Washington University Journal of Law & Policy

Volume 21 *The Rehnquist Court and the First Amendment*

January 2006

The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle

John G. Palfrey Jr.

Robert Rogoyski

The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle

John G. Palfrey, Jr.
Robert Rogoyski*

This Article traces the evolution of thinking regarding the technical concept of the end-to-end principle and the legal concept of the regulation of the flow of packets across the Internet. We focus on the manner in which the state, in concert with private parties, has approached the tension between restricting the flow of certain packets and vindicating their citizens' interests, both legal and otherwise, in free expression. We argue that the primary mode of legal regulation of the Internet has shifted from a focus on outlawing activities at the nodes—end-points in the network—to a growing emphasis on regulating closer to the middle of the network. This trend is, on its face, good for the law enforcement officer, but worrisome to the technologist and the democratic activist; the end-to-end principle, held dear by those who built the Internet for decades, is under threat. In the process, this shift also places corporations, often based in other jurisdictions, in the position of enforcing the rules of the regime in which they are doing business, but whose views on free expression and other civil liberties the corporations' officers and directors do not necessarily share. We argue that the end-to-end principle, once translated loosely into political speak as "net neutrality," is a forceful rhetorical concept—and, if done right, sound public policy—but that it no longer describes the Internet on the ground, if it ever did.

---

* John Palfrey is a Clinical Professor of Law at Harvard Law School and the Executive Director of the Berkman Center for Internet & Society. Rob Rogoyski is a graduate of the Harvard Law School. The authors wish to thank Jonathan Zittrain and each of the participants in the Washington University *Journal of Law & Policy*'s Symposium on the Rehnquist Court and the First Amendment, held in November of 2005, for their commentary on the presentation that led to this paper. The authors alone are responsible for all errors and omissions.

I. INTRODUCTION

It is common for technologists to support the policy that intermediaries on the Internet should "pass all packets." This so-called end-to-end principle of network neutrality calls for intelligence to be located at the edges of the network if at all possible. While the end-to-end principle has been both challenged and refined since Saltzer, Reed, and Clark first documented it in the early 1980s, it remains a sacred concept among true believers in the openness of the Internet's original design.[1] Over the past decade, most nations—the United States among them—have established rules that sometimes encourage and sometimes require intermediaries to block or inspect packets as they travel across the Internet.[2] These rules prompt private actors to violate the end-to-end principle, at least theoretically, in the name of public interest. This Article considers the changes over the past ten years in states' approaches to the rules requiring private parties to control packets at various points in the network, a trend brought into relief by the current public debate over competing "net neutrality" proposals—a political and economic concept often conflated with the end-to-end principle of network design.

We suggest that a trajectory is emerging, whereby fewer controls are imposed at the end-points, and more are imposed closer to the center of the network. (We note also an increasing trend toward states requiring or otherwise causing private parties to exercise control of packets as they pass through the network.) This trend is clearest in those nations that are seeking to impose content-based filters on Internet content, though we make the case that a similar trend is apparent in the United States as well.

In terms of situating these ideas within the cyberlaw literature, this Article strives to build the short conceptual bridge between previous Internet law and policy scholarship concerning the states' and intermediaries' role in the control of online intermediaries and an emerging trend, based in part on new emerging issues, in favor of

1. J.H. Saltzer et al., *End-to-End Arguments in Systems Design*, 2 ACM TRANSACTIONS IN COMPUTER SYS. 277 (1984), *available at* http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

2. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 65–86 (2006).

forcing intermediaries to carry out the interests of the state at the middle of the network. We self-consciously pick up on and seek to extend the work of scholars such as Jonathan Zittrain,[3] Lawrence Lessig,[4] Timothy Wu,[5] Jack Goldsmith,[6] and Joel Reidenberg,[7] among others.[8] The idea is to focus on a key question of Internet law in the context of what is now commonly known as "Web 2.0": What actions are states taking when they do not want certain types of packets to pass through today's network, or when they seek to learn more about the packets and who are sending and receiving them?[9]

The short history of states seeking to block the passage of packets includes five primary regulatory approaches that fall into two broad clusters. The initial, broad cluster involves state-mandated controls at the end-points of the network. First, states have sought to block harmful packets at their source.[10] The idea is to stem the problem by making it illegal to send packets deemed to be harmful to some segment of the public.[11] This idea is based primarily on the notion that access to the information embedded in such packets is harmful to the public interest. Examples of this approach include the

3. *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

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

5. *See* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679 (2003).

