in real-space, legal rules may be enacted to address these problems. However, legal solutions to cyberspace problems may not be able to adapt to the rapid and continuous transformations of the medium. The fundamental malleability of cyberspace thus suggests a different solution, one in which the architectural code is altered to eliminate the problems of cyberspace. This is the "code solution."

Code solutions, like legal rules, allocate and enforce entitlements. According to the model developed by Calabresi and Melamed, entitlements may be allocated and enforced through either property or liability rules.\(^8\) Under a property rule regime, parties are able to contract around the initial entitlement allocation and to set protections at their preferred levels.\(^9\) Under a liability rule regime, parties may not trans-

---

\(^3\) Architecture may be loosely understood as the overarching limits or boundaries of a space — the blueprint of what is possible. See Lawrence Lessig, The New Chicago School, 27 J. LEGAL STUD. 663, 663 (1998) (hereinafter Lessig, Chicago) ("I mean by 'architecture' the world as I find it, understanding that as I find it, much of this world has been made.").

\(^4\) See generally I. Trotter Hardy, The Proper Legal Regime for "Cyberspace", 55 U. PIT. L. REV. 993, 994-95 (1994) (assessing the extent to which cyberspace raises legal problems different from those of real-space). But see Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. CHI. LEGAL F. 207, 207-08 (arguing that there is no more a "law of cyberspace" than there is a "law of the horse" and that real-space legal principles can be applied to cyberspace).

\(^5\) See Reno v. ACLU, 521 U.S. 844, 890 (1997) (O'Connor, J., concurring) ("Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace . . . ."); Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY L.J. 869, 897 (1996) ("With respect to the architecture of cyberspace, and the worlds it allows, we are God.").

\(^6\) For a discussion of the evolution of cyberspace, see supra pp. 1578-79.

\(^7\) Obviously, this is not an exhaustive list, but these particular concerns will be addressed below in sections B-D.

\(^8\) See Guido Calabresi & A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 HARV. L. REV. 1089, 1089-1115 (1972) (describing the rules that may be used to allocate and enforce the state's entitlement determination).

\(^9\) Calabresi and Melamed describe property rules as follows: An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in
fer entitlements without paying state-mandated penalties. Generally, liability rules are more efficient when transaction costs prohibit the parties from allocating entitlements among themselves, and property rules are more efficient when transaction costs are low. Therefore, although code solutions may be adapted to either regime, a property rule regime is preferable in cyberspace because transaction costs are extremely low, enabling individuals to reach bargains that reflect their actual preference levels.

This Part will apply Calabresi and Melamed's property rule paradigm to architectural code. It will concentrate on the ways in which code solutions may be used to solve the problems of cyberspace. Three specific areas will be examined: minors' access to harmful material, the collection of personal information, and the unauthorized use of intellectual property. In each instance, I will first describe the current entitlement. Second, I will examine the ways in which code can address the problem and consider whether it should be used to enforce the current entitlement or to arrive at a different entitlement. Third, I will

which the value of the entitlement is agreed upon by the seller. It is the form of entitlement which gives rise to the least amount of state intervention: once the original entitlement is decided upon, the state does not try to decide its value. It lets each of the parties say how much the entitlement is worth to him, and gives the seller a veto if the buyer does not offer enough.

Id. at 1092 (citation omitted).

The penalty may be in the form of a fine or a court judgment. Calabresi and Melamed describe liability rules as follows:

Whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule. . . . [L]iability rules involve an additional stage of state intervention: not only are entitlements protected, but their transfer or destruction is allowed on the basis of a value determined by some organ of the state rather than by the parties themselves.

Id.

See id. at 1127.

A program that automatically tracked and reported online crimes such as fraud or child pornography would be an example of a code solution tailored to a liability regime. Legal authorities would use this information to impose the state-mandated cost for such activities, including injunctions, fines, or imprisonment.

I. Trotter Hardy has advanced three general explanations for this: reductions in the costs of communication, reductions in the costs of recording data, and the facilitation of institutional innovations. See Trotter Hardy, Property (and Copyright) in Cyberspace, 1996 U. Chi. Legal F. 217, 219-237 ("[A] principal characteristic of property rules — that we rely on them in situations of low transaction costs — applies to cyberspace, because cyberspace lowers the cost of communicating and, hence, of transacting over rights to use private property."). Code innovations may further reduce the costs of transacting in cyberspace. See, e.g., infra pp. 1646-48 (discussion of Platform for Privacy Preferences (P3P)).

A regime that reflects individual preferences is favored because it may lead to the socially optimal regime. Assuming that individuals make decisions to maximize their welfare and that they behave rationally in the aggregate, a regime that reflects the aggregate of individual preferences is likely to maximize social welfare.

In arguing that code solutions facilitate the institution of a property rule regime in cyberspace, this Part builds upon the work of Trotter Hardy, which applied the property rule paradigm to copyright in cyberspace. See Hardy, supra note 13.
explore the particular ways in which code may be used to lower transaction costs thereby enabling a property rule regime.

B. Content Control: Enabling the Private Regulation of Decency

Pornography is abundantly available on the Internet. Moreover, because the current architecture of the Internet distinguishes poorly between adults and children, children can easily access pornographic Internet sites. Children's ready access to pornography online has not escaped the notice of parents or Congress, but to date, attempts to regulate it through law have failed.

In the United States, pornography is difficult to regulate because most forms of pornography, with the exception of child pornography, are considered legally "indecent" rather than "obscene." Because

---

16 See Brief for Appellant, Reno v. ACLU, 521 U.S. 844 (1997) (No. 96-511), available in 1997 WL 32931, at *4a-*36a (describing the vast number of pornographic websites on the Internet and the ease with which they can be found). A recent search, conducted by entering "+porn +xxx +sex" into the AltaVista search engine, retrieved 2,298,215 results.

17 The "reasonable attempt" made by most porn site operators to ensure that their visitors are not minors is to warn visitors that the material provided is intended for adults only and should not be accessed by children. See, e.g., Smutland (visited Apr. 19, 1999) <http://www.smutland.com> (on file with the Harvard Law School Library) (providing the warning: "[this site contains XXX-RATED sexually explicit adult material intended for individuals 18 years of age or older. IF YOU ARE UNDER 18 CLICK ON YOUR BROWSER'S BACK BUTTON"). However, because a single click of the mouse is often all that is required to certify one's age and there are no immediate consequences for falsely certifying one's age, few children are likely to be deterred by this warning.

18 In 1996, the Communications Decency Act (CDA) was drafted to address the problem by prohibiting the knowing transmission or display of obscene or indecent material to anyone under eighteen years of age. See Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-35 (1996). One year later, the Supreme Court struck down the law as unconstitutional because the statute limited the First Amendment rights of adults to access pornographic sites. See Reno v. ACLU, 521 U.S. 844, 874 (1997) (holding that the Act "suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another"). In 1998, the Children's Online Protection Act was passed with the hope that it would succeed where the CDA failed. See Child Online Protection Act (COPA), Pub. L. No. 105-277, § 231, 112 Stat. 2681-2736 (1999) (to be codified at 47 U.S.C. § 201) (punishing "[w]hoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors"). However, COPA has been enjoined and is currently facing constitutional challenge. See ACLU v. Reno, No. Civ.A. 98-5591, 1999 WL 44852, at *2 (E.D. Pa. Feb. 1, 1999) (granting a preliminary injunction at the ACLU's behest to prevent enforcement until constitutional challenges have been heard); see also supra Part II, at notes 96-97 and accompanying text.

19 Of course, one of the most important features of the Internet is that it is transjurisdictional. See infra Part VI.A; infra p. 1689 n.49 (discussing China and Singapore).

20 See Osborne v. Ohio, 495 U.S. 103, 111 (1990) (holding that a state's interest in preventing the production and distribution of child pornography permits proscription of the possession and viewing of such material); New York v. Ferber, 458 U.S. 747, 764 (1982) ("[C]hild pornography... like obscenity, is unprotected by the First Amendment.").

21 The distinction between indecency and obscenity is murky. In Miller v. California, 413 U.S. 15 (1973), the Supreme Court established a three-prong test for obscene material:
Americans have a First Amendment right to access indecent but not obscene material, they have a qualified right to pornography. Notwithstanding this right, in *Ginsberg v. New York*, the Supreme Court held that the Constitution permits children to be prevented from accessing any material deemed "harmful to minors." Thus, material that is considered indecent for adults may be legally obscene for children. However, attempts to regulate children's access to harmful material must be narrowly tailored to restrain only minors according to the least restrictive means. The current entitlement scheme regarding pornography is thus subject to many qualifications, depending partly on the nature of the content and partly on the putative viewer. Furthermore, *Ginsberg* places the burden of this entitlement squarely on the distributors of pornographic content by forcing them to make reasonable attempts to determine their customers' ages.

Code solutions to the problem of cyberspace pornography follow one of two courses: they either facilitate the current entitlement or enable a shifting of the entitlement. Age verification services are a code solution that seek to accomplish the former, and filters are a code solution that seek to accomplish the latter.

| (a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. |
|---|---|

*Id.* at 24 (citations omitted) (internal quotation marks omitted). Moreover, only those in possession of "hard core" pornography may be subject to prosecution under obscenity laws based on the standards of their community. *See id.* at 27.

22 *Sable Communications, Inc. v. FCC*, 492 U.S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment . . . ").


25 *Id.* at 633.

26 In holding that the state may constitutionally restrict children's access to pornography, the Court did not rule that the First Amendment applies differently to children than it does to adults, but rather that the definition of obscenity applies differently to children than it does to adults. Thus, a state may "adjust[] the definition of obscenity to social realities by permitting the appeal of this type of material to be assessed in terms of the sexual interests . . . of such minors." *Id.* at 638 (internal quotation marks omitted).

27 *Sable*, 492 U.S. at 126 (1989) ("The Government may . . . regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest . . . It is not enough to show that the Government's ends are compelling; the means must be carefully tailored to achieve those ends." (citations omitted) (internal quotations omitted)). *But see* Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141, 193 (arguing that, contrary to the Court's current balancing approach, substantial burdens on speech are unconstitutional even if they are necessary to protect children).

28 *Ginsberg*, 390 U.S. at 645 (accepting a statutory provision excusing a defendant's honest mistake in selling pornography to minors provided that he made "a reasonable bona fide attempt to ascertain the true age of such minor" (internal quotation marks omitted)).
Under an age verification regime, Internet users access a service and provide it with information to validate their age.\(^{29}\) Once this information is confirmed, the user is provided with an adult verification number, either in the form of a digital certificate stored on the user's computer and accessed automatically by adult websites\(^ {30}\) or in the form of a password, entered by the user each time she visits an adult site.\(^ {31}\) Although the use of age verification services could be mandated at any level,\(^ {32}\) the entitlement-burden allocation approved in *Ginsberg* suggests that the requirement that content providers "reasonably attempt" to supply only adults with pornography can be viewed as a requirement that they use an age verification system to manage access to their sites.\(^ {33}\)

An age verification regime permits the current entitlement allocation to be instituted through code. This solution differs from the status quo, however, in that it enables enforcement through a property rule rather than a liability rule. If the use of age verification services is accepted as a "reasonable attempt" to determine user age, the law will excuse site operators from liability provided that they engage an age verification service. Thus, the verification service assumes the burden of distinguishing adults from children; the site operator is free to fill all requests from verified adults; and only users with proof of age obtain access to online pornography. The burden and entitlement are thus reallocated through contract as in a property rule regime.

Filtering technology is another code solution that institutes property rule protection against online pornography. Filters are computer programs that automatically screen Internet content and block access

\(^ {29}\) Because these services must collect personally identifying information in order to verify age, privacy concerns may arise. *See infra* section D.


\(^ {31}\) *See, e.g.*, The Adult Check System (visited Apr. 19, 1999) <http://www.adultcheck.com> (on file with the Harvard Law School Library) (stating goals of "regulatingj" ourselves and the Net, helping to prevent minors from accessing adult oriented material, yet allowing Adults to communicate freely").

\(^ {32}\) *See* Lawrence Lessig and Paul Resnick, *The Architectures of Mandated Access Controls 11–12* (Jan. 12, 1999) (unpublished manuscript, on file with the Harvard Law Review) (suggesting that the target of enforcement should be the party — either sender, receiver, or intermediary — who can be most easily or cheaply reached).

\(^ {33}\) *Ginsberg*, 390 U.S. at 645. The transjurisdictional nature of the Internet raises questions regarding the effectiveness of this solution. Site operators and network administrators in Holland, for example, would not be subject to an American law requiring age verification. In response to such a system, indecent content providers are likely to migrate to less restrictive jurisdictions.
according to a set of user preferences. Filters may be applied by a variety of parties at a variety of levels, including personal computers, search engines, Internet service providers, and "proxy-filter" sites. However, because government attempts to mandate filtering constitute state action — bringing the mandate under strict constitutional scrutiny — and because filtering is not likely to be the least restrictive means of regulating Internet pornography, successful private organizations and individual end-users are most likely to institute successful filtering solutions. I thus exclusively address questions relating to a private filtering regime.

34 I use the term "filter" generically to refer to software programs that block content as well as labeling protocols, such as PICS, that may be used to enable blocking programs. See Platform for Internet Content Selection (visited Apr. 19, 1999) <http://www.w3c.org/PICS> (on file with the Harvard Law School Library) [hereinafter Platform]. For an overview of filtering technology, see Paul Resnick, Filtering Information on the Internet, SCIENTIFIC AMERICAN, Mar. 1997, at 62, and Lorrie Faith Cranor, Paul Resnick & Danielle Gallo, Technology Inventory (visited Apr. 19, 1999) <http://www.research.att.com/projects/tech4kids/+4k.html> (on file with the Harvard Law School Library) Furthermore, although the principle concern of this section is pornography, filters may be used for a variety of purposes. For example, a corporation may install a filter to prevent its employees from accessing sites unrelated to their work. It is also worth noting that P3P, the code solution to the privacy problem discussed in section C, see infra pp. 1645–49, is a kind of filter that screens websites in order to warn users about the site owner's privacy practices.


36 See, e.g., AV Family Filter FAQ (visited Apr. 19, 1999) <http://jump.altavista.com/cgi-bin/FF#FAQ> (on file with the Harvard Law School Library) (providing answers to frequently asked questions about the AltaVista filter).


38 Proxy filters are servers through which all of a user's information exchanges are routed, which make content control decisions for the end-user. See, e.g., Family Safe Media, Proxy Based Server-Side Filtering (visited Apr. 19, 1999) <http://www.familysafemedia.com/proxy_filter.html> (on file with the Harvard Law School Library) (describing the benefits of their proxy filter system); Wayne B. Salamonsen & Roland Yeo, PICS-Aware Proxy System vs. Proxy Server Filters (visited Apr. 19, 1999) <http://www.irdu.nus.sg/~wayne/paper.html> (on file with the Harvard Law School Library) (noting the differences between PICS proxy systems and proxy server filters).

39 State-mandated filtering is likely to fail strict constitutional scrutiny because current filtering technology blocks more categories of constitutionally protected speech than other means, such as age verification systems. The problems of state action and strict scrutiny have recently been raised in the context of public libraries. According to an American Library Association survey, 14.6 percent of public libraries apply filters to at least some of their Internet-enabled computers. See American Library Ass'n, Office for Info. Tech. Policy, The 1998 National Survey of U.S. Public Library Outlet Internet Connectivity (visited Apr. 19, 1999) <http://www.ala.org/oitp/research/survey98.html> (on file with the Harvard Law School Library). The emerging rule appears to require libraries with more than one Internet-enabled computer to separate children's computers from adults' computers and to install filters only on the children's computers. See Mainstream Loudoun v. Board of Trustees, 24 F. Supp. 2d 552, 570 (E.D. Va. 1998) (holding that the application of filtering technology to all computers in a public library violates the First Amendment); infra pp. 1642–43.

40 In the absence of state action, there is no constitutional issue. The public forum doctrine may be used to construct state action, especially in cases of high-level private filtering. To date,
By enabling end-users to choose different levels of control, filters provide a private solution to the problem of online pornography. Rather than forcing parents to rely on the pornographer’s legal obligation not to provide pornography to children, filters enable parents directly to control the content appearing on their home computer screens.\(^4\) Moreover, by allowing parents to manipulate the blocking criteria, filtering technology provides the means for individuals to select the level of protection that best suits the needs of their families.\(^4\)

Because computer owners possess better information about the age and maturity levels of those using their computers than do site operators, computer owners are in a better position to make decisions about what content to block. On the one hand, parents know the ages of their children and make decisions about the times, places, and purposes for which their children can use the family computer. On the other hand, absent age-verification technologies, site operators are ill-equipped to determine the ages of their visitors or the information to which each visitor should have access. The Ginsberg rule may thus represent an inefficient allocation of the burden of distinguishing adults from children. A more efficient allocation of the burden might require end-users to control the material that is displayed on their own monitors and entitle online pornographers to permit all access requests.

A default rule of no protection against online pornography would allocate the burden of protection to computer owners. Such a rule would provide the necessary incentives for end-users to solve the pornography problem for themselves. Those who wished to prevent the delivery of pornographic material to their home computer would be required to contract with filter providers for a solution.\(^4\) Although however, courts have been unwilling to accept this argument. See, e.g., CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1021, 1028 (S.D. Ohio 1997) (permitting online service provider to filter mass e-mail sent to its subscribers); Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436, 456 (E.D. Pa. 1996) (same). But each of these cases involved commercial solicitations rather than political speech. Courts might treat the public forum argument more favorably in the context of political speech. See supra Part III.C.

\(^4\) Of course, children may still be able to access pornography by going elsewhere — for example, to a neighbor’s computer — but this is no different from the current regime, in which enterprising youngsters can obtain adult magazines elsewhere even if their parents are careful not to keep them at home.

\(^4\) For example, the Cyber Patrol “CyberNOT” List enables parents to choose to block content from a variety of categories, including: “Partial Nudity; Nudity; Sexual Acts/Text; Gross Depictions; Intolerance; Satanic or Cult; Drugs and Drug Culture; Militant/Extremist; Violence/Profanity; Questionable/Illegal & Gambling; Sex Education; and Alcohol & Tobacco.” Fact Sheet, supra note 35. PICS, on the other hand, has the potential to offer as many blocking alternatives as there are web-users, because it allows filtering labels and lists to be generated by independent Internet users. See Platform, supra note 34.

\(^4\) Pornography protection would thus operate as an “opt-in” regime, under which pornography would be unfiltered unless the user opted for filtering. The alternative “opt-out” regime, under which pornography would be filtered unless the filter were deactivated, is also possible but may be unconstitutional if state action is needed to mandate the filtering of all material. See supra pp. 1640–41.
this regime might appear to burden the end-user excessively, it is identical to the current legal vacuum in which filtering technology has developed.\textsuperscript{44}

However, a private filtering regime is not without its costs. The central cost of filtering is its reduction in the free flow of online information. In particular, two features of filtering technology pose the greatest threats to the flow of information: its inaccuracy and its applicability at any level in the information stream.

The current generation of filtering programs suffers from inaccuracy.\textsuperscript{45} They may block too much or too little information. When filters block too much, they foreclose access to socially beneficial information.\textsuperscript{46} This foreclosure of access imposes an externality on the education of those most likely to be subject to filtering: children.\textsuperscript{47} Moreover, although filtering technology may improve,\textsuperscript{48} the subjectivity of ratings and the ambiguity of standards may be intractable problems.\textsuperscript{49} Thus, filters may never be made perfectly accurate.

Another cause for concern is the level at which filtering occurs in the stream of information distribution. Individual computer owners are not the only consumers of filtering programs. Filters can be applied by any entity\textsuperscript{50} at any level in the stream of content distribution.

\textsuperscript{44} Because of the recurring difficulty in enforcing the Ginsberg entitlement online, the default rule has essentially been no protection for end-users from pornography.

\textsuperscript{45} Errors in filtering software may result either from the machines that automatically screen material or from the humans who set the standards for judging the material. See Jonathan Weinberg, \textit{Rating the Net}, 19 HASTINGS COMM. \& ENT. L.J. 453, 459-470 (1997); see also Lessig, \textit{Speech}, supra note 30, at 654 ("[T]he blocking effected by these systems is crude, and the effect of the blocking created is far too broad").

\textsuperscript{46} See Weinberg, \textit{supra} note 45, at 460-62 (noting that pages of news organizations, support groups, political groups, and constitutional issues are often blocked by software filters); Electronic Privacy Information Center (EPIC), \textit{Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet} (visited Apr. 19, 1999) <http://www2.epic.org/reports/filter-report.html> (on file with the Harvard Law School Library) (describing the results of a study that concluded that "the world's first family-friendly Internet search site" in fact "prevented children from obtaining a great deal of useful and appropriate information that is currently available on the Internet"); Jonathan Wallace, \textit{CyberPatrol: The Friendly Censor} (visited Apr. 19, 1999) <http://censorware.org/essays/cypa_jw.html> (on file with the Harvard Law School Library) (describing socially beneficial speech that is blocked by CyberPatrol).

\textsuperscript{47} This threat will be most pronounced in a regime of high-level filtering. See infra p. 1643.

\textsuperscript{48} See Weinberg, \textit{supra} note 45, at 460 ("These problems . . . may be addressed through proper software design.").

\textsuperscript{49} Subjectivity and ambiguity may prevent even site creators from accurately evaluating their own sites. See Jonathan Wallace, \textit{Why I Will Not Rate My Site} (visited Apr. 19, 1999) <http://www.spectacle.org/cda/rate.html> (on file with the Harvard Law School Library) (describing an author’s crisis of conscience in rating material that may be considered indecent but that also has scientific, literary, artistic, or political value and cautioning against rating systems which “lump [such material] together with the Hot Nude Women page").

\textsuperscript{50} For example, employers may apply filters to bar employees from accessing non-work-related sites. See, e.g., Rosilind Retkwa, \textit{Corporate Censors}, \textit{INTERNET WORLD}, Sept. 1996, at 60 (describing the employer concerns about employee Internet use at work). Private universities may use filters to make their computers “politically correct.” See, e.g., <http://www.eff.org/pub/Censor
Many "upstream" providers, such as search portals and Internet service providers, have integrated filters into their products. One potential problem with upstream filtering is invisibility. Filtering agents are currently under no obligation to notify Internet users when searches are filtered. If Internet users do not know that their online activity is being filtered, they may be unable to disable the filter. Thus, upstream filtering may impose an externality on individuals who want unfiltered Internet activity but who are either unaware of the filtering or are unable to stop it.

Because it disrupts the flow of information, filtering may seem antithetical to free speech values. Individuals must therefore weigh the cost of the disruption to the free flow of information against the benefit of reducing children's access to harmful online content. Filtering solutions will respond to consumer demand for a property rule that will protect them against pornography. Similarly, a number of service providers and search portals are likely to hold themselves out as wholly unfiltered in order to capture the market of users who favor unfettered Internet access. Presumably, the countervailing interests of these users in unfiltered browsing will ensure that it remains available. In this way, the precise level of filtering will be determined by the aggregate of individual preferences as expressed through the market.

51 See Lessig, Speech, supra note 30, at 661 ("[PICS] does not inhibit upstream filtering; nor does it require that upstream filtering be reported; nor does it have built within it any narrowing of the range of content that can be filtered . . . .").

52 See, e.g., Cyber Patrol Partners (visited Apr. 19, 1999) <http://www.cyberpatrol.com/partners.htm> (listing the companies that use Cyber Patrol technology in their products, including America Online, AT&T, IBM, Microsoft, Netscape, and Prodigy); see also supra notes 35-38 (discussing the levels at which filters may be applied).

53 Those who are not technologically adept may not be able to disable the filter even after they are notified that it is active.

54 This model assumes that there is a sufficient market for unfiltered Internet access such that at least some service providers will hold themselves out as wholly unfiltered in order to capture that market. However, because market decisions require a sufficient level of information, invisible filters may produce a market failure whereupon individuals are unable to choose in accordance with their individual preferences.
C. Privacy Protection: Contracting for a Property Right in Personal Information

The Internet poses unique threats to personal privacy. Information may be collected from Internet users and aggregated to create a profile of their online activities and preferences. Moreover, this collection and aggregation of information may take place without the users' knowledge.\(^55\) The current architecture of the Internet facilitates these practices in three ways. First, the user's Internet Protocol (IP) address may be mapped.\(^56\) Second, "cookies" may be placed on the user's computer.\(^57\) Third, site operators exercise vast discretion in storing, releasing, and trading information gathered from users online.\(^58\)

Surveys indicate that Internet users are concerned about these threats to their personal privacy,\(^59\) and the Federal Trade Commission...
acknowledges that current Internet architecture poses a threat to privacy. However, despite longstanding scholarly concern for personal privacy, there is no clear legal liability for the collection of personal information. The current entitlement to personal information benefits the collector and burdens the individual user, thus granting the collector full title to whatever information she can collect and leaving the individual from whom the information is taken with no recourse.

Although some commentators have advocated the shifting of this entitlement through law, a code solution may offer sufficient privacy protection. Several technologies have been developed to address personal information benefits the collector and burdens the individual user, thus granting the collector full title to whatever information she can collect and leaving the individual from whom the information is taken with no recourse.

The Fourth Amendment protects individuals against searches by government officials that violate reasonable expectations of privacy, see U.S. CONST. amend. IV, and a patchwork of ad hoc federal statutes address particular privacy concerns, see EPIC, Online Guide to 105th Congress: Privacy and Cyber-Liberties Bills (visited Apr. 19, 1999) <http://www.epic.org/privacy/bill_track.html> (on file with the Harvard Law School Library). However, no federal enactment prevents the collection of personal data online. Although some states have enacted a right to privacy, few appear to support a cause of action for the collection of personal information online. See Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 FED. COMM. L.J. 195, 221-34 (1992) (summarizing state privacy laws).

One commentator suggests that the current regime produces an inefficient allocation of resources:

The market failure has occurred because of a poor social choice in the allocation of property rights. Under current law, the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers. Individuals have no property rights in their own personal information. As a result, they cannot participate in the flourishing market for personal information, i.e., they receive no compensation for the use of their personal information. As a further consequence, the price of personal information is so low that information-intensive industries become inefficient in its use.


See FTC, Report, supra note 58, at 43 (recommending “that Congress develop legislation to require commercial Websites that collect personal identifying information from children 12 and under to provide actual notice to the parent and obtain parental consent”); Connie Guglielmo & Will Rodger, Can Net Privacy Coexist with E-Commerce? (visited Apr. 19, 1999) <http://www.zdnet.com/zdnn/content/inwo/1216/65765.html> (on file with the Harvard Law School Library) (“We want legislation; we want encryption; we want anonymity; and we want it now.” (quoting EPIC director Marc Rotenberg)).
vacy problems in cyberspace, but the most comprehensive code solution to reallocate the entitlement to personal information between collectors and Internet users is the Platform for Privacy Preferences (P3P).

Currently under development, P3P is a system of protocols through which site providers and Internet users can reach agreement on privacy practices. It works as follows: A user acquires P3P software and configures her privacy preferences. She may, for example, set the software to block or warn her about any site that collects and sells personal information. Once configured, the software works in conjunction with the user’s browser program. Each site visited by the user sends a machine-readable P3P proposal to the user’s computer. If the site’s privacy practices, as embodied in its P3P proposal, are consistent with the user’s privacy criteria, then a privacy agreement is automatically reached and the user gains access to the site without any interruption in her browsing. If, however, the site’s privacy practices are inconsistent with the user’s privacy criteria, then the user is prompted to decide whether she desires to access the site despite the incompatibility of its privacy practices with her preferences.

By reallocating the entitlement in personal information to the Internet user, granting her control over the release and use of her personal information, P3P establishes a technologically — as opposed to a legally — protected property right in personal information. Once a P3P regime is in place, personal information is transformed into property that can be transferred only with the holder’s consent. Of

---


66 Although the remainder of the discussion focuses on P3P, the arguments apply to all software protocols that enable contractual solutions to the problem of privacy.


68 The proposal states in P3P compliant form the site’s privacy practices. The proposal may include additional information, such as the site’s membership in a third-party assurance organization that polices and guarantees the veracity of its privacy statements. See Reagle & Cranor, supra note 67. Furthermore, more than one proposal may be sent by the site provider, in which case P3P will analyze each to determine which, if any, are acceptable. Id. For more on assurance agencies, see the discussion of TRUSTe and BBBOnline in note 72 below.

69 P3P thus functions as a type of filter. Instead of filtering sites with “indecent” material, however, P3P filters sites with unacceptable privacy practices.

70 P3P may be most effective when used in conjunction with anonymizing and cookie-blocking technologies to create a comprehensive privacy solution.
course, she can always exchange pieces of personal information for cash or for access to a particular Internet site or service, in which case the party purchasing the personal information effectively pays a fee for the entitlement. A P3P regime thus offers property rule protection for the privacy entitlement.

A property rule is preferable to a liability rule for the protection of privacy in cyberspace because P3P greatly reduces privacy transaction costs. Negotiations are conducted instantaneously and automatically via software protocols that correspond to user preferences and site practices. Moreover, the multitude of potential substitutes for any particular type of Internet content, coupled with the intense competition among content providers for Internet traffic, ensures a high level of site responsiveness to user preferences. Thus, although the costs of negotiating privacy agreements in real-space may be prohibitively high, low communication costs and automated negotiations minimize transaction costs in cyberspace and enable privacy agreements to be reached efficiently.

A P3P regime will result in the optimal level of privacy protection because it permits individuals to value privacy according to their personal preferences. Individual users will configure their privacy preferences to protect privacy according to the value that they attach to it. In the resulting privacy market, those who value their personal information less will part with it more easily than those who value it more. This market will likely result in a de facto level of privacy protection, in which the interests of information collectors are balanced against the interests of individual users and site operators. Because

---

71 For example, a recent AltaVista search for websites offering "sports scores" retrieved 58,548 results. A search for "stock quotes" retrieved 146,803 results.

72 Verification authorities may be used to police the terms of these agreements. See, e.g., Better Business Bureau Online (visited Apr. 19, 1999) <http://www.bbbonline.com/privacy/index.html> (on file with the Harvard Law School Library) (offering an introduction to its verification program); TRUSTe (visited Apr. 19, 1999) <http://www.truste.org/about> (on file with the Harvard Law School Library) (same). These authorities monitor the congruence of sites' privacy policies with their privacy practices, holding them liable under the terms of their membership agreements for any deviation. Site providers desiring to maximize traffic to their site have an incentive to subscribe to such authorities if enough users mandate the use of verification seals in their privacy preferences under a P3P regime.

73 This conclusion follows from our assumption that the optimal level of protection is the level that most members of society prefer. See supra p. 1636 and note 14.

74 In this market, information collectors will offer incentives — such as prizes, cash, or access to a popular site — for users to part with their personal information.

75 The de facto level represents the protection most commonly offered by site operators as a default. This level is chosen in response to the aggregate of user preferences, but P3P preserves the freedom of individuals to choose greater or lesser protection.

76 The simplest model of this market assumes that the primary goal of site operators is to maximize traffic to their sites and that the main interest of Internet users is to access as many sites as possible without compromising their privacy preferences. Accordingly, site operators will collect personal information only to the extent that it does not adversely impact traffic to their sites,
this market features intense competition and very low transaction costs, the resulting de facto level of protection is likely to be the most allocatively efficient solution, reflecting the aggregate of individual preferences.

However, enabling individuals to determine their own privacy levels may entail social costs.\textsuperscript{77} Privacy, as discussed in this section, essentially involves the ability to conceal one's personal information from others. The online concealment of real-space identity, for example, may create a disincentive to cooperate\textsuperscript{78} and may encourage socially reckless behavior.\textsuperscript{79} Moreover, because much of the personal information that is gathered online is used to target Internet advertising\textsuperscript{80} and because advertising is a major source of revenue for site providers,\textsuperscript{81} the concealment of personal information may limit site providers' ability to attract advertising and thus impair a major source of revenue.\textsuperscript{82} In their search for alternative revenue sources, providers may charge greater access fees for use of their sites, thus reducing the amount of low-cost or free content available on the Internet.\textsuperscript{83} Because it may result in an increase in the cost of online content, the concealment of personal information may impose social externalities.

Although the costs and benefits of privacy protection must be carefully weighed, P3P offers excellent online privacy protection. By enabling individuals to express their privacy preferences through code, P3P reduces transaction costs and leads to automated privacy agreements. When aggregated, these individual preferences will exert pressure on site operators to conform their privacy practices to user preferences. The resulting regime will thus reflect the value that individuals attach to privacy.


\textsuperscript{78} See David R. Johnson, \textit{The Unscrupulous Diner's Dilemma and Anonymity in Cyberspace} (visited Apr. 19, 1999) <http://www.cli.org/DRJ/unscrup.html> (on file with the Harvard Law School Library) ("[T]o achieve a civilized form of cyberspace, we have to limit the use of anonymous communications."); \textit{supra} Part II.C.

\textsuperscript{79} See, e.g., Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997) (upholding summary judgment of Zeran's claim against AOL for defamatory messages posted by an unidentified third party).

\textsuperscript{80} See \textsc{Cliff Allen, Deborah Kania & Beth Yaeckel, Internet World Guide to One-To-One Web Marketing} 223–99 (1998) (discussing the way in which advertisers build and use Internet user profiles).

\textsuperscript{81} See Report: Global Online Ad Spending to Hit $15 Billion by 2003, \textit{InternetNews} (Aug. 20, 1998) <http://www.internetnews.com/IAR/article/0,1087,129971,00.html> (on file with the Harvard Law School Library) (citing the results of a 1998 study estimating that U.S. spending for Internet advertisements will increase eight-fold to $10.5 billion over the next five years)

\textsuperscript{82} Without the guarantee that their advertisements will reach the target audience, advertisers are likely to pay less for online advertising.

\textsuperscript{83} Note, however, that very little is actually "free" under the current architecture of the Internet. The price of Internet content must be understood to include the value of the personal information that is collected by site providers and used to generate revenue.
D. Copyright Protection: Balancing Access and Exclusion

The Internet provides an excellent means for the infringement of copyrights. Anything that can be copyrighted can be converted into digital form, uploaded onto a website, and sent across the Internet, thereby enabling a perfect digital copy to be downloaded onto another computer. The abundance of such information on the Internet has led some to conclude that "[i]nformation wants to be free."84

However, the prospect of free information upsets the delicate balance of copyright law.85 According to the standard economic rationale for copyright, free information renders creators unable to recover costs and thus creates a disincentive for the production of information.86 Sensitive to these concerns, the Framers of the Constitution granted Congress the power to copyright works in order to encourage their creation.87 Copyright, however, is not an absolute right to exclude.88 Instead, it balances exclusive rights against the public benefit of access to copyrighted works. Access rights are preserved by doctrines that limit the duration of copyright,89 the control that an author can exercise over a copy after its first sale,90 and the ability of the author to prevent certain uses of the copyrighted work deemed "fair."91 Copyright law can thus be viewed as an attempt to balance the entitlement

85 See Anne K. Fujita, The Great Internet Panic: How Digitization Is Deforming Copyright Law, 2 J. TECH. L. & POL'Y 1, ¶ 1 (Fall 1996) <http:lljournal.law.ufl.edu/-techlaw/z/fujita.htm> (on file with the Harvard Law School Library) ("The new technology of digitization in our present 'Information Age' has upset the delicate balance created and maintained by copyright law between the rights of authors, users, and the industries that collect the money.").
86 See William M. Landes & Richard A. Posner, An Economic Analysis of Copyright Law, 18 J. LEGAL STUD. 325, 326 (1989) ("For copyright law to promote economic efficiency, its principal legal doctrines must, at least approximately, maximize the benefits from creating additional works minus both the losses from limiting access and the costs of administering copyright protection . . . ").
87 See U.S. CONST. art I, § 8, cl. 8 ("The Congress shall have Power . . . [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").
88 Exclusive rights under copyright are essentially limited to the right to prevent the production and distribution of copies. See 17 U.S.C. § 106 (1994) (listing the exclusive rights in copyrighted works as reproduction, preparation of derivative works, distribution, and public performance and display).
90 See 17 U.S.C. § 109(a) (1994) ("[T]he owner of a particular copy or phonorecord . . . is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.").
91 See 17 U.S.C. § 107 (1994) ("[T]he fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright.").
between exclusive rights (encouraging creation) and access rights (enabling consumption).

The current architecture of the Internet tips the copyright balance in favor of access. The elimination of real-space constraints on copying and distribution has led to widespread "information piracy" in cyberspace. Unless it can be controlled, such piracy is likely to engender strong disincentives for content providers to make commercially valuable information available on the Internet. As a result, the copyright imbalance may hamper the growth of the Internet.

Code solutions may reset the entitlement balance of copyright law. Although technological efforts to protect intellectual property online have taken many forms, the most comprehensive code solution to the problem of online copyright infringement is the development of rights-management containers, which not only protect copyrighted material, but also strengthen the content provider's rights allocation.

Rights-management containers perform two interrelated functions. First, such systems ensure that content is kept in a secure "container," either hardware or software, which performs encryption and decryption on the digital content. Because the content is encrypted and useless outside of the container and because only the container has the

---

92 Digitization enables serial reproduction at negligible cost, while interconnectivity enables cost-free instant distribution. See NICHOLAS NEGROPONTE, BEING DIGITAL 59 (1995) ("With less than a dozen keystrokes, I could redeliver that material to literally thousands of people all over the planet. . . .").


94 Commercial material includes music and video content as well as best selling books. It may be loosely generalized as material whose creation is explained by the economic rationale of copyright.

95 Examples of these technologies include password-access systems and digital watermarking. See, e.g., Digimarc & Copyright Protection (visited Apr. 19, 1999) <http://www.digimarc.com/applications/copyright/copyright_in.html> (on file with the Harvard Law School Library) (explaining the ways in which digital watermarking of online content enables copyright owners to find unauthorized copies of their work online and to prove, with the watermark, that the copies originated from their work); Lexis-Nexis Xchange (visited Apr. 19, 1999) <http://www.lexis.com/research> (on file with the Harvard Law School Library) (prompting the user for an identification name and password).


key to decrypt it, the content can be accessed only through the container. Second, the container stores precise instructions detailing which uses to permit, which uses to deny, and how much to charge for each, thereby "managing" the rights relationship between user and content provider. Because these instructions are embedded in the container and must be passed through every time the content is accessed, they enable the content provider to maintain complete control over every interaction between user and content.

Of course, rights-management technologies are not perfect. The protection offered by container systems is premised upon the assumption that the digital information is available exclusively within the container. Thus, rights-management containers are powerless against a third-party provider who offers the same digital content outside of the digital container, circumventing the protective system and posting the content on a website to be downloaded for free. Confronted by such problems, copyright owners may seek to supplement rights-management technologies with legal protections.

98 This is accomplished through public and private key cryptography, which can be made strong enough to discourage almost all efforts to break it. See generally A. Michael Froomkin, The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. PA. L. REV. 709, 718–34 (1995) (detailing some of the uses of cryptography and the legal issues raised by these uses).