6. *See* GOLDSMITH & WU, *supra* note 2; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998); Jack Goldsmith & Timothy Wu, *Digital Borders*, LEGAL AFF., Jan.–Feb. 2006, *available at* http://www.legalaffairs.org/issues/January-February-2006/feature_ goldsmith_janfeb06.msp.

7. *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213 (2003–04).

8. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003); Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. REV. 323 (2003); Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001); Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 359 (2003); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395 (2000); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1 (1996).

9. The term "Web 2.0" was coined by eminent technologist and writer Tim O'Reilly. *See* Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

10. *See* Zittrain, *supra* note 3, at 659.

11. *See id.*

Communications Decency Act of 1996,[12] which sought (unsuccessfully) to stop the transmission of pornography to minors, and the CAN-SPAM Act of 2003,[13] which (at least somewhat successfully) disallows the sending of unsolicited commercial e-mails if certain rules are not followed.

Second, states have banned the possession, or receipt, of the information enclosed in data packets, such as child pornography or copyrighted works.[14] Third, some regulations mandate that certain packets be accompanied by specific information in order to be sent or received. CAN-SPAM is again an example of this type of regulation. CAN-SPAM requires that certain header information is included in some messages.[15] Also, the Children's Online Privacy Protection Act of 1998 (COPPA)[16] requires that web sites verify that users are over thirteen years of age before providing most online services. None of these first three approaches necessarily represent a substantial departure from the end-to-end principle, so long as no intermediaries, such as Internet service providers (ISPs), are required to take any action on behalf of the state to enforce the rules.

The second cluster involves state-mandated controls at the middle of the network. These other two primary strategies, described below, represent a greater impingement on the end-to-end principle. Each is more sophisticated from a regulatory perspective and, many argue, more likely in the near-term to be effective at achieving its stated goals. In the first strategy of this type, states prompt private parties to block or listen in on packets as they pass.[17] Ordinarily, an ISP—whether serving the source or the destination of the packet—bears this burden, almost always without direct compensation.[18] Examples of such "unfunded mandates" are the takedown provisions in section

12. 47 U.S.C. § 223 (2000).

13. 15 U.S.C. § 7701 (2000); *see also* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 5 (2005).

14. *See* Zittrain, *supra* note 3, at 659, 671–72.

15. 15 U.S.C. §§ 7704–05 (2000).

16. *Id.* §§ 6501–06.

17. *See* Zittrain, *supra* note 3, at 664–76.

18. There is no provision in U.S. federal law to compensate ISPs for most of the basic monitoring tasks required of them, such as responding to routine police requests for information regarding subscribers.

512 of the Digital Millennium Copyright Act, under which the United States federal government requires ISPs and other service providers to filter packets as they flow through the network.[19]

In the second strategy, the state itself plays a direct role in filtering and reviewing packets as they pass.[20] For example, libraries play such a role to protect minors from potentially harmful online content, as required by the Children's Internet Protection Act of 2000 (CIPA).[21] While rare as an approach, some countries, such as Saudi Arabia and Burma, place an apparatus of government at or near a single point of control on the network and exercise the state's will at that aperture, as research by the OpenNet Initiative has demonstrated.[22]

This Article concludes that regulatory approaches of this second sort—whereby the state either requires an intermediary to filter packets or the state itself takes on the job of filtering—are likely to continue to be prominent, as approaches of the first sort fail to get the job done effectively when it comes to the thorniest of online problems.[23] Courts are unlikely to stand in the way of such a trend. The state action involved in the first cluster of regulations is no less clear than in the second. Further, the negative impact on the technologists' network design is not a factor in the analysis. The regulations of the second cluster are more likely, absent changes in social norms and enforcement practices, to achieve the goals driving the state action. In other countries, such as China, where constitutional protection of free expression is less strong, or at least less consistently upheld, the relative effectiveness of regulations placing control closer to the center of the network will likely lead to

19. 17 U.S.C. § 512 (2000).

20. This case is made broadly through the work of the OpenNet Initiative, a collaborative initiative that joins researchers from the University of Cambridge, the University of Toronto, and the Harvard Law School, which has documented Internet filtering worldwide. The principal investigators are Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. For the results of the research, see OpenNet Initiative, http://www.opennet.net/ (last visited Aug. 16, 2006).

21. *See* Zittrain, *supra* note 3, at 670; *see also* 114 Stat. 2763A-335.

22. *See* OPENNET INITIATIVE, INTERNET FILTERING IN SAUDI ARABIA IN 2004 (2004), http://www.opennetinitiative.net/saudi/; OPENNET INITIATIVE, INTERNET FILTERING IN BURMA IN 2005 (2005), http://www.opennetinitiative.net/burma/.

23. Joel Reidenberg came to a similar conclusion. "The essay maintains that states will increasingly try to use network intermediaries such as payment systems and Internet Service Providers (ISPs) as enforcement instruments." Reidenberg, *supra* note 7, at 216.

more approaches of this kind, especially as the importance of the Internet continues to grow and problems take on higher potential consequences. Absent a strong argument to the contrary, or effective action by a legislature to give "net neutrality," a cousin of the end-to-end principle, the force of law, this trend toward control of the middle of the network—tying private actors into the web of those who must exercise control—is likely to continue.

From the vantage point of some participants, there is reason to consider such a trend to be a positive one. As a matter of international governance, approaches that involve asserting authority over fewer points of control—as when control is stationed only at the intermediaries through which packets must flow—rather than at billions of end-points are more likely to enable efficiency and international coordination of enforcement. The primary benefit of such a trend is that, barring approaches that would require a wholesale change in user behavior, those who seek to enforce the laws related to Internet matters are more likely to be effective through the assertion of control at intermediate points in the network.[24] The fear that the Internet can devolve into a haven for lawless behavior if left untended—for instance, a thriving market in money-laundering, illicit gambling, and child pornography—might be allayed.[25]

However, there are several substantial costs likely to stem from such a trend. First, the end-to-end principle—both as a matter of effective network design and of ancillary benefits it has introduced—has served global society well and should not lightly be discarded as a strong preference.[26] The end-to-end principle per se has no legal

24. *See* Zittrain, *supra* note 3, at 669, 673, 682–84.

25. *See* R.S. Rosenberg, *Controlling Access to the Internet: The Role of Filtering*, *in* ETHICS AND INFORMATION TECHNOLOGY 35 (2001). In some contexts, there is a strong argument to be made that the Internet community can govern itself effectively through the peer-production of Internet governance. *See, e.g.*, David R. Johnson et al., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004).

26. A parallel argument is made in an amicus curiae brief filed by Professor William W. Fisher III et al. with the Supreme Court in the case of *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd*. *See* Brief of Amici Curiae Internet Law Faculty in Support of Respondents, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005) (No. 04-480), 2005 WL 508098 (arguing that the so-called *Sony-Betamax* standard, which shields the makers of dual-use technologies from copyright infringement lawsuits, should be preserved despite the fact that some third-parties use these technologies to break the law).

force, and therefore is unlikely to be defensible, other than rhetorically or insofar as it aligns with other rights, such as speech and privacy, upon judicial review.

Second, the switch toward intermediaries inquiring into passing packets may encourage them to make further efforts to control what travels through the network, beyond that which the state mandates, to ensure compliance with the state's rules.[27] The costs of such interference include higher transaction costs, borne initially by the ISPs but likely passed on to consumers or partners in the value chain, and further potential encroachment on civil liberties—carried out by private actors at the behest of states or by states directly. In the hands of private actors, initially prodded by states but later no longer meeting the state action threshold, fewer safeguards exist to protect the speech rights of citizens.