100 The paradigmatic example of this problem is the file format known as "mp3," which allows digital audio files to be compressed to a fraction of their usual size, thus enabling them to be stored and played on computers. Shareware programs are available to convert compact discs (CDs) into mp3 format so that any CD can be digitally encoded and distributed via the Internet, e-mail, or floppy disk. Rights-management technology is not a solution to the existing mp3 piracy problem. It merely provides a means for the legitimate online distribution of digital content. See MP3.com (visited Apr. 19, 1999) <http://www.mp3.com> (on file with the Harvard Law School Library) (providing links to mp3 news and resources); MP3 Rocks the Web, WIRED (Feb. 23, 1999) <http://www.wired.com/news/news/mpthree> (on file with the Harvard Law School Library) (linking to news stories on mp3 and related technologies); see also Recording Indus. Ass’n of Am., Inc. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624, 625 (C.D. Cal. 1998) (denying the RIAA’s request for a temporary restraining order to prevent distribution of the Rio, a device capable of storing and replaying mp3 files).

101 See, e.g., Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (to be codified at 17 U.S.C. § 1201) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title."). One commentator argues that, because rights-management containers can be used to lock up information that should be freely accessible, there should be a “right to hack” into rights-management systems in order to obtain this information. See Julie E. Cohen, Copyright and the Jurisprudence of Self-Help, 13 BERKELEY TECH. L.J. 1089, 1141 (1998) ("If the user privileges established by copyright... are to mean anything, users must be afforded affirmative rights to protect themselves. A ‘right of fair breach’ is meaningless unless it includes a right to effectuate the breach — a right to hack the digital code that implements and enforces the challenged restriction"); Pamela Samuelson, The U.S. Digital Agenda at WIPO, 37 VA. J. INT’L L. 369, 410 (1997) (criticizing "the perceived need for law to regulate infringement-enabling technologies"). To the extent that liability rule protection is neces-
If the impact of these technological problems can be minimized, then the adoption of rights-management containers to protect intellectual property represents a shift in the nature of intellectual property rights, granting copyright owners far greater control over their works than they would otherwise enjoy under existing copyright law. Rights-management containers change the nature of the copyright entitlement by granting copyright owners extra-legal and absolute control over their material, thus reversing the Internet trend toward access rights and resetting the copyright balance in favor of exclusion. This shifting of the rights allocation may significantly abridge the three doctrines that had guaranteed access rights under copyright law: public domain, first sale, and fair use.

First, rights-management systems may constrict the public domain. Currently, the copyright holder loses exclusive rights to her work at the end of the copyright term. Because container-based technology provides direct control of access and its power depends not on the authority of law but on the strength of its technology, technologically protected works may never lapse into the public domain. Obviously, as long as substitutes for online digital content exist — as long as some information remains available in old-fashioned book form — information will eventually fall into the public domain. However, digital information that is provided only within containers — as might even-
tually be the case for music, video, and software — might never be released from technological protection.109

Second, rights-management technologies may nullify the "first sale" doctrine. Currently, copies of a copyrighted work can be freely transferred after the initial purchase. The first sale doctrine permits books and music to be loaned or resold by limiting copyright owners' ability to control the distribution of copies of their works beyond the first sale. However, rights-management technology enables copyright owners to control access to the work beyond the initial distribution.110 Because the providers of technologically protected works control access rather than copies, it is irrelevant whether they are charging the first or the fifty-first user to access a particular copy; they can still collect the fee. As a result, the first sale doctrine is effectively destroyed.

Finally, rights-management technologies may expunge the fair use doctrine. Currently, fair use is a defense to copyright infringement. If the issue of infringement is never reached — because rights-management protection prevents infringement before it can occur — then the fair use question never arises. Again, because information providers control access to the content, it would be within their discretion to grant or deny access for uses that might otherwise constitute "fair use."111 Moreover, the special fair use exceptions carved out of the copyright statute for libraries might also be affected by the access control of rights-management technologies,112 forcing librarians and patrons to incur an access fee for each use of technologically protected information.

Although rights-management containers facilitate the elimination of access rights, such elimination is not inevitable. Other regulatory forces favor the preservation of access rights.113 The constraint of social norms through academic criticism and public outcry114 has already risen in opposition to the potential unbalancing effects of rights-

109 Of course, the unprotectable elements of a work — for example, uncopyrightable ideas — will always be in the public domain and are thus unlikely to be substantially affected by the development of rights-management technology. See generally Jessica Litman, The Public Domain, 39 Emory L.J. 965 (1990) (offering a broad survey of the public domain by describing the theoretical justifications of the law alongside the activities of authors).

110 See infra p. 1655.

111 When asked for his opinion on fair use rights, Microsoft CEO Bill Gates is said to have replied: "You don't need fair use; we'll give you fair-use rights when you need them." See Pamela Samuelson, Legally Speaking: Does Information Really Need to be Licensed, COMM. OF THE ACM, Sept. 1998, at 15, 18 (relating the anecdote of a student intern) (internal quotation marks omitted).


113 See Lessig, Chicago, supra note 3, at 662–63 (arguing that behavior is regulated by four types of constraints: law, social norms, markets, and architecture).

114 See, e.g., Cohen, supra note 101; Pamela Samuelson, The Copyright Grab, WIRED, Jan. 1996, at 191 (criticizing the strengthening of copyright monopolies).
management technologies. Existing law may also correct some of the inequities of a rights-management regime.\textsuperscript{115}

The market, however, is likely to be the most effective regulator of rights-management regimes. Having brought rights-management technology into existence, the market is likely to play a major role in shaping the future development of rights-management technologies.\textsuperscript{116} Elements of the relationship between the market and rights-management technologies include the economic benefits of these technologies, the new types of transactions likely to develop under a rights-management regime, and the types of content that are most likely to be protected by rights-management containers.

The principal economic benefit of rights-management containers is the reduction in the transaction costs associated with intellectual property. By eliminating unauthorized access, container technology effectively eliminates free-riding, enabling the content provider to distribute the cost of the content more accurately. Internet commerce also substantially reduces the costs of distribution. The purchase price no longer needs to reflect retail costs.\textsuperscript{117} The content provider can therefore pass savings on to the purchaser, bringing the purchase price closer to the manufacturer's marginal cost.\textsuperscript{118}

The most significant new transaction type permitted by rights-management containers is metered usage. Because every transaction must pass through the container, the content provider is able to meter information transactions and to charge an incremental amount per unit of use.\textsuperscript{119} Metered usage may lead to two further developments in information commerce: the elimination of free sharing and the facilitation of superdistribution. In a rights-management regime, sharing would no longer be free because every end-user would have to go through a rights-management container and thus would be made to pay. Similarly, this mechanism allows the "superdistribution" of digital

\textsuperscript{115} For example, antitrust law may be used to prevent digital distributors from fixing prices and from charging prices far in excess of marginal cost. See Sherman Act, 15 U.S.C. § 1 (1994) ("Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is hereby declared to be illegal.").

\textsuperscript{116} Rights-management technologies arose in response to a demand by copyright owners for some means of protecting their property online.

\textsuperscript{117} Digital music, for example, no longer needs to be encoded onto a plastic disc, which is shipped to retail outlets, where it consumes shelf space and requires the attention of salespersons. Online distribution reduces manufacturing costs and eliminates the retail costs that are otherwise reflected in the final price of the merchandise.

\textsuperscript{118} Content providers pass savings on to the customer because a failure to price near marginal cost may constitute an antitrust violation.

\textsuperscript{119} See Tom W. Bell, \textit{Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine}, 76 N.C. L. Rev. 557, 566 (1998) ("More sophisticated [rights-management] systems . . . employ methods such as steganography, micropayments, and imbedded applications to give information providers exact and continuous control over proprietary information.") (footnotes omitted).
content. In this way, a popular single could spread instantly across the digital community, as friends send copies to friends, who send copies to their friends, and so on. The content provider would reap substantial rewards from such a phenomenon because rights-management containers would ensure payment for every end-use.

Finally, even in a future where rights-management containers are common, not all content is likely to be protected. Some intellectual property relies upon an economic model that differs from the traditional economic rationale for copyright. For example, compensation for academic writing takes the form of increased prestige, which may result in a tenured academic position. Because denying access to this material results in fewer people reading it and therefore in diminished fame and prestige, such producers are unlikely to use rights-management containers and are unlikely to deny access to their works if they do use them. Similarly, sites that generate revenue through advertising, such as online news sources, are unlikely to use rights-management containers to deny access because doing so might diminish the number of visitors to their site, reducing advertising revenues. Thus, market forces are likely to demand the adoption of rights-management containers to protect only commercially valuable content, such as audio or video files. Because the fair use rationale is much less applicable to this kind of content than to academic writing, the

---

120 See Brad Cox, Superdistribution, WIRED, Sept. 1994, at 91–92 (arguing that digital material, through ease of copying and distribution, enables a new kind of information commerce based on widespread distribution); see also Bell, supra note 119, at 567 (“Rights-management technology allows information providers to market documents that disallow certain types of uses (e.g., copying) and provide continuing revenue (e.g., charging 2¢ per access) regardless of who holds the document (e.g., including someone who obtained it post-first sale).”); Stefik, Letting Loose, supra note 96, at 235 (“Digital property can be anywhere on the planet without the knowledge of its creators and still make money for them whenever it is used or copied by a repository.”).

121 Providers could impose fees at any point during this transaction. It might be in their best interests, however, to charge only for the end-use because charging a fee at the copying stage might provide a disincentive to make and disseminate copies.

122 The standard economic rationale for copyright is discussed above at p. 1649 and note 86. See also Hardy, supra note 13, at 221 (describing alternative economic models for information exchange); Eric Schlachter, The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet, 12 BERKELEY TECH. L.J. 15, 24 (1997) (“An intellectual property owner can use a myriad of alternative business models to extract value from the free distribution of intellectual property. If successful, these business models will permit the cross-subsidization of intellectual property creation.”).

market may develop in such a way that the lack of a fair use exception never becomes a problem.

The market will thus protect access to copyrighted material in two ways. First, nontraditional markets will guarantee that certain kinds of material, including academic writing, will continue to be offered for free even after the widespread adoption of rights-management technologies. Second, by reducing transaction costs and enabling new transaction types, rights-management technologies will reduce consumer prices for protected material. Under current copyright law, were it to function properly on the Internet, users have very limited (if any) fair use rights to commercial content\(^1\) and would have to pay for access. By enabling them to pay less than they would in the imperfect regime, rights-management technologies may actually increase user access to copyrighted material.

Because the reallocation of intellectual property rights affected by rights-management technologies may preserve and even increase consumers’ legal access to online digital content, it would be a mistake to rush in with legislative restraints on the development of this technology.\(^2\) The best strategy for lawmakers may be to adopt a wait-and-see strategy because other forms of regulation are likely to curb the potential excesses of rights-management containers.\(^3\) If the problems sketched here arise and are not controlled by other regulatory forces, then legislation should be drafted to restore the original balance of copyright, enabling creators to recoup the costs of production while also preserving public access to their works. However, because legislative intervention may chill the development of rights-management technologies and, with it, the progress of online information commerce, it should be resisted until the potential harms of such technologies are manifest.

E. Conclusion

This Part has explored the application of Calabresi and Melamed’s property rule paradigm to code solutions by examining three specific cyberspace problem areas: the accessibility of harmful material, the collection of personal information, and the unauthorized use of intellectual property. In each of these areas, I examined the current entitlement, the changes entailed by the code solution, and the reduction

\(^{1}\) Pornographic photographs and popular singles are common targets of online piracy. It is difficult to imagine a scenario in which a user could construct a successful fair use defense based on §107’s four factors to preserve free access to a Miss January photograph or to an Alanis Morissette song.

\(^{2}\) Potential legislative restraints include the mandatory inclusion of a fair rights regime or “copy duty” in rights-management technologies.

\(^{3}\) See Samuelson, supra note 114, at 191.
of transaction costs. In each case, the code solution resembled a property rule regime.

The preceding analysis may be read as suggesting that state regulation of the Internet is unnecessary given the ability of cyberspace architects to build code solutions to correct specific problems.\(^\text{127}\) Considering the recent flurry of state regulatory initiatives directed at the Internet,\(^\text{128}\) however, legislative restraint appears improbable. Thus, it may be useful to view this Part as recommending a method of regulation. Because property rules are optimal where, as in cyberspace, transaction costs are low, states should adopt Internet regulations that resemble property rule protections. Such protection can be built into the architecture of the Internet through code. States should therefore adopt regulatory solutions that incorporate, or at least resemble, code solutions.

V. THE DOMAIN NAME SYSTEM: A CASE STUDY OF THE SIGNIFICANCE OF NORMS TO INTERNET GOVERNANCE

A. Introduction

In recent years, scholars have debated whether the Internet is a unique environment that requires a new set of legal rules.\(^1\) Many believe that the Internet should be governed in a manner suited to its particular history, customs, and technological capabilities.\(^2\) The question that remains is how different Internet governance\(^3\) should be in order to accommodate the Internet's novel circumstances and adapt to explosive growth in users, commerce, and political stakeholders. This

---

\(^{127}\) In the words of Holmes: "[The state's] cumbrous and expensive machinery ought not to be set in motion unless some clear benefit is to be derived from disturbing the status quo. State interference is an evil, where it cannot be shown to be a good." OLIVER WENDELL HOLMES, JR., THE COMMON LAW 77 (Mark DeWolfe ed., 1963) (1881).


\(^1\) See, e.g., Lawrence Lessig, The Path of Cyberlaw, 104 YALE L.J. 1743, 1743 (1995) ("Is cyberspace really anything new? Is there really a form of life here that we haven't known before, or is cyberspace just an electronic version of ordinary space, where the electronics might add something, but not really very much?").


\(^3\) The term "Internet governance" has two meanings: the governance of people's behavior on the Internet and the governance of the Internet as a system. In this Part, the term is used in accordance with the latter meaning.
Part contends that Internet governance will be most successful when it encompasses the unique norms and customs that have evolved within the Internet, and expresses itself in familiar forms that are practical, understandable, and predictable for individual and commercial entities. New management regimes that embody well-developed Internet customs — such as open participation, consensus-building, and grassroots organization — will foster a common code of behavior for an increasingly diverse Internet, provide individuals with a stronger voice in a rapidly commercializing Internet, and create an environment that experienced Internet actors, who play key roles in the formation of new governance structures, know and trust.

This Part uses the controversy surrounding the overhaul of the domain name system (DNS) as a case study through which to analyze the value of traditional Internet norms to the future of Internet governance. Section B traces the evolution of Internet norms from the early history of the Internet through the development of the domain name system. Section C discusses the recent controversy surrounding the domain name system and the vital roles that Internet norms have played in that debate. Section D outlines the proposed solutions to domain name system problems, and section E illustrates the key functions that norms have served in the construction of a new regime of domain name governance. Finally, section F evaluates the effectiveness and future role of indigenous Internet norms against the model of norm-based governance described in Robert Ellickson’s seminal work, Order Without Law.4

The resolution of the domain name dispute exemplifies how diverse interest groups can come together to address an Internet-related governance issue. As the Internet crosses national borders, individual governments cannot properly manage the domain name system.5 Recently, the United States government and a worldwide community of Internet stakeholders united to form a nonprofit corporation to manage domain names and Internet addresses.6 This endeavor’s success depends upon the ability of reformers to cultivate the unique customs of past Internet users and policymakers, while embracing the new Internet stakeholders who are pressuring those very customs.

The above thesis faces a formidable objection: why will the norms developed by a small, cohesive Internet community influence today’s much larger and increasingly commercial and international Internet? The answer is threefold. First, although the former Internet stakeholders, many of whom have ties to academia and government, repre-

5 Sovereignty and jurisdictional issues on the Internet are more thoroughly discussed elsewhere in this Development. See infra Part VI.
6 See infra sections D, E.
sent only a small fraction of the new Internet interests, they created a culture of open participation, grassroots coordination, and consensus that will continue to influence Internet interactions for years to come. This phenomenon is not unique in our nation's history. The United States was founded by a small group of men who created a unique form of government and instilled in the citizenry a culture of distrust of monarchy, disdain for nobility, and faith in the power of the individual that has survived to the present day—despite the influx of diverse populations, the empowerment of women, and the rise of the United States as a world power. Second, the prevalence of these norms may benefit the Internet by fostering common customs among diverse users and augmenting the power of individuals in an increasingly commercial environment. Finally, seasoned Internet actors will play a disproportionately significant role in the implementation of a new domain name system, because they are the most organized, outspoken, and knowledgeable Internet stakeholders to date. Although the Internet touches the lives of almost one billion people, a small

---

7 See, e.g., Gerald E. Critoph, The American Quest for Affluence, in AMERICAN CHARACTER AND CULTURE IN A CHANGING WORLD 27, 27 (John A. Hague ed., 1979) (contending that Thomas Jefferson’s assertions in the Declaration of Independence “have continued to be considered by most Americans to be fundamental to the American Way of Life”); see also John D. Buenker, Mainstream America and the Immigrant Experience, in THE DEVELOPMENT OF AN AMERICAN CULTURE 312, 318 (Stanley Cohen & Lorman Ratner eds., 1983) (arguing that the “essentials of the Constitution, the Bill of Rights, and the Declaration of Independence have survived” and that this “political-legal-governmental complex provides a framework and a value system that a wide range of socioeconomic, geographical, and ethnoreligious groups rely upon to compromise their differences”).

8 See, e.g., E-mail 1 from Michael Roberts, Interim CEO of the Internet Corporation for Assigned Names and Numbers (ICANN), to author (Jan. 25, 1999) (on file with the Harvard Law School Library) (discussing the “politico-sociological players” who have had and will continue to have “a controlling voice” in the DNS area) [hereinafter E-mail 1]. Several ICANN board members have roots in the old-guard Internet community. For example, George Conrades worked for a company that built the ARPANet in 1969. See ICANN Public Meeting Transcript, Cambridge, Mass., Nov. 14, 1998, at 18–19 (transcript available at <http://cyberlaw.harvard.edu/icann/cambridge-ixg8larchive/transintro.html> (on file with the Harvard Law School Library) [hereinafter Meeting]. Michael Roberts was involved in “technology policy work” in Washington, D.C., for the university networking community, and Jun Murai, dubbed “Mr. Internet” in Japan, has worked with the Internet Engineering Task Force (IETF) for “quite some time.” E-mail 2 from Michael Roberts, Interim CEO of ICANN, to author (Jan. 25, 1999) (on file with the Harvard Law School Library). In addition, Dr. Jon Postel’s pivotal role in Internet management from 1969–1998 illustrates the power and longevity of experienced Internet players. See infra section B; see also Todd Spangler, Net’s Old Guard Shaping New DNS (last modified Feb. 23, 1998) <http://www.internetworld.com/print/1998/02/23/news/19980223-guard.html> (on file with the Harvard Law School Library) (reporting that many of the Internet’s “founding engineers” were working to formulate a plan for a new domain name management system). But see E-mail 1, supra (“[T]he influence of the old guard of the IETF . . . is waning both because of the scaling up factor and because of generational aging.”).

cadre of individuals assumes positions of power in most Internet-related forums, thereby magnifying the normative influence of this core group.

B. The History and Leadership of the Internet

The Internet developed a set of indigenous norms early in its history. The trust-based governance structure of the early Internet encouraged reliance on the norms of open participation, bottom-up coordination, and consensus-building. These customs helped to make the small group of academics who created and ran the Internet accountable to each other and to new users.

Until recently, the Internet was governed like a monarchy with gossamer ties to the United States government. Dr. Jon Postel was one of a small group of graduate students at the University of California that set up the first node of an experimental computer network in 1969 called the ARPANet. Over the next ten years, Postel helped to design the Internet Protocol (IP), a system of addresses that enabled computers on the ARPANet to communicate with those on a second network built by the National Science Foundation (NSF).