Finally, the change may affect the current character of the Internet—a global, unitary conglomeration of networks—leading to a balkanized series of smaller networks ringed by national, regional, or other geographic borders. While some might cheer such an outcome, the possibilities of cross-cultural understanding, reconnection of diasporan populations, gains in international commerce, and the "generativity" that Jonathan Zittrain celebrates may be less fully realized over time as a result.[28]

II. A HANDFUL OF PROBLEMS IN CYBERSPACE

The rapid rise in popularity of the Internet has spawned a series of problems that are different in kind from problems that existed beforehand. Four cases of "harmful" online speech frame the general problem giving rise to this inquiry. The general problem is the tension between the desirability of the end-to-end principle and the desire to regulate certain behavior online. These problems, with fact patterns that bleed across each other's borders, cover a series of

27. *See* Zittrain, *supra* note 3, at 685–87.

28. Jonathan Zittrain, *The Generative Intent*, 119 HARV. L. REV. 1974, 1980–93 (2006) (arguing that "Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences" and contending that generative computers and a generative network, the focus of this Article, are desirable but can also lead to unanticipated problems).

topics—sex, commerce, culture, and politics—and span the short history of the Internet. Consider the following four scenarios: the child pornographer peddling his wares over the Internet, the spammer paid by a stock-trading firm to peddle a penny stock hoping to pump-and-dump it to millions of prospective investors, the young remix artist with a hard-drive full of copyrighted music files, and the human rights activist using the Internet to organize on an unpopular topic in a repressive regime, such as in Burma or China.[29]

A. Sex

The original problems in the mid-1990s that gave rise to control over the Internet mostly dealt with offensive images, such as pornography, or text, such as hate speech.[30] Child pornographers found the Internet to be an easy way to share images, and also found it easier to hide online than in real space.[31] A pornographer who had made his early fortune in the hard-copy (and hard-core) magazine

29. With respect to the interactions between human users and internet architecture, we adopt a participation-centered approach, rather than a technology-centered one. Our inquiry is focused on the human component of speech on the web. For these purposes, the essence of the net is a set of nodes and conduits. Conceptualized this way, a node in the network can be: an end user who sends information directly to another user (e.g., a user who sends an email), a user who posts information online with the intention that the information be accessible to other users (e.g., a website operator), a recipient of a directed communication (e.g., an email recipient), or a user who surfs accessible websites. By conduit, we mean the points along the route that the information travels, which are regulated by any intermediary other than the party responsible for posting or sending the content, or the intended recipient. This node/conduit conception of the network paints the Internet in the broadest of brush strokes, and is misleading in its simplicity. All the same, this conceptualization is useful for two reasons. First, a participation-centered approach situates the analysis in terms of practical burdens on free expression. The Internet itself is not speech, and computer terminals at the end points of the network are not speakers. The Internet is a conduit for speech, a medium. It is true that electronic transmissions will undertake an intricate series of hops as they maneuver through and along the various layers of the net. Yet, what matters is whether a human speaker could speak, and whether a willing listener could hear that voice. A participation-centered approach puts the focus where it should be for First Amendment purposes: whether, as a practical matter, speech actually travels from end-to-end—that is, from speaker to recipient. Second, this broad categorization is useful because it highlights a problematic trend: over the last decade, attempts to control the network have moved from the nodes to third-party intermediaries in the middle of the network.

30. *See, e.g.*, Reno v. ACLU, 521 U.S. 844 (1997).

31. Prepared Remarks of Attorney General Alberto R. Gonzalez at the National Center for Missing and Exploited Children, Apr. 20, 2006, *available at* http://www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html.

business would quickly find that the Internet offered much fatter margins.[32] The images he posted online, some accessible for free and some for a fee, could be accessed by minors anywhere that the network reached, whether in the heartland of America or in a Muslim state in the Middle East. Likewise, a troubled undergraduate found a home on the Internet, and an all-too-ready audience, for his lurid musings about what he would like to do to a young woman in his class.[33]

These problems persist online today, only now they are better understood, more widespread, and more complex than they were during the earlier iterations of the Internet. This is due to changes in scale and social norms. Solutions adopted to address problems such as these vary widely across the world. However, most attempts to regulate sexually-charged speech of this sort have sought to regulate the end-points of the network—either by punishing the sender or the receiver of the data after the transmission has occurred.[34]

B. Commerce

The Internet, initially used for government and academic purposes, quickly became a powerful commercial medium. Its promise of serving as a series of low-friction marketplaces became obvious by the end of the 1990s. The network itself has become a "trade route" of unprecedented proportions, complete with checkpoints.[35] Rather than picking up the phone to do business, commercial actors began to rely on e-mail—the first "killer app"—as a preferred means of reaching customers, suppliers, and business partners.[36] Legitimate commercial e-mail generated high returns on

32. It is widely known that online publication is less costly to produce than traditional publications because the cost of printing and physical distribution is eliminated in the online context and most text and images are now initially created in digital format.

33. The most famous case of this sort is the Jake Baker matter. *See* Electronic Frontier Foundation's "Legal Cases-Jake Baker, the U. of Michigan, & the FBI" Archive, http://www.eff.org/legal/cases/Baker_UMich_ case/ (last visited May 16, 2006) (chronicling the matter).

34. *See supra* Part III.A.2.

35. ROLAND L. TROPE & GREGORY E. UPCHURCH, CHECKPOINTS IN CYBERSPACE: BEST PRACTICES TO AVERT LIABILITY IN CROSS-BORDER TRANSACTIONS (2005).

36. JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 7 (2005) (noting the ubiquity of e-mail, even

investment for marketers, in many cases at far lower costs than mail or telemarketing.[37] But for these purposes, consider the direct-marketing company that helps stock speculators tout penny stocks for little-known drug treatment companies. For a fee, these companies infect "zombie" computers and hijack them to send out millions of messages.[38] The unwanted messages, delivered to in-boxes around the world, promise that the penny stock will "soar" in the next few days.[39] The stock does in fact rise after the e-mail is sent, but only to plummet a few days later to a level below where it started, leaving only a few people, including the spammer, better off. However, many others are left holding the bag (in this case, filled with devalued stock).[40] A related set of problems, the security threats to the network often borne by spam and other means of dissemination, increase the potential damage of these activities.[41]

C. Culture

The most dramatic dispute regarding the Internet, at least in the United States, has been the culture war between the publishers of copyrighted materials and those who wish to copy, modify, or redistribute them, often without permission from or compensation to the creator.[42] This dispute over the control of digital media, most colorfully displayed by the public debates and lawsuits over peer-to-

---

ahead of search, as the most popular Internet application).

37. For the same reasons that online publication is cheaper than distributing printed publications, e-mail marketing saves printing and mailing costs to marketers who relied in the past on direct mail as a means of reaching customers. Telemarketing involves the expense of paid staff to call prospective customers, while e-mail requires far less in terms of human involvement, even when tailored to individual names and preferences.

38. The London Action Plan, a joint effort by anti-spam enforcement authorities, describes in detail efforts to decrease the threat of zombie bots. *See* The London Action Plan on International Spam Enforcement Cooperation, http://www.ftc.gov/os/2004/10/041012london actionplan.pdf (last visited May 16, 2006).

39. *See* Nat'l Ass'n of Securities Dealers, Stock Spams and Scams, http://www.nasd.com/web/idcplg?IdcService=SS_GET_PAGE&ssDocName=NASDW_006041 (last visited Aug. 16, 2006).

40. *Id.*

41. Zittrain, *supra* note 28 (establishing the threat of a technological disaster on a massive scale and its impact on policy-making).