The invention of domain names followed. IP addresses are long strings of numbers that facilitate the sending of information from one network computer to another. To assist in remembering the addresses, Postel and his coworkers assigned each computer a name, which a file on each computer translated into numbers. By the early 1980s, updating the files on every computer in the network became unwieldy, and the "nicknames" were separated into groups called "domains." These "top-level" domains consisted of two types: national domains, such as ".us" for the United States or ".ca" for Canada; and generic domains, such as ".edu" or ".com." Separate computers administered each domain, and the "root server" directed traffic among domains.

---

10 See discussion supra note 8.
12 See Paulsen, supra note 11.
13 See id.
14 See id.
15 See id.
16 Id.
17 See id.
Postel ran this network almost single-handedly through an organization called the Internet Assigned Numbers Authority (IANA). He not only made administrative decisions for the Internet, but also assigned IP addresses and the correlating "domain names" and monitored the root servers. Reflecting the Internet norm of trust-based leadership, Postel succeeded in holding this system together by gaining the respect of what was then a small community of users; during his long tenure managing the Internet, Postel never appeared to make self-interested or foolish judgments. Postel’s minimalist administration was possible because the Internet had historically been a purely research-oriented network used by a manageable group of scientists, engineers, and government officials.

But such heavy reliance on one individual for executive decisions rendered the Internet governance system inherently unstable. Postel’s colleague, David Clark, asserted that the loss of Postel could devastate the Internet because his "personal stature" helped hold the domain name system together. This tenuous reliance on charismatic leadership illustrated the need for a more practical, structured, and lasting governance system for the Internet. The need became even more acute when Postel passed away unexpectedly in the fall of 1998, in the midst of efforts to institutionalize the responsibilities that he had previously managed alone.

Despite his central role, Postel never worked in a vacuum. Several nonprofit advisory boards, comprised mostly of Internet engineers, helped to define Internet policies. The Internet Society (ISOC), one of the main advisory bodies responsible for running the Internet, appointed the Internet Architecture Board (IAB) to help set Internet standards and allocate resources. The ISOC and its subsidiary bodies possessed no official power but governed through norms of consensus, open participation, and bottom-up management. Those within the ISOC, like Postel, believed that the organization maintained power...
by acting "rationally" and maintaining "competence and quality and respect." 27 In keeping with an informal, consensus-based style, the ISOC issued policy documents, called Requests for Comments (RFCs), which the rest of the Internet community typically adopted. 28 The many former ISOC and IAB members who continue to hold positions of power in the Internet arena will help to spread ingrained Internet customs throughout the larger body of users and commercial interests. 29

As businesses, universities, and individuals clamored for Internet access in the early 1990s, domain name management overwhelmed Postel and the IANA. 30 In 1992, Congress requested that the NSF outsource domain name management to the private sector. 31 The NSF awarded Network Solutions, Inc. (NSI) the task of constructing and managing an information center called "InterNIC," which would assign new domain names within the popular ".com," ".edu," and ".org" domains and operate the "A" root server with Postel's assistance. 32 As of September 30, 1998, NSI had registered a total of 2,777,000 domain names and reaped gross profits of $35.9 million. 33

C. Domain Name System Difficulties

As the Internet grew increasingly large and commercial, both business and individual users expressed dissatisfaction with the status of the domain name system. Many commercial interests that were "staking their future on the successful growth of the Internet" wanted a more "formal and robust management structure." 34 In a commercialized environment, it was becoming "less appropriate" for U.S. research agencies to govern and fund Internet functions. 35 In addition, as the Internet transcended national borders, international interests

27 Id.
28 See id. RFCs, which were accessible online, usually addressed new standards for different aspects of the Internet or simply provided explanation or information about a given topic. See id. Clark, a former member of several Internet governance organizations including the ISOC, summarized ISOC governance: "We reject kings, presidents, and voting. We believe in rough consensus and a running code." Id.
29 See discussion supra note 8.
30 See Paulsen, supra note 11.
31 See id.
32 See id. In 1995, Science Applications International Corporation (SAIC), a company with years of experience contracting with the government, purchased NSI. SAIC helped NSI negotiate a profitable deal with the government, which enabled NSI to charge $100 for each new domain name. See id.
35 Id.
called for a global, rather than a United States-centered, governance structure.\(^3\)

Moreover, leaving the domain name system in the hands of NSI proved to be an inequitable situation, because it offered users no alternative places in which to register and prevented new registrars from entering the lucrative domain name business. By the early part of the next century, burgeoning use of the Internet will create a surge of electronic commerce that could reach as high as \(\$300\) billion.\(^3\) The management of such an explosive industry could prove to be problematic for one firm. Furthermore, allowing NSI to retain monopolistic control of the lucrative business of domain name registration would be unusual in a capitalist economy.\(^3\)

Internet users have also had their gripes with NSI. Some users claim that NSI has a poor customer service record.\(^3\) In light of such problems, customers were displeased that they had no choice but to register with NSI if they wanted a domain name and the ability to reach customers through the Internet.\(^4\)

Considerable controversy has also arisen over the relationship between domain names and trademarks.\(^4\) Representatives from the business community continually assert that extensive trademark protection is necessary to promote "a stable commercial environment."\(^4\) Because domain names guide consumers to their desired locations on the Internet, companies doing business online have "a strong desire to acquire domain names that are easy to remember and that relate to their products, trade names or trademarks."\(^4\) Individuals who do not know the domain name of a company often try to "intuit" the name of the company's website by adding "\(\text{.com}\)" to the company's trademark.\(^4\)

\(^3\) See id.
\(^3\) See Hearing, supra note 9 (testimony of Anne Chasser).
\(^3\) Renewals of the existing registrations alone would generate \(\$670\) million per year in business. See Paulsen, supra note 11.
\(^3\) For example, users have complained that NSI's database of domain name holders' names, addresses, and telephone numbers, called "WhoIs," is of little help to customers as it is often incorrect or out of date. Moreover, companies and individuals often send NSI customers listed on the WhoIs database "a blizzard of direct mail and spam." Randy Barrett, "WhoIs" Net Database to be Released on CD (last modified Sept. 21, 1998) <http://www.zdnet.com/zdnn/st...dnn_sm graph_display/o,4436,2139578,00.htm> (on file with the Harvard Law School Library).
\(^4\) See id. Internet users also complained about the \(\$100\) fee charged by NSI to register domain names because IANA had performed this service for free. See Paulsen, supra note 11.
\(^4\) Hearing, supra note 9 (testimony of Anne Chasser).
\(^4\) Id.
\(^4\) See id.
NSI has attempted to distance itself from the trademark controversy. Prior to 1995, NSI asserted that the registration of a domain name did not establish trademark rights in the registered name and made it the domain name holder's responsibility to ensure that she was not infringing upon any trademark rights. Under its formal domain name dispute resolution policy, NSI registers domain names on a "first-come, first-served" basis and does not "evaluate [up front] whether that registration or use may infringe upon the rights of a third party." The policy also states that NSI may revoke, suspend, transfer, or modify a domain registration that is shown to interfere with a federally registered trademark. Furthermore, the policy recognizes orders from any court of competent jurisdiction to revoke a registration that interferes with a valid federal trademark.

NSI's treatment of trademarks has led to the problem of "cybersquatting." Speculators, recognizing the value of particular domain names, register those names in order to resell them at a substantial profit to the business normally associated with that name. Although cybersquatters are usually motivated by the high prices that businesses are sometimes willing to pay for a particular domain name, occasionally companies register a domain name akin to a competitor's trade name in order to attack the owner or product of the corresponding trademark.

Even absent malevolent intent, companies of-

---

46 In 1995, NSI issued its first formal policy on domain name dispute resolution. See id. The 1995 policy permitted third parties to "challenge the registration of a domain name" if the trademark owner presented NSI with evidence that the registered domain name violated the trademark owner's rights. Id. After several revisions, NSI published its current dispute resolution policy in 1998. See id. at 787-91.
47 Network Solutions' Domain Name Dispute Policy (last modified Feb. 25, 1998) <http://rs.internic.net/domain-info/nic-revo3.html> (on file with the Harvard Law School Library). The registrant must also agree to defend, indemnify, and hold harmless NSI in any dispute and to limit NSI's liability for damage awards above $500 dollars. See id.
48 See Albert, supra note 45, at 791.
50 For example, Compaq Computer purchased the rights to the domain name "www.altavista.com" for $3.35 million dollars. See Compaq Acquires "altavista.com" Domain Name, THE COMPUTER LAW., Sept. 1998, at 27.
51 For instance, Princeton Review registered the domain name "kaplan.com" and posted at that site negative comments about Kaplan Educational Center, Princeton Review's most significant competitor. See Hearing, supra note 9 (testimony of Anne Chasser).
ten experience conflict registering domain names when they share the same name or trademark with another firm.\textsuperscript{52}

In response to these problems, businesses have arisen to offer the domain name and dispute resolution services that NSI lacks. A company called NetNames will search more than two million registered domain names, as well as U.S. federal trademarks, to inform potential users whether existing names match or closely resemble the names they desire.\textsuperscript{53} NetNames has even created relationships with some of the "Web's biggest cybersquatters" and can negotiate with them on behalf of NetNames clients.\textsuperscript{54} Recognizing the demand for more comprehensive services, NSI recently allied with other Internet businesses to protect its market power.\textsuperscript{55}

\textbf{D. Proposed Solutions}

As NSI's contract with the government drew to a close in 1998, Internet interest groups attempted to create better alternatives to the domain name system. Reform efforts such as the International Ad Hoc Committee's (IAHC) Generic Top-Level Domain Name Space Memorandum of Understanding (gTLD-MoU) and the Clinton Administration's Green Paper and White Paper proposals are united by the common themes of open participation, bottom-up coordination, and consensus-building.

The first domain name reform idea originated with Postel, who advocated adding up to two hundred new generic top-level domains in order to dilute the importance of the "\.com" domain and to multiply the number of names available for registry.\textsuperscript{56} In the fall of 1996, the ISOC and IANA helped form the IAHC to develop a future plan for the domain name system "[t]he IAHC process was as open and available for public partici-\textsuperscript{57}

\begin{footnotesize}
\footnotesize\textsuperscript{52} See id.
\footnotesize\textsuperscript{53} See Nancy Weil, \textit{Excuse Me, Is This Domain Name Taken?} (last modified Aug. 7, 1998) <http://www.thestandard.net/articles/article_print/0,1454,1361,00.html> (on file with the Harvard Law School Library).
\footnotesize\textsuperscript{54} Id.
\footnotesize\textsuperscript{56} See Paulsen, \textit{supra} note II. The United States government also realizes the importance of increasing the number of domain names available for registry. In 1998, the U.S. Commerce Department began exploring ways to encourage use of the "\.us" domain name space. The "\.us" domain is the "country code" top-level domain assigned to the United States. All countries can choose to have their own "country code" domains. The "\.us" domain space is currently managed as a "locality based hierarchy in which second-level domain space is allocated to States and U.S. territories." \textit{Commerce Department Extends Comment Period for \textit{.US Domain Space} (last modified Aug. 25, 1998) <http://www.ntia.doc.gov/ntiahome/press/prusext.htm> (on file with the Harvard Law School Library).}
\footnotesize\textsuperscript{57} Paulsen, \textit{supra} note II.
\end{footnotesize}
pation as the organizers and participants knew how to make it.\textsuperscript{58} The IAHC process culminated in the May 1997 gTLD-MoU, which called for the establishment of seven new top-level domains — including "firm" for businesses, "shop" for stores, and "arts" for cultural activities — operated by a consortium of private domain name registrars.\textsuperscript{59}

Many DNS reform critics questioned the authority under which the gTLD-MoU recommendations were made.\textsuperscript{60} Critics also challenged the accountability of the new system, claiming that the proposals would tighten control of the Internet by IANA and the engineering community, thereby leaving a group of academics in charge of an increasingly commercial Internet.\textsuperscript{61} Finally, many critics doubted the wisdom of expanding the number of top-level domains on a seemingly random basis and called for a more thoughtful and organized expansion.\textsuperscript{62}

The Clinton Administration entered the domain name debate in January 1998.\textsuperscript{63} Although historically an invisible authority in the Internet area,\textsuperscript{64} the United States government recognized the need for a more "formal and robust management structure" for the domain name system and exercised its power as the founder of the Internet and signatory to the domain name contract with NSI.\textsuperscript{65} The government issued a "Green Paper," an initial draft of a plan for the domain name system.\textsuperscript{66} The Green Paper proposed a plan for transferring control of the domain name system from the federal government to the private sector.\textsuperscript{67} More specifically, it recommended the formation of a U.S.-based nonprofit corporation to run the domain name system.\textsuperscript{68} In addition, the plan included many of the gTLD-MoU recommendations, such as the immediate creation of new top-level domains and competing registries and registrars.\textsuperscript{69} The Green Paper met with much criticism because of the rush to create new domains and the absence of a policy to resolve trademark disputes.\textsuperscript{70} Others complained that the government, although claiming to relinquish Internet governance to

\textsuperscript{58} Id.
\textsuperscript{59} See Heather N. Mewes, Memorandum of Understanding of the Generic Top-Level Domain Name Space of the Internet Domain Name System, 13 BERKELEY TECH. L.J. 235, 238 (1998); Paulsen, supra note 11.
\textsuperscript{60} See Mewes, supra note 59, at 242; Paulsen, supra note 11.
\textsuperscript{61} See White Paper, supra note 34, at 31,743.
\textsuperscript{62} See Mewes, supra note 59, at 243.
\textsuperscript{63} See White Paper, supra note 34, at 31,743.
\textsuperscript{64} See Clark Interview, supra note 18.
\textsuperscript{66} See id. at 8826–33.
\textsuperscript{67} See id. at 8826.
\textsuperscript{68} See id. at 8827–28.
\textsuperscript{69} See id. at 8828–29.
\textsuperscript{70} See Hearing, supra note 9 (testimony of Anne Chasser).
the private sector, was actually extending its control by "dictat[ing] the details" of the new system. In addition, critics argued that the Green Paper did not adequately represent international interests.

Although many aspects of the Green Paper proposals changed during the revision process, the idea of transferring domain name control to a private nonprofit corporation remained. The government and Internet stakeholders chose a corporation rather than an international policymaking body, such as the International Telecommunications Union (ITU), to supervise domain names for three reasons. First, the allocation of governance powers to a private corporation follows the current movement toward privatization of government activities and industry self-regulation. Second, the corporate structure ostensibly allows for more efficient decisionmaking than a large, deliberative international organization. Third, a small body devoted to problems of names and addresses is better able to gain expertise in this technological area.

In response to public comments, the Clinton Administration released a revised DNS policy statement, the "White Paper." Unlike the Green Paper, which proposed a top-down solution to Internet problems, the White Paper reflected the established norms and customs of the Internet. Through the publication of the White Paper, the U.S. government codified these nebulous principles and contributed to the birth of a written history of Internet governance. For instance, the White Paper begins by outlining four guiding principles for the development of a new domain name system: stability, competition, private bottom-up coordination, and representation. The emphasis on stability might ease the transfer of management power from the American government to the private sector and prevent disruption of current operations.

Competition encourages innovation, flexibility, and con-

---


72 See id.


74 See White Paper, supra note 34, at 31,741.

75 See supra pp. 1666-67.

76 See White Paper, supra note 34, at 31,749.

77 See id.
sumer choice. The preservation of the Internet's grassroots style of organization reflects Internet community traditions and promotes flexibility. Finally, successful development of Internet policies depends on representative input from the geographically diverse Internet community. Although Internet use and commerce will expand, reliance on entrenched norms will promote efficiency by further ingraining the culture that has proved successful in Internet affairs.

Like its predecessor, the White Paper called for creation of a private nonprofit corporation to coordinate key Internet functions such as managing IP addresses and root servers, increasing the number of top-level domains, and setting protocol parameters. Although the company would be incorporated in the U.S. to ensure stability, the White Paper states that the company's board of directors and members should come from around the world. Most importantly, official government representation would not be permitted on the board of directors, but governments and intergovernmental organizations would be encouraged to participate in the corporation as Internet users or as nonvoting advisors. This framework assuages much of the fear that a particular government might have an undue influence on Internet affairs. Once the board of directors is in place, it would "develop policies for the addition of" new top-level domains and "establish the qualifications for domain name registries."

Reflecting the customs of the Internet community, the White Paper instructs that the organizing documents of the company should provide for governance on the basis of a "transparent decisionmaking process" in order to protect against "capture" by self-interested factions. The White Paper suggests that the corporation rely upon separate "councils" responsible for developing, reviewing, and recommending specific policies for the board's approval.

The White Paper's treatment of trademark issues won the approval of the International Trademark Association. First, the White Paper states that current and prospective trademark holders and domain name registrants should have access to searchable databases of registered domain names in order to provide contact information and to avoid potential conflicts. Second, the proposal recognizes trademark

---

78 See id.
79 See id.
80 See id.
81 See id.
82 See id. at 31,749-50.
83 See id. at 31,750.
84 Id.
85 Id.
86 See id.
87 See Hearing, supra note 9 (testimony of Anne Chasser).
88 See White Paper, supra note 34, at 31,750.
conflicts and cybersquatting as legitimate concerns and suggests modes of addressing such problems.89 Third, the White Paper asks the World Intellectual Property Organization (WIPO) to develop recommendations for a uniform approach to resolving trademark and domain name disputes in the future.90 Finally, the White Paper outlines the steps for an orderly transition to private sector control over the allocation of domain names. These steps mandate that the U.S. government wind down its agreement with NSI and ensure that NSI permits the development of competition in domain name registration, recognizes the role of the new corporation, and makes databases, software, and expertise available to the new corporation.91 In addition, the government must enter into an agreement with the new corporation regarding the transfer of responsibility for the management of domain name space92 and consult with the international community as it makes decisions pertaining to the transfer.93

Public response to the White Paper was generally positive94 due in part to the proposal’s respect for traditional Internet norms. Ira Magaziner, President Clinton’s Senior Advisor on Internet policy, credited the policy development process, including draft proposals, public comment periods, and communication among interest groups, for the White Paper’s acceptance.95 Others appreciated the government’s sensitive treatment of the Internet community’s comments96 and praised the Administration for delaying the addition of new domain names and other specific policy decisions until after the new corporation became operational.97 Even NSI, which was to lose its mo-

89 See id. at 31,750-51 ("Domain name registrants would agree, at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting ... they would submit to and be bound by alternative dispute resolution systems ... for the purpose of resolving those conflicts.").
90 See id. at 31,751.
91 See id.
92 See id.
93 See id.
94 There was “almost universal agreement” that the government should turn over its domain name authority to a nonprofit corporation and that NSI should face competition. Janet Kornblum, Magaziner: Domain Consensus Possible, CNET News (June 5, 1998) <http://www.news.com/News/Item/o,4,23879,00.html> (on file with the Harvard Law School Library) (quoting Ira Magaziner, Internet policy advisor to President Clinton) (internal quotation marks omitted).
97 See id. (reporting the statement of Jay Fenello, president of an Atlanta domain name registry).
ropolistic control over the registration of domain names, praised the White Paper.98

Others, such as Professor Lawrence Lessig, have questioned aspects of the White Paper. Lessig argues that delegating domain name management to a private agency raises weighty legal and constitutional issues.99 He asserts that the new corporation would be charged with regulating activity in "the most significant new jurisdiction we’ve known since the Louisiana Purchase," yet would be beyond constitutional review.100 Lessig views the nonprofit corporation as a government-substitute that is unaccountable to an electorate.101 For example, when government controls an activity, the general public can voice its opinion on different aspects of the activity by voting for legislators who support particular positions. In contrast, the public has no formal mechanism for influencing a private corporation’s actions. However, this problem can be addressed by using the Internet norms of open processes, consensus-building, and grassroots style management in formulating the corporation’s structures and practices. These customs render the corporation accountable to members of the interested public who make the effort to attend open meetings and to reply to posted Requests for Comments.