42. *See generally* LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

peer file sharing of recorded movies and music, has resulted in calls for further regulation of Internet activities.[43] Just as the music recording and motion picture industries have sought to control the distribution and use of digital media through legal, technical, and market-oriented means, a community has developed supporting the notion that this revolution in digital media affords new opportunities for creativity, the furtherance of cross-cultural understanding, and new modes of money-making.[44]

A "free culture" movement has arisen, both on the Internet and in real-space, that seeks, in the words of Professor Lawrence Lessig, "a balance between anarchy and control" of digital content.[45] The key player in this movement is the young, expressive digital re-mix artist with a hard-drive, and probably a few iPods, full of digital sound recordings—some of which he has paid for, and some of which he has not. The fight over how he obtained those recordings and what he can, or ought to be able to, do with them—particularly online—continues unabated. Most relevant for this inquiry, the holders of copyrighted materials have asked for more extensive regulation as to how the re-mix artist and hundreds of millions of others may pass these packets over the network.[46] The parties best positioned to help the copyright holders, and in some cases the law enforcement officers, have been those who provide Internet access services to the would-be file-sharers.

D. Politics

Somewhat later in this short history, roughly in 2000 with the meteoric rise and fall of John McCain's presidential bid, the Internet became a powerful tool for those seeking to affect political change.

---

43. One of the many sources of information on this cultural debate is the weblog of Derek Slater. A Copyfighter's Musings, http://blogs.law.harvard.edu/cmusings/.

44. WILLIAM W. FISHER ET AL., CONTENT AND CONTROL: ASSESSING THE IMPACT OF POLICY CHOICES ON POTENTIAL ONLINE BUSINESSES IN THE MUSIC AND FILM INDUSTRIES (2005), *available at* http://cyber.law.harvard.edu/media/files/content_control.pdf.

45. LESSIG, *supra* note 42, at xvi.

46. The examples of this phenomenon over the past decade are many. A specific recent example is the INDUCE Act, a proposal to make it unlawful to induce others to violate copyright. Although Congress did not pass such a law, the Supreme Court, in *MGM v. Grokster*, 125 U.S. 686 (2005), effectively established such a standard through its ruling.

The most compelling cases for protecting the free flow of information online are derived from these sets of problems.

Consider the situation of a human rights activist operating in an Asian country known, among other things, for its mistrust of labor organizers. The activist seeks to share information about a campaign to improve the lives of low-wage hotel workers. The activist, after consulting with a college roommate who works in Silicon Valley, sets up a free weblog—an online, personal journal accessible to anyone located anywhere in the world.[47] The weblog is hosted by a prominent American technology company with a subsidiary based in this Asian country. For a few weeks, the activist posts stories about the poor treatment of hotel workers, takes and publishes photographs of striking workers, and offers free, globally accessible syndicated feeds of her writing and pictures. Her blog quickly becomes the hub of an online debate about the hotel industry. A month into her blog experiment, the service provider informs the activist by e-mail that her blog has been taken off the Internet and may not be restarted, her RSS ("Really Simple Syndication") feed silenced. When pressed, the blog-hosting company admits that a state official made plain to the company that the blog was to be taken off the Internet because it was a threat to state security.[48]

In each instance, the runaway success of the Internet as a cheap, effective international communication and distribution network has led to difficult problems. These problems give rise to state-driven solutions that, in turn, threaten network neutrality. Most of these threats to network neutrality bring with them threats—sometimes justified—to speech and privacy interests online.

III. MODES OF CONTROL

Despite the challenges of regulating the decentralized and global Internet, many countries have sought to exert control over the flow of packets on the network as soon as problems that seemed to implicate

47. *See* Dave Winer, What Makes a Weblog a Weblog, http://blogs.law.harvard.edu/whatMakesAWeblogAWeblog (last visited Oct. 15, 2006).

48. There are a number of stories that roughly fit this fact pattern. One example involved the Microsoft Corporation's MSN Spaces product. *See, e.g.*, David Barboza & Tom Zeller, Jr., *Microsoft Shuts Blog's Site After Complaints by Beijing*, N.Y. TIMES, Jan. 6, 2006, at C3.

public policy arose.[49] These regulatory efforts have taken five broad forms, falling into two large clusters. These five regulatory schemes are not crisply delineated, nor are they mutually exclusive in terms of their application to a certain public policy issue. The organization of this typology is meant to demonstrate a trend toward control at mid-points in the network. However, it is not meant to demonstrate that other modes of regulation are unusable or likely to be unused hereafter. The key point emerging from this typology is the general trend away from modes of regulation that are consonant with the end-to-end principle, towards modes of regulation that are not.

A. The First Wave of State Regulation: Control at the Nodes

It is worth noting, before getting into what has and has not been done with respect to regulating the Internet, that there are many modes of regulating the flow of packets online. Most famously, Lawrence Lessig argued that there are four primary modes of regulation: law, code, markets, and norms.[50] This theory has withstood a (short) test of time. Alternative institutions that achieve regulatory, or at least political force, also continue to emerge, as Yochai Benkler argued in multiple contexts.[51] This Article suggests that online regulation can take many forms as a starting point, but focuses on the specific approaches that countries have taken—the "law" mode—in regulating the flow of packets.

The first cluster of state-based regulatory approaches relies on controls at the end-points of the network. State entities have attempted to ban the transmission of certain types of information deemed as a matter of public policy to be harmful, to ban possession or intentional receipt of such information, and to mandate that some packets be accompanied by specific information in order to be sent or received. None of these three approaches represents a substantial departure from the end-to-end principle, so long as no intermediaries, such as the ISPs, are required to take action on behalf of the state to

49. This Article chronicles most of these efforts, of which the Communications Decency Act of 1996 is a prime early example.

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

51. YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006).

enforce the rules. When viewed chronologically, it is clear that they also represent the first wave of efforts to control the Internet. Although some of the court battles over these approaches have only recently ended, their legislative impetus was primarily a phenomenon of the mid- to late-1990s.[52]

1. Ban the Transmission of Packets at Their Source

The most common regulatory approach has been to ban the transmission of packets at their source—that is, to make it unlawful to send, or attempt to send, certain packets via the Internet.[53] The idea is to render illegal the act of sending packets that carry information deemed harmful to some segment of the public, primarily on the grounds that open access to the information embedded therein is harmful to the public interest.

The most notable of these efforts are the attempts to control access to sexually explicit materials. The year 1996 was a watershed for regulations of this sort. The Communications Decency Act (CDA),[54] part of the Telecommunications Act of 1996, included several such restrictions.[55] The CDA amended federal obscenity laws to ban the transmission of obscene materials using an "interactive computer service."[56] The CDA also amended the telecommunications laws to ban the transmission of "indecent" messages to minors.[57] Later that year, Congress made another major effort to control source transmissions with the Child Pornography Prevention Act (CPPA),[58] which banned the transmission of virtual child pornography.

The CDA provisions banning certain transmissions to minors and the CPPA were challenged on constitutional grounds shortly after

52. *See, e.g.*, Reno v. ACLU, 521 U.S. 844 (1997).

53. A variant of banning transmission of packets on the Internet is the regulation of broadcast transmissions in the traditional telecommunications context. *See, e.g.*, Derek Bambauer, *Shopping Badly: Cognitive Biases, Communications, and the Fallacy of the Marketplace of Ideas*, 77 U. COLO. L. REV. (forthcoming 2006) (discussing the regulation and the relationship of the state and intermediaries in this parallel context).

54. The CDA is codified in the Telecommunications Act of 1996, 47 U.S.C. § 223 (2000).

55. *Id.* § 223(a), (d).

56. *Id.* § 223(d)(1)(A)–(B).

57. *Id.* § 223(b)(2)(A).

58. 18 U.S.C. § 2256 (2000).

their passage.[59] The Supreme Court found both to be overbroad under the First Amendment—the CDA provisions in 1997,[60] and the CPPA in 2002.[61] After the Court overturned these provisions of the CDA, Congress passed the Child Online Protection Act (COPA) in 1998.[62] Although COPA's provisions were narrower than the CDA provisions they replaced, banning instead the commercial transmission of "harmful material" to minors, these too were eventually defeated by critics on the Supreme Court on First Amendment grounds.[63]