Concerns about efficiency and the need to take immediate action also animated the choice of a private governing body for domain name registration.102 In fact, Magaziner asserted that the White Paper’s recommendations were partly based on the need to act quickly in the face of an expiring contract with NSI.103 Corporations, unlike government agencies, are equipped to work rapidly and efficiently, a vital attribute in the fast-changing Internet arena.

In addition, the White Paper garnered crucial international support. Although the European Commission (EC) criticized the Green Paper for its U.S. bias,104 the revised proposals addressed its concerns

---

98 See John Borland, Registrars Applaud New Domain Name Policy (last modified June 5, 1998) <http://www.techweb.com/wire/story/TWB19980605S0013> (on file with the Harvard Law School Library). NSI had other reasons to support the White Paper. Its stock rose twenty percent on the day the White Paper was released, reflecting the benefits that NSI would likely receive from its role as an advisor to future registrars and its edge over competitors. See id.


102 See id.

103 See id.

about international representation on the board and in the membership of the new corporation.\textsuperscript{105} The EC emphasized Europe's increasing importance as a major segment of the Internet user population\textsuperscript{106} and welcomed the White Paper's conflict resolution policy as well as its promotion of global Internet directories.\textsuperscript{107}

Some dispute this version of the history of the domain name controversy. These observers view the White Paper process not as a bottom-up, consensus-driven exercise, but rather as a "sham" designed to shield "naked power politics."\textsuperscript{108} Moreover, some critics claim that throughout this process the government treated NSI unfairly by forcing it to turn over a large portion of its business and expertise to competitors.\textsuperscript{109} This debate highlights the Internet's lack of a "Federal Register" or official record of its governance activities. Internet stakeholders must strive to create a record from memory. Thus, encased in the struggle over governance is the contest to determine the true history of the Internet.

\subsection*{E. The Road to ICANN}

Once the White Paper was generally accepted, Internet stakeholders faced the task of preparing for privatization. In the bottom-up, consensus-building tradition of the Internet, a broad-based coal...
tion of Internet associations, including NSI and the ISOC, initiated a worldwide forum, the International Forum on the White Paper (IFWP), to discuss the various implementation issues left unresolved by the White Paper. In the summer of 1998, members of the IFWP, led by Ira Magaziner, traveled around the world holding open meetings in order to gain insight and support for the new corporation.

Much like the founding fathers, these individuals sought to design a new structure of governance from scratch. Because of the global, technological, and changeable nature of the Internet, traditional forms of corporate governance were less likely to succeed. Thus, the IFWP sponsored something akin to a series of traveling constitutional conventions in order to make the experiment work as well as possible. The IFWP held meetings in Virginia, Geneva, Singapore, and Argentina. Outstanding issues discussed included: formation of the corporation, board and membership composition, development of a new domain name registry and dispute resolution system, and Internet infrastructure security and privacy issues. In Geneva, a consensus emerged that distinguished individuals should govern the new corporation, and interest groups should participate in councils addressing specific issues. Internet stakeholders encouraged regional meeting participants to continue discussions online, in keeping with the historical style of Internet deliberation. Similarly, Tamar Frankel, law professor and moderator of the Virginia conference, noted that Internet groups were "beginning to build a real trust and dependence on each other."

By the end of the summer, the Internet engineering, commercial, and user communities had essentially agreed on the structure of the

\[^{111}\text{See id.}\]
\[^{112}\text{See infra Part VI, section A.}\]
\[^{113}\text{See Mary Mosquera, Internet Groups Build Unity, Lay Down Swords (last modified July 3, 1998) <http://www.techweb.com/wire/story/TWB19980703S003> (on file with the Harvard Law School Library) (describing the meetings as the "Internet groups concluded the U.S. leg of their constitutional convention").}\]
\[^{115}\text{See IFWP, supra note 110; Mosquera, supra note 113.}\]
\[^{117}\text{See Mosquera, supra note 113.}\]
\[^{118}\text{Id. (quoting Tamar Frankel) (internal quotation marks omitted).}\]
new corporation for domain name management. Although many supported the proposal, others worried that the structure left too much power in the hands of Postel and the IANA.

With a few additions, NSI agreed to the IANA proposal in mid-September of 1998. The new corporation would be called the Internet Corporation for Assigned Names and Numbers (ICANN). Under the proposal, Postel and his advisers would nominate an interim board of directors to organize the corporation and elect permanent directors. In order to smooth the transition, the U.S. government extended its contract with NSI to September 2000, under the condition that NSI would begin to develop a system to support new registrars, create a searchable domain name database, and provide technical assistance to the inexperienced corporation.

ICANN’s structure reveals its foundation in the Internet’s established norms and customs. Its bylaws begin by emphasizing that the corporation shall operate in “an open and transparent manner” in order to “ensure fairness.” Specifically, ICANN intends to post its policies and decisions on its website and encourages input from interested parties. ICANN’s disclosure policy reflects the customary open atmosphere of Internet interactions. The initial board of directors will be replaced by a permanent board of directors, chosen through an open and deliberative process, no later than September 30,

119 See The Network Is the Story: News on the Latest Internet Standards and Struggles (last modified Aug. 25, 1998) <http://www.sunworld.com/sunworldonline/swol-08-1998/swol-08-idf.html> (on file with the Harvard Law School Library) [hereinafter Network]. The new corporation would be a nonprofit California-based organization; it would be managed by a board of directors to be chosen by an initial nine-member board of directors; board membership would be closed to government officials; no more than half of the members of the board would be from one geographic region; and “Supporting Organizations,” representing “Protocols,” “Addresses,” and “Names,” would nominate board members and fund part of the new organization. See id.; see also Janet Kornblum, Domain Name Accord a Step Closer, CNET NEWS (Aug. 25, 1998) <http://www.news.com/News/Item/0,4,25678,00.html> (on file with the Harvard Law School Library).

122 See id.


122 See id.

123 See id.

124 See id.


126 The final version of ICANN’s bylaws was completed on November 6, 1998. See Bylaws for Internet Corporation for Assigned Names and Numbers (Nov. 6, 1998) <http://cyber.law.harvard.edu/icann/bylaws.html> (on file with the Harvard Law School Library).

127 Id.

128 See id.
2000.129 The permanent board of directors will be composed partly of at-large members and partly of members selected by the three Supporting Organizations, which represent address, domain name, and protocol interests.130 The source of ICANN’s funding is still an open question.131

The continuing importance of the Internet norms of openness, consensus, trust, and legitimacy resurfaced when ICANN convened for its first public meeting on November 14, 1998.132 Of all the tasks facing ICANN, interim board member133 Esther Dyson emphasized the need to create a “culture.”134 Like the early United States, ICANN will best achieve success and unity by instilling an established body of norms in newcomers. In her opening statements at ICANN’s public meeting, Dyson outlined the corporation’s goals for the day — goals that reflect ICANN’s commitment to continuing the spirit of open communication indigenous to the Internet — including the desire to “collect input,” “talk,” “hear,” answer questions, and get to “know one another as individuals.”135 Dyson noted that ICANN would have to “get its legitimacy” from people using and learning to trust it, as did the original IANA and the former domain name management system.136 Moreover, Dyson contended that the best way to achieve legitimacy was to

129 See id.
130 See id.
131 In early September 1998, the Global Internet Project (GIP), a group of technology companies led by IBM and MCI, began a pledge drive to raise $500,000 of start-up money for ICANN. Members of GIP claim that they are not interested in influencing Internet policy, but only in advancing the launch of the new company. See John Borland, Pledge Drive For New Domain System Kicks Off (last modified Sept. 9, 1998) <http://www.techweb.com/wire/story/donnam/TWB1998o909S0017> (on file with the Harvard Law School Library); Business Seeks Funds for New Names Body, INTERNET MAGAZINE (Sept. 9, 1998) <http://www.Internet-magazine.co.uk/news/sept/o9a.htm> (on file with the Harvard Law School Library); Paul Festa, Raising Funds for Net Names Body, CNET NEWS (Sept. 9, 1998) <http://www.news.com/NewslItem/o,4,25,26132,00.html> (on file with the Harvard Law School Library).
132 The meeting focused on three major concerns: representation, supporting organizations, and transparency. See Meeting, supra note 8, at 90–155.
133 In addition to Dyson, the interim ICANN board includes: interim ICANN CEO and computing, networking, and telecommunications expert, Michael Roberts; Hans Kraaijenbrink, chairman of the European Telecommunications Network Operators Association; Eugenio Triana, a European telecommunications consultant; Greg Crew, an Australian Internet expert; George Conrades, an American venture capitalist; Frank Fitzsimmons, Vice President of Dun and Bradstreet; Linda Wilson, president of Radcliffe College; Geraldine Capdeboscq, Executive Vice President for Strategy, Technology and Partnerships, BULL France; and Jun Mural, Professor of Environmental Information, Keio University, Japan. See Meeting, supra note 8, at 13–35; Interim Board Members (visited Apr. 19, 1999) <http://www.icann.org/board.html#capdebosq> (on file with the Harvard Law School Library).
135 Meeting, supra note 8, at 5–6 (quoting Esther Dyson) (internal quotation marks omitted).
136 Id. at 9.
attain "a bottom-up consensus."\(^{137}\) She spoke of using the input from public meetings to build something "organic, that has within it learning mechanisms" and "feedback loops."\(^{138}\)

In contrast to the often charismatic, consensus-based norms of the Internet, however, ICANN requires a practical and independent structure that will outlive its current leadership. In James Madison's terms, ICANN needs to build a governance structure that will endure even when those in power are not "angels."\(^{139}\) Dyson asserted: "[W]e have to create something that will not be based on our own personalities, but that will have within it the checks and balances, responsiveness, the decision-making mechanisms that will enable it to work effectively after we are gone."\(^{140}\) A corporate entity such as ICANN introduces the danger of "ad-hocracy," in which individuals come together and create a system tied to their own talents that evaporates when they leave.\(^{141}\) Dyson claimed that the board was striving to establish practical organizational structures in order "to get to the point where . . . we can open up a transparent cocoon and let a butterfly out and all of [the interim board] disappear."\(^{142}\)

The public had its own concerns at the meeting, expressing the desire that ICANN's culture mirror well-developed Internet norms.\(^{143}\) Although ICANN will be a powerful corporation embarking on a worldwide mission, myriad comments emphasized the need for ICANN, its board members, and its decisionmaking process to gain the trust of Internet stakeholders and individual users;\(^{144}\) the desire to achieve public consensus regarding ICANN's goals;\(^{145}\) the quest to establish the appropriate authority for the creation of ICANN and accountability for its actions;\(^{146}\) and the importance of providing public

\(^{137}\) Id. at ii.

\(^{138}\) Id.

\(^{139}\) See THE FEDERALIST NO. 51, at 262 (James Madison) (Buccaneer Books, Inc. 1992) ("If men were angels, no government would be necessary.").

\(^{140}\) Meeting, supra note 8, at 12 (quoting Esther Dyson) (internal quotation marks omitted).


\(^{142}\) Meeting, supra note 8, at 38. The meeting also addressed the importance of the transparency of ICANN's procedures, see id. at 213-50, and the need to balance openness with efficiency, see id. at 215. Linda Wilson stated, "My biggest concern . . . is how to be extremely open and still function in a timely way . . . ." Id.

\(^{143}\) See, e.g., id. at 248 (statement of Ronda Hauben) ("It's not decisions by you [the ICANN board of directors], but . . . your participation in our community that is the only thing that will make you trustworthy.").

\(^{144}\) See, e.g., id. at 47 (statement of Jay Fanello of Microdome) ("It's also apparent that we do not trust this Board, nor this process.").

\(^{145}\) See, e.g., id. at 191 (statement of Don Telage of NSI) ("This is not a governance body, this is a body that gets its legitimacy from a strong consensus from the people.").

\(^{146}\) See, e.g., id. at 51 (statement of Michael Sondow) ("Where does the authority spring for this organization? Who do you [board members] represent? Why were you chosen?").

\(^{147}\) See, e.g., id. at 63 (statement of Dan Steinberg) (asserting that the Internet community needs the power to oversee the board and to make it fiscally accountable).
notice and comment on any ICANN activity. This list demonstrates that in order to achieve a consensus, ICANN needs to embrace the established norms of the Internet.

F. The Importance of Norms: How to Make ICANN as Successful as Possible

The scholarship of social norms illuminates the domain name controversy by helping to account for Internet customs such as bottom-up, consensus-driven, trust-based governance. In his pivotal work Order Without Law, Robert Ellickson proposes a theory designed to illustrate the contexts in which social norms emerge to create order in the absence of official rules. Ellickson asserts that members of “close-knit” communities develop and abide by norms aimed to “maximize the aggregate welfare that members obtain” in their everyday interactions with one another.

Some additional explanation helps clarify Ellickson’s thesis. First, “welfare maximization” denotes an increase in the “shareable welfare” of the community as a whole. In other words, enlarging the overall size of the proverbial pie provides everyone with a proportionately larger piece. Second, Ellickson claims that a community is “close-knit” when its members possess the informal power to sanction one another and have ready access to information about the internal events of the community. Ellickson notes that a “close-knit” community does not necessarily mean a small community. Finally, Ellickson maintains that norms represent “everyday behaviors” that call for informal “rewards and punishments.”

Ellickson concludes that in nonhierarchical communities, norms often create efficient rules, which address problems directly and generate few transaction costs. For example, in the late nineteenth century, New England whaling communities developed the custom, to

---

148 See, e.g., id. at 146 (statement of Michael Roberts) (“[ICANN is] obliged by the by-laws . . . to provide notice and comment . . . for anything we do.”).

149 More recently, the Berkman Center for Internet & Society at Harvard Law School convened a workshop on ICANN membership issues. See Workshop on Membership Issues for ICANN (Jan. 23, 1999) <http://cyber.law.harvard.edu/rcs/meeting.html> (on file with the Harvard Law School Library).

150 See ELLICKSON, supra note 4, at 123. Ellickson based his findings on his study of a community of ranchers in Shasta County, California. See id. at 167.

151 Id. But see Robert D. Cooter, Against Legal Centrism, 81 CAL. L. REV. 417, 426 (1993) (arguing that Ellickson’s thesis breaks down when the stakes of a conflict increase and when power is unequally distributed).

152 ELLICKSON, supra note 4, at 170.

153 See id. at 177–78, 181.

154 See id. at 182.

155 Id. at 184.

156 See id. at 192 (citing Herman Melville’s description of the efficacy of community norms on whaling expeditions).
which the courts deferred, of splitting a beached whale between its killer and the person who found it on the shore.\textsuperscript{157} Ellickson argues that legal rules are often most efficient when they mirror established custom.\textsuperscript{158} However, as "social distance" between group members increases, stakes in a conflict enlarge, and outside interests become important, formal legal controls often prove more effective.\textsuperscript{159}

Other scholars have expanded on Ellickson's theory, making it more applicable to the Internet context. For example, Robert Cooter claims that social norms signify a decentralized form of social control that is of interest not only in the context of lawmaking, but also in the realm of governance.\textsuperscript{160} Like Ellickson, Cooter believes that lawmakers, as well as managers, can enhance efficiency by "enacting custom."\textsuperscript{161} He provides the example of English medieval merchants who developed industry-specific rules and courts.\textsuperscript{162} When official judges gained jurisdiction over such issues, they did not possess sufficient knowledge about the merchant business to impose new rules. Instead, the judges discovered and enforced existing merchant customs.\textsuperscript{163} Cooter states that when lawmakers are pulled into particular business communities to impose legal rules or organizational structures, they should defer to the industries' customs in order to produce the most efficient outcome.\textsuperscript{164} In the context of governance, adherence to existing norms may also create a sense of familiarity that will help seasoned players, who often hold key positions in the Internet arena, work together in a congenial manner.

The question remains whether the Internet fits the model developed by Ellickson and his colleagues. Despite the high stakes of the domain name controversy, the power of commercial interests, and the dramatic increase in the number of users, in some ways it does. First, Internet technology facilitates the rapid dissemination of information, enabling a large number of people to become familiar with a given set of norms.\textsuperscript{165} Second, the Internet has been and continues to be informally guided by standards committees such as the ISOC and the IAB.\textsuperscript{166} Finally, the Green Paper, the White Paper, the IFWP, and the

\textsuperscript{157} \textit{See id. at} 202 (citing Ghen v. Rich, 8 F. 159, 162 (D. Mass. 1881)).
\textsuperscript{158} \textit{See id. at} 254.
\textsuperscript{159} \textit{Id. at} 283–84.
\textsuperscript{160} \textit{See Cooter, supra note} 151, at 418.
\textsuperscript{162} \textit{See id.}
\textsuperscript{163} \textit{See id. at} 445–46.
\textsuperscript{164} \textit{See id. at} 446.
\textsuperscript{165} \textit{See Henry H. Perritt, Jr., Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?}, 12 BERKELEY TECHNOL. L.J. 413, 420 (1997) ("Proposals for new rules can be published almost instantly to members of the electronic communities, and they or their representatives can debate the desirability of the proposed rules without having to assemble physically.").
\textsuperscript{166} \textit{See supra} pp. 1661–62.
ICANN public meeting demonstrate a continuing commitment to the custom of open processes developed on the Internet. In each of these instances, interested parties had the opportunity to attend open meetings, answer Requests for Comments, ask for notice and comment periods, and strive for legitimacy and trust.

In some ways, however, today's Internet is different from the communities that Ellickson describes. Richard McAdams argues that norms arise "because people seek the esteem of others" and are thus quick to conform to community standards. Norms of behavior arose in the Internet community because of its close ties, internal self-awareness, and ability to disseminate information rapidly. However, these norms may not survive the current influx of users and commerce. In addition, Ellickson's model applies to everyday interactions, and the institution of a new form of governance for the domain name system may not be an "everyday" occurrence. Nevertheless, ICANN is being established to address domain name assignment, which is practically an "everyday" activity.

Other aspects of the Internet illustrate the viability of norms in governance. "Netiquette," generally accepted rules of appropriate behavior on the Internet, prevails in both popular communities such as newsgroups and the less common multi-user domains (MUDs). In addition, individual online communities often post informal social norms in the form of Frequently Asked Questions (FAQs) in order to familiarize newcomers with the behavior acceptable to that community. Newsgroup and MUD system operators (sysops) possess the power, sanctioned by their communities, to expel individuals from the group for breaking customary rules. For example, users have been punished for sending large quantities of unsolicited mailings ("spam-

---

167 See supra sections D, E.
168 See id.
170 See Jonathan Zittrain, The Rise and Fall of Sysopdom, 10 Harv. J.L. & Tech. 495, 500-01 (1997) (asserting that Internet newsgroup community norms are drowned out by "restless mobs" of new users).
171 See supra p. 1677.
172 See supra section E.
173 For a more thorough discussion of the social and political dynamics of Internet communities, see discussion above in Part II.B.
174 See Valauskas, supra note 2 (citing Netiquette rules such as: "every member of every Internet community works to preserve the Internet, to do nothing that in any way would harm the Internet functionally ... Text is everything ... so take care in communicating with others in this environment.").
176 See Gibbons, supra note 24, at 493-94.
DEVELOPMENTS — THE LAW OF CYBERSPACE

The Internet even has the equivalent of self-appointed policemen and policymakers. These individuals develop programs called "cancelbots" that delete offending messages. In addition, the Guardian Angels, a volunteer organization created to protect neighborhoods from crime, has begun patrolling the Internet with "CyberAngels," individuals who search out and report vulgar material. Richard McAdams notes that when disinterested third parties begin enforcing community norms without recompense, it marks the customs' full development and power.

Community efforts in the adjudication of online disputes are emerging through mechanisms such as the Virtual Magistrate, which strives to settle disagreements online with Internet-savvy arbitrators. Although the importance of insular, norm-based Internet communities has declined as the Internet has expanded in user numbers, financial importance, and technological capability, their legacy has informed the behavior of many players in the domain name controversy.

Even though some of the Internet's norm-based features, such as FAQs and RFCs, developed when the Internet was still a small, academically-oriented body, they have much to teach today's burgeoning and increasingly commercial Internet. These norms will provide a common code of behavior to unify diverse Internet users. Furthermore, the customs of open participation, consensus, and bottom-up coordination may offer individuals a stronger voice in an ever-commercializing Internet. Because seasoned Internet stakeholders are

---

177 For example, when two individuals sent six thousand Usenet groups an advertisement for their legal services in 1994, tens of thousands of Internet users protested by sending return e-mails and crashing the offenders' computers at least fifteen times. In addition, Internet Direct canceled the offenders' account. See Valauskas, supra note 2.

178 See Dibbell, supra note 175, at 36 (describing how the "wizard," or sysop, of a MUD expelled an individual from its community for committing "virtual rape" against another community member); see also supra p. 1592.

179 See Perritt, supra note 165, at 442 (citing "Cancelmoose" as an example of a "deputy sheriff" in a newsgroup who acted on community norms by canceling offending messages).

180 See Lance Rose, CyberAngels Flap Their Wings (last modified Feb. 1996) <http://boardwatch.Internet.com/mag/96/feb/bwM27.html> (on file with the Harvard Law School Library). Rose also contends that CyberAngels threaten constitutional free speech protections by using their own judgment in deeming certain materials offensive. See id.

181 See McAdams, supra note 169, at 372–73.

182 See David J. Loundy, Virtual Magistrate Becomes a Reality, Sort of, CHI. DAILY L. BULL., June 13, 1996, at 5; The Virtual Magistrate Project, Virtual Magistrate Issues its First Decision (last modified May 21, 1996) <http://www.jmls.edu/cyber/docs/vn1.html> (on file with the Harvard Law School Library); see also Robert C. Bordone, Electronic Online Dispute Resolution: A Systems Approach — Potential, Problems, and a Proposal, 3 HARV. NEGOTIATION L. REV. 175, 178 (1998) ("Customs, norms, and rules that differ from those we experience in the 'real' world have developed within these virtual communities. These differences must be recognized and taken into account if an effective model of dispute resolution is to be created and implemented for Cyberspace.").

183 See Zittrain, supra note 170, at 500.
playing key roles in the leadership of the current Internet, their established norms and customs will likely exert a significant influence over Internet governance and may help to make the new Internet a respectful and inclusive place to learn and work.

G. Conclusion

As a new form of governance emerges in the area of Internet domain names and addresses, policymakers should embrace the unique norms and customs that have grown up with the Internet. Although cyberspace is no longer populated by a small group of like-minded individuals, traditions of openness, consensus, trust, and legitimacy still pervade the thoughts and actions of many Internet stakeholders and can help to unify a variety of Internet interests. These norms may percolate through the increasing ranks of Internet users and businesses, as individuals steeped in Internet custom hold positions of power in the new governance structures and thus exert a disproportionate influence on the thoughts and actions of the larger community. As the White Paper illustrates, the U.S. government has helped to crystallize Internet customs and begin the task of recording an Internet history. Storytelling solidifies norms. Thus, the cataloguers of the Internet's history will have a measure of control over the norm-building process. The steps leading to the creation of ICANN illustrate a continuing commitment to the values of openness, trust, and grassroots coordination and portend that, even in the face of an expanding and commercializing Internet, governance structures that respect indigenous norms and customs will prove most successful. However, the explosive growth and commercial importance of the Internet demonstrate that established norms should be balanced against the vital need to construct a practical governance system that will outlast the character and charisma of individual leaders and ensure stable and positive relationships with powerful Internet businesses.

VI. CYBERSPACE REGULATION AND THE DISCOURSE OF STATE SOVEREIGNTY

This Part focuses on a foundational principle of contemporary debates about Internet regulation — the sovereign state. The seemingly borderless, transnational scope of Internet communications has made state sovereignty a common theme in commentaries discussing the propriety of Internet regulation. Often, state sovereignty concerns have prompted regulatory initiatives. China, for instance, has sought
to insulate itself from western websites to protect its informational sovereignty. Similarly, the United States has relied on the preservation of state sovereignty as a rationale for regulating exports of encryption technology and for promoting national regulation of Internet gambling. Appeals to state sovereignty, however, have also been made to justify restricting Internet regulation. For example, commentators and governments frequently claim that regulation of Internet activities that originate in another state is an illegitimate encroachment on that state's sovereignty. More radical opponents of Internet regulation have seized upon this idea, arguing that cyberspace constitutes its own "state" over which territorial governments have no sovereign authority to enact regulations. For other commentators, the transnational scope of the Internet has contributed to the dispersion of "sovereign" authority away from the state, making Internet regulations both ineffectual and illegitimate.

In each of these instances, the concept of state sovereignty provides a stable, yet emotive, reference point for defining the scope of legitimate government authority. For many commentators and officials, a state either can assert sovereignty over Internet activities or it cannot; either a state acts to protect its sovereignty or it loses it. The concept of sovereignty, however, is seldom analyzed. This Part provides such an analysis of the concept as it is used in the regulatory debate and argues that assessments about the legitimacy of Internet regulation differ, in part, because of ambiguities inherent in the concept of sovereignty.

---


3 See 143 CONG. REC. S6724-25 (daily ed. June 27, 1997) (statement of Rep. Burns) (arguing that without encryption technology regulations, "our national security and sovereignty will surely be threatened").

4 See infra pp. 1687-88.

5 See, e.g., American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 177 (S.D.N.Y. 1997) (holding that a New York law that criminalized the dissemination of obscene materials to minors unconstitutionally encroached "upon the sovereignty of New York's sister states [and was] per se violative of the Commerce Clause").

6 John Perry Barlow, co-founder of the Electronic Frontier Foundation (EFF), made the seminal statement to this effect:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.


7 See infra p. 1689-90.
To the extent that Internet regulations demand an evaluation of a state's legitimate authority, this Part concludes that an alternative understanding of the state is required.

Drawing on international relations theory, the assumptions of individuals engaged in the Internet regulatory debate, and popular perceptions about the changing role of the state, section A distills three conceptions of sovereignty that have informed discussions about Internet regulation. These positive conceptions of sovereignty function primarily to assess when state sovereignty exists, but supporters and opponents of Internet regulation have also applied them normatively to determine whether a state regulates legitimately. Because of the malleability of the assumptions underlying each conception, however, arguments about Internet regulation that rest on a normative approach to state sovereignty prove indeterminate or contradictory.

In an effort to avoid the problems caused by reliance on traditional notions of state sovereignty, section B advocates adopting a liberal-constructivist approach to domestic politics to examine government regulation of the Internet. This approach shifts the analysis of Internet regulation away from generalized discussions about the "state" and toward a focused consideration of the manner in which government regulation "constructs" collective identity and allocates power among competing normative perspectives in a jurisdiction. Section B concludes that adopting a liberal-constructivist framework forces judges and policymakers to confront the implications of Internet regulation for domestic social relations and community identity.

Finally, section C examines how the liberal-constructivist paradigm can inform a contemporary area of debate about the proper relationship between government authority and cyberspace: personal jurisdiction in Internet-related cases. Courts' current confusion about the exercise of jurisdiction over nonresident website operators stems largely from indeterminate conceptions of sovereignty embedded in traditional personal jurisdiction doctrine. Adopting a liberal-constructivist framework avoids the ambiguity of these concepts and enables a more thorough assessment of the implications of exercising jurisdiction in particular cases. To the extent that courts' determinations of jurisdiction over website activities would differ, such differences would result from specific policy considerations rather than the formalistic application of an indeterminate doctrine.

A. The "Sovereign" Discourse

An examination of the Internet regulatory debate reveals three positive conceptions of state sovereignty: the realist, the representational, and the postmodern. Each conception flows from a different set of assumptions about the nature of the state system, with each set of assumptions reflecting academic and popular attitudes toward the
role of the modern state. This section shows how commentators and governments frequently apply these concepts normatively to assess the legitimacy of Internet regulations. In the process, however, they subject their arguments to the indeterminacies of the assumptions that underlie each conception.

1. The Realist Conception. — The realist conception of sovereignty stems from the realist theory of international politics. Two fundamental assumptions of the realist theory are that states are the primary actors in the international system and that they act rationally to maximize their power. A state’s territorial boundaries fulfill a crucial role in this theory by circumscribing the extent of state power. For realist international lawyers, control over a defined territory is “the first criterion of statehood, an indispensable prerequisite for participation in the international system.” According to this theory, states are “sovereign” to the extent that they are the supreme authority within a given territory. When applied normatively, the realist conception asserts that a “sovereign” state possesses sole jurisdiction over its citizens and internal affairs. Any restriction of its exclusive jurisdiction within its own territory appears as an illegitimate “diminution of its sovereignty to the extent of the restriction.”

States seeking to regulate the Internet usually rely on realist assumptions. These assumptions inform two of the most common principles for asserting jurisdiction: the territoriality principle and the effects principle. Under the territoriality principle, a state has authority to regulate the transmittal of information across its borders and the use of that information by individuals within its territory. This principle underlies China’s regulatory initiative to prevent “detrimental information” from entering its territory via the Internet. Further, states rely on the territoriality principle to regulate in-state hardware and software used in Internet communications. For example, Bavaria used this aspect of the principle to enforce its antipornog-

8 See Paul R. Viotti & Mark V. Kauppi, International Relations Theory: Realism, Pluralism, Globalism 35 (2d ed. 1993).
9 Id. at 723–24.
12 See Stephan Wilske & Teresa Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet?, 50 FED. COMM. L.J. 117, 129–42 (1997). The territoriality principle grants a state jurisdiction to prescribe law with respect to “conduct that, wholly or in substantial part, takes place within its territory.” Restatement (Third) of Foreign Relations Law § 402(1)(a) (1987). The effects principle grants a state jurisdiction to regulate “conduct outside its territory that has or is intended to have substantial effect within its territory.” Id. § 402(1)(b).
14 Lewis, supra note 2, at 471.
15 See Goldsmith, supra note 13, at 482.
raphy laws against CompuServe's Munich office after the service provider refused to shut down over two hundred Usenet newsgroups that contained pornographic content.\(^\text{16}\)

States rely on the effects principle in applying their domestic laws to out-of-state Internet activity. For example, the Minnesota Attorney General has asserted jurisdiction over nonresident individuals who use the Internet to "cause a result to occur in Minnesota."\(^\text{17}\) The Attorney General's peremptory assertion of jurisdiction is emblematic of the realist view of regulatory power: because control over territory assumes the legitimacy of state actions taken inside that territory, states need not explicate the basis for their jurisdictional assertions.

Despite government reliance on realist logic, the realist concept of sovereignty fails to provide a normative basis for Internet regulation. Indeed, the realist conception supports many of the arguments against government regulation of the Internet. During debates about the Internet Tax Freedom Act,\(^\text{18}\) state and local governments frequently argued that the Act was illegitimate because it infringed on their sovereignty over commercial transactions occurring within their jurisdictions.\(^\text{19}\) Similarly, government officials have relied on realist assumptions to restrict the application of domestic laws to Internet activities out of respect for states' jurisdictional limits.\(^\text{20}\)

Not surprisingly, much of the scholarship advocating Internet self-regulation also relies on realist logic. In their ground-breaking article on cyberspace self-governance,\(^\text{21}\) David Johnson and David Post employ realist assumptions to reveal the illegitimacy of territorial regulation of the Internet. They begin by articulating the realist premise that geography-based laws "make sense" when a government has "[c]ontrol over physical space, and the people and things located in that space"\(^\text{22}\) and when actions have a primary effect on persons and things within a


\(^{19}\) See Bill Pietrucha, *Battle Lines Form on Tax Freedom Act*, NEWSBYTES NEWS NETWORK, Feb. 2, 1998, available in 1998 WL 5029262 (quoting a city council member who declared the Internet Tax Freedom Act to be "a significant infringement on state and local sovereignty").

\(^{20}\) See infra p. 1696.


\(^{22}\) Id. at 1369.
single jurisdiction.23 The Internet, however, undermines this system because electronic activity occurs across multiple jurisdictional boundaries and in a form that governments are incapable of effectively controlling.24 Johnson and Post note that the assertion of jurisdiction by the U.S. over Internet-based activities only lays the foundation for an argument that "any other sovereign can regulate the activities of U.S. companies operating in Cyberspace from a location physically within the United States."25 Moreover, the effects of online activities are not tied to geographic locations; rather, they exist "everywhere, nowhere in particular, and only on the Net."26 Consequently, "no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws."27

Johnson and Post also illustrate the manner in which advocates of Internet self-regulation rely on realist assumptions to assert the legitimacy of deferring to cyberspace as an independent jurisdiction. Consistent with the realist conception, they use the traditional characteristics of a territorial state to describe cyberspace. A "legally significant border" exists between "Cyberspace" and the "real world" that is "just as distinct as the physical boundaries between our territorial governments — perhaps more so."28 Within this space, "responsible law-making institutions"29 have arisen to control online behavior: system operators (sysops) condition access on users' respecting defined rules of behavior,30 communities of "Cyberspace citizens" informally proscribe conduct,31 and online dispute resolution mechanisms address larger disputes.32 Their realist focus on territorial control therefore leads

23 See id.
24 See id. at 1370–74 ("Because the Net is engineered to work on the basis of 'logical,' not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together."); see also James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 66 U. Cin. L. Rev. 177, 178–83 (1997) (summarizing the argument that "the technology of the medium, the geographical distribution of its users, and the nature of its content all make the Internet specially resistant to state regulation.").
25 Johnson & Post, supra note 21, at 1374.
26 Id. at 1375.
27 Id. at 1376.
28 Id. at 1379; see Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 EMORY L.J. 911, 917–19 (1996) (asserting that the Internet's infrastructure creates "visible borders" that replace national borders in regulating online interactions).
29 Johnson & Post, supra note 21, at 1390; see Henry H. Perritt, Jr., Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?, 12 BERKELEY TECH. L.J. 413, 414 (1997) ("[Cyberspace] may be distinct enough to have its own law and legal institutions — a system of 'cybergovernment.'").
30 See Johnson & Post, supra note 21, at 1388.
31 Id.; see supra p. 1678–79 (examining the manner in which Internet norms regulate online conduct).
32 See id. at 1389; see also Reidenberg, supra note 28, at 917 (noting that the abilities of network communities to define and enforce rules of citizenship and behavior represent "distinct sov-
them to conclude that states "should defer to this new form of self-
government." 33

Thus, Johnson and Post attempt to flip the realist justification for
regulatory authority by establishing cyberspace as a separate, self-
governing "territory." Nonetheless, their reliance on realist assump-
tions to define the structure of a proper regulatory regime suffers from
the same normative indeterminacy that has frustrated many govern-
ment officials. First, their assertion that cyberspace is immune from
territorial regulation is susceptible to an empirical rebuttal: realist
commentators who disagree with them need only refer to examples of
successful Internet regulations to refute their argument. 34

Second, realist arguments about cyberspace self-government implicitly support
indirect government regulation of the Internet. As James Boyle has
shown, governments can shape and develop the Internet through "pri-
vately deployed, materially based, technological methods of surveil-
lance and censorship." 35 In particular, the United States government
has frequently eschewed direct regulation in favor of subsidizing filter-
ing software and hardware to achieve privately what it lacks the
constitutional power to achieve directly. 36 Yet because this type of
regulation enrolls private actors as enforcement agents, it comports
with a realist understanding of Internet self-regulation. As this exa-
ples suggests, it is not the state but the realist conception that lacks the
capacity to contain the Internet.

2. The Representational Conception. — The representational con-
ception of sovereignty originates in traditional liberal ideology, which
views the individual as the most important unit of analysis in the in-
ternational system. 37 The state plays a secondary role as a representa-
tive institution composed of numerous individuals representing a mul-
titude of interests. 38 Although liberal theorists disagree about the

33 Johnson & Post, supra note 21, at 1393; see also Jason Kay, Sexuality, Live Without a Net:
Regulating Obscenity and Indecency on the Global Network, 4 S. Cal. Interdisciplinary L.J. 355, 387 (1995) ("Because government regulation has been unsuccessful, and self-regulation has
succeeded, the Internet should continue to be allowed to regulate itself.").

34 See, e.g., Timothy S. Wu, Note, Cyberspace Sovereignty? — The Internet and the Interna-
tional System, 10 Harv. J. L. & Tech. 647, 654-55 (1997) (describing examples of Internet regula-
tion in China and Singapore that cast doubt on "the arguments for cyberspace sovereignty inasmuch as they seem to make sense only in particular contexts").

35 Boyle, supra note 24, at 190.

36 See id. at 194. The recent World Intellectual Property Organization treaties are a promi-
nent example of this type of indirect regulation. By imposing strict liability for copyright in-
fringement on Internet service providers, the government encourages service providers to investi-
gate technologies that minimize their liability, thereby making them the government's "private
colice." Id. at 197. For a more thorough discussion of regulation through filtering technologies, see supra pp. 1640-44.

37 See Viotti & Kauppi, supra note 8, at 230-31.

38 See id.
extent to which a sovereign state actually "represents" domestic society, proponents of the representational conception assume that a truly sovereign state represents the general will of its populace. This inherently normative assumption suggests that "only a State that respects human rights and the principle of democratic representation is legitimate and therefore entitled to represent citizens internationally." Moreover, the legitimacy of applying a state’s laws to conduct that occurs in another state’s territory depends on whether such laws "would prevent [that] State from functioning as a sovereign; that is, the extent to which such generally applicable laws would impede a state government’s responsibility to represent and be accountable to the citizens of the State."

Government officials have often relied on the representational conception’s assumptions to support Internet regulations. In particular, officials have relied on its assumptions to support Internet regulations where online activities appear to undermine a sovereign’s ability to represent its populace. While introducing the Internet Gambling Prohibition Act of 1997, Representative Goodlatte noted:

The ability of the World Wide Web to penetrate every home and community across the globe has both positive and negative implications — while it can be an invaluable source of information and means of communication, it can also override community values and standards, subjecting them to whatever may or may not be found online. In short, the Internet is a challenge to the sovereignty of civilized communities, States, and nations to decide what is appropriate and decent behavior . . . . The legislation I am introducing today will protect the right of citizens in each State to decide through their State legislatures if they want to allow gambling within their borders and not have that right taken away by offshore, fly-by-night operators.

Thus, one can argue that Internet regulations are necessary to protect state sovereignty.

39 See id. at 228; Andrew Moravcsik, Taking Preferences Seriously: A Liberal Theory of International Politics, 51 INT’L. ORG. 513, 518 (1997). For a discussion of an alternative liberal understanding of the state, see infra section B.

40 See, e.g., Roxanne Lynn Doty, Sovereignty and the Nation: Constructing the Boundaries of National Identity, in STATE SOVEREIGNTY AS SOCIAL CONSTRUCT 121, 122 (Thomas J. Biersteker & Cynthia Weber eds., 1996) ("Today no state possesses legitimacy which does not also claim to represent the will of the nation." (quoting Anthony Smith, National Identity and the Idea of European Unity, 68 INT’L AFF. 55, 62 (1992)) (internal quotation marks omitted)).


44 143 CONG. REC. E1633 (daily ed. Sept. 3, 1997) (statement of Rep. Goodlatte); see 144 CONG. REC. S8815, S8816 (daily ed. July 23, 1998) (statement of Sen. Torricelli) ("If we want to have Indian tribes having Indian gaming, let them do it on their reservation. That is their right, their sovereignty. But my State has sovereignty, too. We have decided not to allow gaming in every community.").
Yet the assumptions underlying the representational conception also support arguments opposing Internet regulations. During the Gambling Prohibition Act’s debate, critics of the Act countered arguments about the need to protect states’ ability to represent their citizens with similar arguments that the Act would inhibit the ability of Indian nations to represent their own populations who might favor online gambling. For example, Senator Biden criticized the proposed regulations as continuing Congress’s hypocrisy in formally recognizing the sovereignty of Indian nations when distributing financial assistance but denying their sovereignty “whenever they do anything we don’t like.”

As the debate over gambling suggests, a representational conception of sovereignty shares the realist conception’s incapacity to provide a normative justification for Internet regulation. This failure results from the representational conception’s underlying circularity. In numerous contexts, a state’s populace may pursue activities that affect populations in other states or may desire regulations that restrict activities in foreign jurisdictions. In such cases, requiring one sovereign state to respect the “sovereignty” of another state presupposes that one is more sovereign than the other — a presumption that raises the question: what makes a state sovereign? Moreover, a normative application of a representational conception fails to explain Internet regulations in nondemocratic governments. Indeed, under a representational conception of sovereignty, these countries possess no sovereignty for the Internet to threaten.

3. The Postmodern Conception. — The postmodern conception of sovereignty combines several views about the dispersion of authority in an era of increasing globalization. Many of these viewpoints appear in the “New Medievalism” — an approach to international relations that asserts “a secular reincarnation of the system of overlapping or segmented authority that characterized” pre-Reformation Europe. As the world has become increasingly integrated, it is argued, authority patterns have dispersed into a variety of overlapping layers, much like the overlapping medieval authorities of emperor, pope, prince, and

46 HEDLEY BULL, THE ANARCHICAL SOCIETY 264 (1977); see Peter J. Spiro, New Global Communities: Nongovernmental Organizations in International Decision-Making Institutions, WASH. Q., Winter 1995, at 45, 46 (“It is almost as if the world has arrived at a sort of neo-medievalism in which the institutions and sources of authority are multifarious.”) This conception of dispersed state authority surfaces in various scholarly contexts. See, e.g., Rosemary J. Coombe, The Cultural Life of Things: Anthropological Approaches to Law and Society in Conditions of Globalization, 10 AM. U. J. INT’L L. & POL’Y 791, 831 (1995) (noting that because of globalization, cultures can no longer be considered bounded by territorial terms, but instead exist across borders); Alexander B. Murphy, The Sovereign State System as Political-Territorial Ideal: Historical and Contemporary Considerations, in STATE SOVEREIGNTY AS SOCIAL CONSTRUCT, supra note 40, at 81, 82-84, 107 (asserting that globalization challenges the sovereign state’s conceptual integrity by dispersing authority to a multitude of “significant functional spaces”).
feudal lord.\textsuperscript{47} New Medievalists note that states have gradually ceded sovereignty over significant social and economic issues to supranational institutions including the European Union and the World Trade Organization.\textsuperscript{48} Likewise, technologies such as the Internet have enabled individuals to create "new commonalties of identity that cut across national borders and challenge governments at the level of individual loyalties."\textsuperscript{49} Normatively, this dispersion provides a "flexible, multilayered approach to political-territorial governance"\textsuperscript{50} that can better address current transnational issues.\textsuperscript{51} By allowing individuals to form freely chosen, transnational communities, this dispersion also permits the full realization of democratic ideals. These interest-based communities encourage political activism directed to achieve commonly held goals\textsuperscript{52} and permit individuals to define themselves autonomously — to "shed the drab single-hued identities deterministically front-loaded onto their lives by the accidents and myths of birth and blood."\textsuperscript{53}

Many proponents of cyberspace sovereignty have relied on postmodern assumptions to assert the legitimacy of cyberspace self-governance. In addition to noting the demise of the sovereign state, these advocates assert that cyberspace has the capacity to realize a purer form of democratic government. Johnson and Post, for example, point to the "erosion of national sovereignty in the modern world and the failure of the existing system of nation-states to cultivate a moral connection between the individual and the community (or communities) in which she is embedded."\textsuperscript{54} Through the dispersion of sovereign authority, however, the Internet provides "[a] more promising basis for

\textsuperscript{49} Thomas M. Franck, Community Based on Autonomy, 36 Colum. J. Transnat'l L. 41, 43 (1997). Numerous commentators have asserted that the Internet facilitates the dispersion of individual loyalties from the state. See, e.g., Steven R. Salbu, Who Should Govern the Internet?: Monitoring and Supporting a New Frontier, 11 Harv. J.L. & Tech. 429, 457–58 (1998) ("Interactive computer technology signals a paradigm shift away from geographic conceptualizations of community, in favor of nongeographical communities." (citation omitted)).
\textsuperscript{50} Murphy, supra note 46, at 111.
\textsuperscript{51} See Thomas M. Franck, Clan and Superclan: Loyalty, Identity, and Community in Law and Practice, 90 Am. J. Int'l L. 359, 376 (1996) ("In many areas of endeavor — commerce, defense, environmental protection, health, entertainment, education — human needs and wants cannot ... be satisfied by, or in, the state alone.").
\textsuperscript{52} See Franck, supra note 49, at 49.
\textsuperscript{54} Johnson & Post, supra note 21, at 1397 (citing Michael J. Sandel, America's Search for a New Public Philosophy, Atlantic Monthly, Mar. 1996, at 57, 73–74).
a democratic politics.\textsuperscript{55} In particular, the highly heterogeneous character of cyberspace facilitates the development of separate "spheres of activity," each with its own set of rules.\textsuperscript{56} In contrast to a territorial government, which assumes a citizen's consent through his continued presence, cyberspace permits users to exit easily from disagreeable sets of rules, "thus providing a more legitimate 'selection mechanism' by which differing rule sets will evolve over time."\textsuperscript{57} Further, the segmentation of cyberspace and the ability to "fractionat[e]" one's online identity permit individuals to abide by rule sets that correlate with their own multi-variegated selves.\textsuperscript{58} For many advocates of cyberspace sovereignty, imposing government regulations in the face of this "social contract" is simply tyranny.\textsuperscript{59}

Commentators adopting postmodern logic, however, have often contested the potential of the Internet to realize democratic ideals. In particular, commentators have focused on the potential of real world power differentials to shape online social relations. In studying the development of Internet intellectual property protection, Keith Aoki notes that intellectual property owners' "privatization" of the Internet has created significant disparities of wealth. "[M]apping electronic space as 'private' creates conditions under which a privately constructed and owned electronic information system . . . embody[es] the essential features of a private enterprise economy: inequality of income along with the production of goods and services for profit."\textsuperscript{60} Simi-

\textsuperscript{55} Id. at 1398 (quoting Sandel, supra note 54, at 74); see ESTHER DYSON, RELEASE 2.1, at 128 (1998) (noting existence of "'legitimate' Net governments . . . [that] control Net territory by consent and indeed request of the governed"); Todd H. Flaming, The Rules of Cyberspace: Informal Law in a New Jurisdiction, 85 ILL. B.J. 174, 179 (1997) (asserting that territorial governments should recognize cyberspace as an autonomous space that orders itself according to the preferences of the Internet community); Aaron Mefford, Note, Lex Informatica: Foundations of Law on the Internet, 5 IND. J. OF GLOBAL LEGAL STUD. 211, 236 (1997) (asserting that self-regulation is more legitimate than territorial law because users create "Net law"); Barlow, supra note 6 ("Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours . . . . We are forming our own Social Contract.").

\textsuperscript{56} Johnson & Post, supra note 21, at 1396.

\textsuperscript{57} Id. at 1399. Esther Dyson similarly believes that deference to "Net governments" is warranted by an "exit" theory. See DYSON, supra note 55, at 128. She notes that in contrast to "territorial governments[, which] are natural monopolies in their own territories, cyberspace governments compete." Id. Thus, a Net government must "provide its citizens with real benefits if it wants them to stick around." Id.

\textsuperscript{58} See Johnson & Post, supra note 21, at 1399 n.102.

\textsuperscript{59} See Barlow, supra note 6 ("I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us.").

larly, Margaret Chon argues that real world power disparities, stemming from geographical or cultural privilege, continue to exist on the Internet, making some users “more free to contract than others.” This characteristic of cyberspace facilitates “private acts of oppression,” which governments are obligated to address. These concerns may in part motivate advocates of cyberspace government to hedge their arguments; as Johnson and Post note, the authority of cyberspace government should be limited to areas “unrelated to vital and localized interests of a territorial government.”

Ultimately, arguments for cyberspace governance based on postmodern assumptions support the same realist conception of sovereignty that they seek to repudiate. Within the postmodern conception exists a fixation with the traditional, territorial concepts of “sovereignty” that bolsters realist modes of thinking. Despite averring the dispersion of sovereignty, proponents of cyberspace governance cannot completely break loose from its influence, identifying themselves as a singular “Cyberspace” even as they celebrate the multitude of separate communities. Moreover, the postmodern depiction of the Internet as a space in which individuals may pursue any and all interests seems to sustain governments’ concerns that the Internet represents a “lawless” realm in need of “line drawing.” The end result is a discourse of sovereignty that imbues the Internet regulation debate with significant rhetorical flare, yet is bereft of persuasive normative arguments about particular regulatory regimes.

B. Reassessing Cyberspace, Sovereignty, and the State

Notwithstanding the arguments opposing Internet regulation, governments around the world seem determined to regulate cyberspace. At least twenty countries currently restrict access to Internet websites,
and more than a dozen are considering restrictions.\textsuperscript{66} Within the United States, the number of Internet-related bills introduced in Congress has almost doubled in the past two years.\textsuperscript{67} What might explain these attempts to regulate the Internet aside from indeterminate appeals to sovereignty? This section argues that adopting a liberal-constructivist approach to domestic politics provides insights into the motivation of states to regulate the Internet and, more importantly, about the implications of such regulations.

Liberal international relations (IR) theory posits three core assumptions about the international system.\textsuperscript{68} First, the system’s fundamental actors are individuals and private groups who seek to advance differentiated interests through collective action.\textsuperscript{69} The theory rejects the notion of an automatic harmony of interests among individuals in society; rather, material scarcity, conflicting values, and variations in societal influence promote conflicting social goals and the willingness to use coercion to achieve them.\textsuperscript{70} Second, states (and other political institutions) represent some subset of domestic society whose interests define state preferences.\textsuperscript{71} According to this view, the state is a representative institution that is constantly subject to capture and recapture by individuals and groups who turn to the state to effectuate their particular interests.\textsuperscript{72} Third, state behavior reflects a state’s attempt to realize its preferences under the constraints imposed by the preferences of other states.\textsuperscript{73} When a state’s preferences are harmonious with those of other states, there are incentives for the full realization of its preferences; when they conflict, the potential for interstate tension encourages policy negotiation or, at times, interstate conflict.\textsuperscript{74}

Liberal IR theory can be combined with “constructivist” notions of social identity formation to create an account of domestic politics and interstate relations that proves much more useful in analyzing Internet regulations than existing conceptions of sovereignty.\textsuperscript{75}


\textsuperscript{68} See Moravcsik, supra note 39, at 516.

\textsuperscript{69} See id.

\textsuperscript{70} See id. at 517.

\textsuperscript{71} See id. at 518.

\textsuperscript{72} See id.

\textsuperscript{73} See id. at 520.

\textsuperscript{74} See id. at 521.

\textsuperscript{75} “Constructivist” international relations theory focuses on the manner in which states form their identities and interests in “intersubjective” relationships with one another. See Alexander Wendt, Anarchy Is What the States Make of It: The Social Construction of Power Politics, 46 INT’L ORG. 391, 393–94 (1992). The notion that actors acquire their identities and interests through participation in collective meanings has also informed several other academic disciplines. See Jerry Frug, Decentering Decentralization, 60 U. CHI. L. REV. 253, 273–78 (1993) (surveying...
ory's focus on a society's multiple, competing interests suggests that a state (or other political entity) must continually "construct" itself as a unified political community. Only by constructing a unified community that has discrete, stable interests can dominant social groups hope to legitimize their capture of governmental institutions and turn their interests into community preferences. Furthermore, societal criteria such as ethnicity, cultural traits, and history "are themselves fuzzy, shifting and ambiguous," making it difficult to articulate clearly who the state actually represents. Under this "liberal-constructivist" approach, law functions in two ways. First, as a coercive instrument of state power, it allows social groups to allocate power among their competing normative perspectives. Second, it enables the dominant social group to articulate an authoritative vision of the state — to construct the borders of an "imagined" community.

The Internet triggers government regulation for both of these reasons. In the first instance, the Internet can inject perspectives into a political community that conflict with the dominant social group's interests, thereby requiring legal resolution. *United States v. Thomas* provides a vivid example of this type of conflict in the context of Internet pornography. The defendants, operators of a California bulletin board service, were convicted under a Tennessee obscenity statute after a federal agent in Memphis downloaded allegedly obscene images from the defendants' service. On appeal, the defendants argued that the lower court incorrectly applied the Memphis community's standard of obscenity. They reasoned that "the computer technology used here requires a new definition of community, i.e., one that is based on the broad-ranging connections among people in cyberspace".

---

76 See Note, Constructing the State Extraterritorially: Jurisdictional Discourse, the National Interest, and Transnational Norms, 103 HARV. L. REV. 1273, 1275 (1990) ("[T]he determination of the 'national interest' [affixes] a badge of national legitimacy onto the interests of a particular group.").


78 See Doty, supra note 40, at 122 ("When it is no longer clear who makes up the nation, a state's internal sovereignty and the existence of the state itself is threatened.").

79 Michel Foucault called this the juridical aspect of the law. See MICHEL FOUCAULT, 1 HISTORY OF SEXUALITY 136–52 (Robert Hurley trans., 1980). It regulates negatively, through limitation, prohibition, and control. See id.

80 Cf. BENEDICT ANDERSON, IMAGINED COMMUNITIES: REFLECTIONS ON THE ORIGIN AND SPREAD OF NATIONALISM 6–7 (2d ed. 1991) (noting that every nation is "an imagined political community"). Foucault believed this function to be the primary characteristic of law in the modern era. See MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 194 (Alan Sheridan trans., 1977). Law's power "produces; it produces reality; it produces domains of objects and rituals of truth." Id.

81 74 F.3d 701 (6th Cir. 1996).

82 See id. at 705.

83 See id. at 711.
rather than the geographic locale of the federal judicial district of the criminal trial.84 By juxtaposing the two standards, the argument highlighted the Internet's facilitation of conflict between the normative perspectives held by a community's dominant social group and those held by the members of an outside community — in this case, a "virtual community."

Such conflicts will require a legal resolution because of the continued importance of geography in constructing values. Despite postmodern assertions that non-geographic communities will replace "chats across white picket fences,"85 evidence suggests that an inherent connection exists between geography and cultural values.86 Even on the Internet, activity generally centers around geographically-based interests. Recent studies of "virtual communities," for instance, show that most interactions are between people who are seen in-person at work or at leisure,87 and website providers have responded to increased demands for regional and local focuses.88 Given the continued importance of geographic communities, individuals are likely to turn first to

---

84 Id.
85 Franck, supra note 49, at 49.
86 See, e.g., Peter A. Andersen, Myron W. Lustig & Janice F. Andersen, Regional Patterns of Communication in the United States: A Theoretical Perspective, 54 COMM. MONOGRAPHS 128, 140 (1987) (arguing that despite homogenizing forces in the United States, distinct regional cultures continue to exist); see also H.R. Trevor-Roper, Fernand Braudel, the Annales, and the Mediterranean, 44 J. MODERN HIST. 468, 470 (1972) (summarizing the Annales school of history, which focuses on the importance of "[g]eography, climate, [and] population" in social development). But see Hubert J.M. Hermans & Harry J.G. Kempen, Moving Cultures: The Perilous Problems of Cultural Dichotomies in a Globalizing Society, 53 AM. PSYCHOLOGIST 1111, 1111 (1998) ("In an increasingly interconnected world society, the conception of independent, coherent, and stable cultures becomes increasingly irrelevant.").
87 See Barry Wellman & Milena Gulia, Net Surfers Don't Ride Alone: Virtual Community as Community, in NETWORKS IN THE GLOBAL VILLAGE (Barry Wellman ed., 1998), at *11 (draft available at <http://www.acm.org/ccp/references/wellman/wellman.html> (on file with the Harvard Law School Library); see also Personality Crisis? Not on the Net, PSYCHOL. TODAY, Mar./Apr. 1998, at 70 (finding that the majority of participants in an Internet study avoided the "anarchy" of chat rooms and virtual communities and used the Internet only for work). But see Karen L. Michaelson, Information, Community, and Access, 14 SOC. SCI. COMPUTER REV. 57, 58-59 (1996) (noting that people may possess stronger ties to their virtual communities of interest than their own physically based communities because virtual communities are based on shared interests and not just shared location); supra p. 1591-92 (describing virtual communities that "provide vivid examples of the capacity of online groups to facilitate sustained and meaningful interaction").
88 Several large Internet businesses have cited consumer demand as a motivating factor in reorienting their websites toward the local and the regional. See, e.g., Randi Bussin, Multilingual Web Site Strategy & Implementation: Microsoft (visited Apr. 19, 1999) <http://www.headcount.com/globalsource/articles.htm> (on file with the Harvard Law School Library) (explaining that Microsoft moved toward localized websites because its "customers expressed a genuine demand for local content"). International portals have also begun to offer local assistance. See, e.g., Lankaweb (visited Apr. 19, 1999) <http://www.lankaweb.com> (on file with the Harvard Law School Library) (providing Sri Lankan users with regional offerings and access to local Usenet discussions, Sri Lankan IRC chat channels, news, and travel information).
their community’s laws for resolution of conflicts that occur in cyber-space but manifest themselves in real-space.

In addition, legal resolution of these conflicts permits the dominant social group to articulate a vision of the political community’s collective identity and values. Here, the object of the regulation is the community as a whole. In *Thomas*, the court’s upholding of the local community standard enabled Memphis residents to articulate a unified vision of their community. Although there was initial opposition to the Thomases’ convictions, the jury’s verdict established that Memphis spoke with one voice about the issue of Internet pornography. Commenting on the outcome of the case, a Memphis Assistant U.S. Attorney noted, “when the case is brought and decided by a judge or jury, that’s when the community speaks.” For the broader Memphis community, the verdict redefined Memphis as “the country’s porn-fighting capital.”

A liberal-constructivist approach also suggests that there are significant limitations to a government’s willingness to regulate the Internet. According to the third assumption of liberal theory, a state is less inclined to pursue its preferences when doing so imposes negative externalities on dominant social groups in other states. The current architecture of the Internet, however, necessarily creates negative externalities with Internet regulations. As discussed above, Germany’s regulation of CompuServe’s Usegroups forced CompuServe to shut down approximately two hundred groups, affecting subscribers in 147 countries. Regulation in the face of such externalities suggests that global virtual communities are of minor concern to officials pursuing state preferences. In the cases of CompuServe and the Thomases, purchasers of Internet pornography — even on a global scale — did not constitute a sufficiently dominant social group to create risks of costly interstate conflict. In contrast, a state will likely refrain from regulating if doing so would impose externalities on socially dominant groups. Thus, it is not surprising that, despite asserting its right to regulate U.S. mutual fund websites under its domestic law, the British government has refrained from taking enforcement action after recognizing a conflict with United States regulations.

---

89 For example, one Memphis editorial, published shortly before the trial, argued against convicting the Thomases, noting that “it would be better to err on the side of freedom than a heavy-handed, old-time censorship.” *Porn Trial: Memphis Case Points to New World of Law*, COM. APPEAL (Memphis, Tenn.), July 19, 1994, at A6.
90 Michael Kelley, *Banned in Memphis: City Has High Profile in Obscenity Case History*, COM. APPEAL (Memphis, Tenn.), June 1, 1995, at C1.
91 *Id.*
92 See *Moravcsik*, supra note 39, at 521.
A liberal-constructivist approach also provides a clearer assessment of the implications of Internet regulations. First, its focus on the societal competition of interests reveals that both Internet and non-Internet regulations privilege some perspectives while subordinating others. Through the translation of privileged perspectives into a community’s preferences, such privileging results in the construction of a community identity achieved by “selecting, editing, and unifying disparate elements — the creation of a sameness out of a multitude of differences.” Such a unified image “hinders an individual’s ability to express multiple solidarities or to dissent from a determination viewed as neither collective nor good.” Whereas these regulatory costs ordinarily affect only a particular jurisdiction’s residents, the Internet allows a community to impose these costs on distant populations and individuals that might adhere to differing normative frameworks. Moreover, because these individuals may be globally dispersed, a liberal-constructivist approach suggests that the international system imposes few constraints on a community’s desire to enact such regulations.

Second, the emphasis on a community’s construction of identity suggests that regulations may nevertheless prove beneficial in creating social stability and facilitating the formation of group values and interests. Just as the Thomas verdict enabled a community to articulate a collective vision of itself, it also provided a means for defining and communicating dominant group values. Yet Internet regulations may impede other communities from similarly constructing collective identities and from forming such values. Indeed, permitting the flow of controversial information may enable some social groups to articulate a commitment to freedom of expression. Germany’s prohibition...
of pornographic content thus ignored the extent to which the presence of such content — even if not substantively desired — permits social groups to affirm and develop their own values. In time, such regulations will drive the development of Internet filtering technology that will permit geographical targeting of activities; but in the meantime, assessing the legitimacy of a regulatory regime must entail recognizing the regulatory costs for individuals and social groups.

C. The Issue of Personal Jurisdiction

Court opinions addressing the scope of personal jurisdiction in Internet cases reflect the same formalist reliance on the normative aspect of state sovereignty as the debates about cyberspace regulation. As in the context of the regulatory debate, the normative indeterminacy of “sovereignty” has contributed to persistent confusion among the courts about the legitimacy of establishing jurisdiction over Internet activities. The following section addresses the role that sovereignty has played in this confusion and how a liberal-constructivist approach might clarify the issues involved in the cases.

1. Personal Jurisdiction and the Internet. — A primary source of confusion for courts’ assessing the scope of their personal jurisdiction in cyberspace results from realist assumptions inherent in contemporary personal jurisdiction doctrine. According to traditional civil procedure lore, the Supreme Court abandoned these realist assumptions in *International Shoe v. Washington* in favor of a more flexible “minimum contacts” test. Yet as numerous commentators have noted, the “minimum contacts” test remains quintessentially territorial, inquiring whether a “defendant purposefully avails itself of the privilege of conducting activities within the forum State.”

---

100 *See* Goldsmith, *supra* note 13, at 489–90.

101 *Pennoyer v. Neff*, 95 U.S. 714 (1878), was the primary articulation of the realist view of personal jurisdiction. The Court asserted that “[t]he authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established.” *Id.* at 720.

102 326 U.S. 310 (1945).


105 *Hanson v. Denckla*, 357 U.S. 235, 253 (1958). In *Hanson*, the Court emphasized the personal jurisdiction doctrine’s implicit realist assumptions, noting that restrictions on personal jurisdiction were a “consequence of territorial limitations on the power of the respective States.” *Id.* at 251. *See* World-Wide Volkswagen v. Woodson, 444 U.S. 286, 291–92 (1980) (stating that the doctrine “acts to ensure that the States, through their courts, do not reach out beyond the limits imposed on them by their status as coequal sovereigns in a federal system”).
when the Court has sought to depart from the territorial aspect of the doctrine, it has relied on realist principles. For example, in Calder v. Jones,106 the Court allowed the exercise of jurisdiction over a nonresident defendant by adopting the inherently realist "effects" doctrine.107

The Court's attempt to connect jurisdiction to a state's territorial authority has divided lower courts over the proper interpretation of personal jurisdiction in cases in which a defendant "contacted" a forum state solely through a website.108 An initial point of contention for courts has been whether a defendant falls within the "doing business" prong or the "effects" prong of a state's long-arm statute.109 Courts addressing allegedly tortious acts have generally relied on the effects prong,110 but they have differed over the "location" of a harm. For instance, in Bensusan Restaurant Corp. v. King,111 the plaintiff, New York's Blue Note Club, alleged that the defendant, the owner of a Missouri club of the same name, had diluted its trademark by advertising on a Missouri-based website.112 In addressing where the "passing off" occurred, the court held that to the extent that confusion about the relationship of the clubs existed because of the website, it occurred in Missouri rather than in New York.113 In contrast, other courts considering online trademark disputes have found the location of the plaintiff's harm to be in the state in which the plaintiff accessed a website rather than in the state in which the site was operated.114 Courts interpreting a "doing business" prong have similarly divided

---

107 See discussion and sources cited supra note 17.
109 Most states have adopted long-arm statutes that provide for personal jurisdiction over any cause of action arising from a nonresident's "transaction of any business within [the] State." JACK H. FRIEDENTHAL, MARY KAY KANE & ARTHUR R. MILLER, CIVIL PROCEDURE 139 (2d ed. 1993) (quoting ILL. REV. STAT., Ch. 110, para. 2-209). Several states also have long-arm statutes that contain an "effects" prong. These statutes provide for jurisdiction over any defendant who "commits a tortious act without the state causing injury to person or property within the state." Id. at 143 n.11 (quoting N.Y. C.P.L.R. 301(a)(3) (McKinney 1998)).
110 See e.g., Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1331 (E.D. Mo. 1996) (finding that trademark infringement was tortious in nature and that application of the "effects" provision was proper); Panavision Int'l v. Toeppen, 938 F. Supp. 616, 621-22 (C.D. Cal. 1996) (same). But see Cybersell v. Cybersell, 130 F.3d 414, 420 n.6 (9th Cir. 1997) (rejecting the application of "effects" doctrine in a trademark infringement case).
112 See id. at 297.
113 See id. at 299. The Second Circuit, in affirming the district court's judgment, did not refer to this finding. Rather, it held that "[e]ven if Bensusan suffered injury in New York, that does not establish a tortious act in the state of New York within the meaning" of the New York long-arm statute. Bensusan Restaurant v. King, 126 F.3d 25, 29 (2d Cir. 1997) (emphasis added).
114 See, e.g., Maritz, 947 F. Supp. at 1331 (finding that alleged injury occurred in Missouri); Panavision, 938 F. Supp. at 621-22 (asserting that "the brunt" of alleged harm was "borne in California").
over whether maintaining a website constitutes "doing business" in the state in which the defendant operates the website or the state in which the plaintiff accessed the website.\footnote{Compare Panavision, 938 F. Supp. at 622 (refusing to hold that cyber-pirate was not "doing business" in California via the Internet), with Hasbro v. Clue Computing, 994 F. Supp. 34, 44 (D. Mass. 1997) (holding that a company had "solicit[ed] business" in Massachusetts through the use of a website domain name that allegedly infringed the plaintiff's trademark).}

The realist aspect of personal jurisdiction has also divided courts applying due process analysis in Internet-related cases. In particular, courts have applied different interpretations of the "purposeful availment" standard in cases involving Web-based activities. Several courts have found that a defendant's website is a sufficient basis for upholding jurisdiction based on the theory that the defendant, through her website, "purposefully availed" herself of the benefits of all fifty states.\footnote{See, e.g., Hasbro, 994 F. Supp. at 44-45 (asserting jurisdiction because the defendant, by advertising on its website, purposefully directed its advertising at all the states); Heroes, Inc. v. Heroes Found., 958 F. Supp. 1, 4-5 (D.D.C. 1996) (summarizing cases that held that the mere existence of a website was a sufficient basis for personal jurisdiction); Inset Sys. v. Instruction Set, Inc., 937 F. Supp. 161, 165 (D. Mass. 1996) (holding that existence of website subjected defendant to Connecticut jurisdiction).}

Over the past two years, however, a moderate consensus has emerged: courts assessing personal jurisdiction examine the level of "interactivity" on a particular website and the presence of any additional forum-related activity.\footnote{See, e.g., McDonough v. Fallon McElligott, Inc., No. Civ. 95-4037, 1996 WL 753991, at *3 (S.D. Cal. Aug. 5, 1996) (noting that "[b]ecause the Web enables easy world-wide access, allowing computer interaction via the [W]eb to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists").} The mere use of a "passive" website fails to prove that a defendant "purposefully availed" herself of the forum state.\footnote{See Patriot Sys., Inc. v. C-Cubed Corp., 21 F. Supp. 2d 1318, 1324 (D. Utah 1998) (stating that "current case law reveals three general categories along a 'sliding scale' for evaluating jurisdiction," with jurisdiction existing over an individual who "clearly does business over the Internet," but lacking over one who merely uses a "passive Web site that does little more than make information available to those who are interested in it" (quoting Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123-24 (W.D. Pa. 1997)) (internal quotation marks omitted)); accord Cybersell v. Cybersell, 130 F.3d 414, 418 (9th Cir. 1997) (requiring "something more" than a "passive" website for jurisdiction to be proper).}

2. Reconstructing Personal Jurisdiction in Internet-Related Cases. — A liberal-constructivist vantage point would significantly change the focus of the personal jurisdiction analysis of online activities. Rather than relying on concepts of "minimum contacts" or "interactivity," a liberal-constructivist approach would use two primary considerations to resolve personal jurisdiction inquiries: how would the determination allocate power between competing normative perspectives,
and how would it affect the ability of other communities to construct identities and interests?

First, because the determination of personal jurisdiction may affect the substantive outcome of a lawsuit, such a determination allocates power between competing normative perspectives within a jurisdiction. Even before the Internet existed, this issue arose in a variety of contexts such as consumer action claims. For instance, in *McGee v. International Life Insurance Co.*, the Supreme Court empowered consumer interests by upholding a California court's finding of personal jurisdiction over a nonresident insurance company. The Court reasoned that "residents would be at a severe disadvantage if they were forced to follow the insurance company to a distant State in order to hold it legally accountable." In other contexts, the Court has shifted the scales in favor of business interests. In *Carnival Cruise Lines, Inc. v. Shute*, the Court upheld a forum selection clause that required cruise ticket purchasers to file all lawsuits in Florida. The Court refused to strike down the clause on the basis of a lack of bargaining parity, and instead focused on the efficiency gains such clauses provided to businesses.

The Internet magnifies this issue because of the Internet's expansive reach and its accessibility to individual users. Because of these characteristics, personal jurisdiction determinations are more likely to affect the substantive outcome of Internet disputes than other disputes. For the operator of a website, an adverse jurisdictional finding might lead to suits in multiple, distant forums, thereby significantly increas-

---

120 To a certain extent, current doctrine reflects this fact through the requirement that courts assess the "reasonableness" of jurisdiction in light of "the burden on the defendant ... and the plaintiff's interest in obtaining relief." *Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102, 113 (1987). Nonetheless, most courts accord little weight to personal jurisdiction's "reasonableness" prong, see *Burger King Co. v. Rudzewicz*, 471 U.S. 462, 474-75 (1985), and generally determine the issue under the heading of the "purposeful availment" test, requiring the court to couch its analysis in the language of "contacts," see Earl M. Maltz, *Visions of Fairness — The Relationship Between Jurisdiction and Choice-of-Law*, 30 ARIZ. L. REV. 751, 754 (1988). "Taken together, *World-Wide Volkswagen, Keeton* and *Burger King* clearly establish the primacy of the concept of 'purposeful availment' in the analysis of specific jurisdiction cases." *Id.*


122 Id. at 223.


125 *See* id. at 596-97.

126 *See* id. at 593.

127 *See* id. at 593-94.

128 The Sixth Circuit has noted that "[t]he Internet represents perhaps the latest and greatest manifestation of ... historical, globe-shrinking trends. It enables anyone with the right equipment and knowledge ... to operate an international business cheaply, and from a desktop." *CompuServe, Inc. v. Patterson*, 89 F.3d 1257, 1262 (6th Cir. 1996).
ing the cost of litigation. For parties seeking to enforce their rights on
the Internet, an adverse jurisdictional finding might require them to
initiate lawsuits across the country, similarly making litigation exces-
sively costly. Thus, by denying personal jurisdiction in Bensusan, the
court allocated power away from New York trademark owners to non-
resident, Web-based infringers of those trademarks. In contrast, the
Ninth Circuit’s upholding of California’s jurisdiction over an Illinois-
based Web “pirate” allocated power in favor of Californian trademark
owners. In neither case, however, did the court directly address the
reasons for favoring one perspective over the other.

A liberal-constructivist approach would seek a more transparent
assessment of the competing normative perspectives at issue. A nota-
ble illustration of such an approach appeared in Digital Equipment
Corp. v. AltaVista Technology, Inc. In Digital, the Massachusetts
district court directly addressed the two competing normative perspec-
tives in considering whether it could exercise personal jurisdiction over
the owner of a California-based website that allegedly diluted the
plaintiff’s trademark. The court expressed concern about “forc[ing]
corporations that do business over the Internet, precisely because it is
cost-effective, to now factor in the potential costs of defending against
litigation in each and every state; anticipating these costs could make
the maintenance of a Web-based business more expensive.” Nonetheless, the court noted that it was “troublesome to allow those who
conduct business on the Web to insulate themselves against jurisdic-
tion in every state, except in the state (if any) where they are physically
located.” After framing the issue as a competition between these
two perspectives, the court could better evaluate the consequences of
its decision to grant jurisdiction.

In addition to focusing on the effect of personal jurisdiction deter-
minations on allocations of power, a liberal-constructivist approach
would also examine the manner in which such determinations affect a
community’s ability to define itself. The process of self-definition con-
ists of two elements. First, a community defines itself through the ar-
ticulation of collective identity. Second, this articulation, in turn,
shapes the community’s underlying values and interests. In the per-
sonal jurisdiction context, a court’s grant of jurisdiction allows a
community to articulate its collective identity through the resolution of
a particular legal conflict; however, it also prevents other courts from
hearing the same case. The zero-sum nature of personal jurisdiction,

129 See Panavision, Int’l v. Toeppen, 141 F.3d 1316, 1318 (9th Cir. 1998).
131 Id. at 471.
132 Id.
133 See id. at 472.
134 See supra pp. 1695–97.
in part, led the Supreme Court to permit the evaluation of "the forum State's interest in adjudicating the dispute" as part of the reasonableness prong of the personal jurisdiction test.

The Internet complicates this understanding of personal jurisdiction because of the ease with which one community may impede the ability of other communities to construct their identities. A finding of personal jurisdiction in an Internet-related case enables a community to resolve a conflict in accordance with its preferences, but in so doing, it elevates these preferences over those that exist in other communities. In Blumenthal v. Drudge, for example, the plaintiffs sought jurisdiction in the District of Columbia over the writer of an online political magazine based in California that had allegedly defamed them in a series of articles published on the Internet. The defendant's objection to jurisdiction was undoubtedly grounded in a belief that the Washington, D.C., community's values could potentially influence the outcome of the case. In particular, the distinct population that resided within the court's jurisdiction most likely shared a different normative perspective on political satire than residents of an alternative forum. As in Thomas, the court's jurisdictional grant elevated the District of Columbia's preferences above those of other communities that might view the conduct differently. Similarly, the jurisdictional grant potentially altered the substance of the community's dominant values: first, by providing a means for Washington, D.C., residents to "speak with one voice," it allowed for an affirmation of the dominant group's values and, second, by imposing costs on the online-publication of political satire, it affected the quality and quantity of the information through which the group develops such values.

The Blumenthal court's reliance on territorial terminology obscured the manner in which its holding effectively imposed the District of Columbia's values on the rest of the political satire-writing world, potentially shaping those values as it did so. Although the court noted

---

137 See id. at 46.
138 The differing attitudes expressed by Los Angeles and Washington reporters toward Drudge suggest how the two populations' normative perspectives may have differed. Compare Karen Kaplan, A Question of Ethics: Online Gossip Columnist Drudge Debates Establishment Media, L.A. TIMES, Nov. 17, 1997, at D3 (characterizing Drudge as merely a "media establishment symbol" for the substantial problems of the "freewheeling Internet"), and Neal Gabler, GOSSIP: Why Let Truth Get in the Way of a Good Story?, L.A. TIMES, Oct. 26, 1997, at M1 (perceiving Drudge as satisfying a society's need for entertainment value through the ease of Internet publication), with Howard Kurtz, In Lewinsky Saga, A Cast of Dozens, WASH. POST, March 2, 1998, at C1 ("Blumenthal is understandably seeking retribution for a false story that he had a history of spousal abuse."), and John Schwartz, Journalism's Old Rules Should Apply to Cyber-Libel, WASH. POST, Jan. 26, 1998, at F20 ("I have never met Matt Drudge, but I have a powerful feeling that if I did, I wouldn't like him at all.").
the "non-geographic nature of communicating via the Internet," it found jurisdiction on the basis of the defendant's use of an "interactive" website and his additional forum-related activities. According to the court, the defendant had "engaged in a persistent course of conduct in the District of Columbia." Behind this seemingly objective finding, however, the court failed to explain its choice to impose one community's normative framework over all others. Had it viewed the personal jurisdiction issue through a liberal-constructivist lens, the court might have directly confronted the significance of its decision: What was the importance of allowing the court's local community to define itself through the case at issue compared to the importance of allowing another community this opportunity? To what extent did elevating a single community's values affect the development of those values both inside and outside the community? What was the importance, if any, of allowing the online magazine to operate as a forum for dissent from the community's normative framework?

The proposal advanced here elicits a different understanding of the issues involved in a personal jurisdiction inquiry in Internet-related cases. Faced with an Internet-related case, the decisionmaker would not be able to justify her holding by invoking the indeterminate categories of "minimum contacts" or "sovereignty" when adjudicating particular claims. Rather, she would have to recognize her decision as a normative choice and consider the issue on its merits.

D. Conclusion

The Internet forces us to face anew the tension between pluralism and order. By placing ideas in contact with people, the Internet accentuates the diversity of perspectives that characterizes our world. Yet in so doing, it highlights the difficulties that arise as communities — both those delimited by jurisdictional borders and those defined by commonalities of interests — struggle to define themselves. In the context of Internet regulation, the law must recognize the role it plays in shaping the outcome of these struggles.

The multitude of conflicts that can arise because of the Internet suggests that order might require national uniformity; only by imposing uniform rules will judges know how to resolve conflicts that arise between communities. The lessons of the Internet, however, suggest that "lawless" pluralism may have value that proponents of order frequently overlook. If individuals differentiate their normative orders according to their localities, race, gender, or creeds, then an unregulated Internet may provide a valuable asset in decreasing the social

139 Blumenthal, 992 F. Supp. at 54.
140 See id. at 56.
141 Id. at 57.
costs associated with the hegemonic effect of law. Nevertheless, for those individuals who identify themselves primarily on the basis of shared, local norms, either an unregulated Internet or nationally directed regulations may entail other social costs.

In the end, this conception of Internet regulation reveals not the "answer," but the persistent question about how to balance pluralism and order within a territorial state.