Outside the realm of pornography, there have also been a variety of other efforts to stop the transmission of packets at their source since the mid-1990s. The Food and Drug Administration (FDA), Federal Trade Commission (FTC), and Security Exchange Commission (SEC) have each adopted regulations for their respective domains that ban various source transmissions.[64] In the realm of copyright, Congress passed the No Electronic Theft (NET) Act in 1997 to address fears of widespread online digital piracy.[65] The NET Act established criminal penalties for willfully infringing upon copyrighted works by distributing them online, regardless of financial benefit.[66] In 2003, Congress passed the CAN-SPAM Act,[67] which prohibits a variety of spam transmission practices, such as false or deceptive subject lines, using a "dictionary attack"[68] to generate an e-mail address for spam transmissions, or using another computer as a spam relay without permission.[69] Most of the several dozen spam

59. For a chronology of *Reno v. ACLU*, 521 U.S. 844 (1997), which brought this challenge, see Electronic Frontier Foundation, EFF, ACLU et al. v. Dept. of Justice (ACLU v. Reno), http://www.eff.org/legal/cases/EFF_ACLU_v_DoJ/ (last visited May 16, 2006).

60. *Reno*, 521 U.S. 844.

61. Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002).

62. 47 U.S.C. § 231 (1998).

63. Ashcroft v. ACLU, 542 U.S. 656 (2004).

64. *See* Zittrain, *supra* note 3, at 660.

65. 17 U.S.C. §§ 101, 506, 507 (2000); 18 U.S.C. §§ 2319, 2319A, 2320 (1997).

66. *Id.*

67. 15 U.S.C. §§ 7701–13 (2003).

68. A dictionary attack is a method used both by spammers and by those seeking to break encryption schemes by trying every word in the dictionary as a possible password or e-mail handle. *See* http://www.webopedia.com/TERM/D/dictionary_attack.html (last visited Aug. 16, 2006).

69. Alternative modes of blocking spam, which rely far less on the role of the state but rather on the collective action of individuals, are considered alongside the merits and demerits

laws around the world ban the sending of unsolicited commercial e-mail if certain criteria are not met.[70]

2. Ban the Possession or Receipt of Packets

The second form of regulation in the first cluster—banning the possession or receipt of certain messages—is the obvious counterpart to banning the distribution of certain information in Internet protocol-based packets. The most notable examples of this sort are combined with other regulatory efforts. For example, in addition to the provisions regarding dissemination, the CDA also amended the federal obscenity laws to prohibit the receipt of obscene materials using an "interactive computer service."[71] The CPPA also included a ban on the possession of virtual child pornography.[72]

3. Place Encumbrances on the Flow of Information in Packets

The third form of control at the end-points includes mandates that messages be accompanied by certain additional information in order to be sent or received in packets traveling over the Internet. This mode of regulation operates in more subtle fashion than the outright ban on dissemination, receipt, or possession of packets. These control measures are also generally coupled with other regulatory approaches, though not as intimately. Although these laws represent an encumbrance on free expression for both the senders and recipients, the laws implementing them have focused on senders.

COPA provisions provided affirmative defenses for restricting access to content with age verification technology or a credit card.[73] These provisions met prompt and stiff resistance on First Amendment

---

of state action. *See* Johnson, *supra* note 25.

70. *See* DEREK E. BAMBAUER ET AL., A COMPARATIVE ANALYSIS OF SPAM LAWS: THE QUEST FOR A MODEL LAW (2005), *available at* http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf (discussing the various types of spam regulation in place around the world).

71. 18 U.S.C. § 1462 (2000).

72. *Id.* § 2252A(a)(2).

73. *See* ACLU v. Ashcroft, 322 F.3d 240, 258–60 (3d Cir. 2003) (discussing such affirmative defenses as enacted by Congress).

grounds.[74] The Supreme Court ultimately held them to be constitutionally infirm.[75] In the related domain of e-mail messages, provisions of the CAN-SPAM Act render certain commercial e-mails permissible only insofar as they contain an opt-out mechanism, whereby a recipient can take herself off the mailing list, notification that the e-mail is an advertisement, and a valid postal address for the sender.[76]

None of the first cluster strategies represent a major departure from the end-to-end principle as described by Saltzer, Reed, and Clark. That is not to say that these approaches do not burden online communication, however; witness the fact that several examples of regulation of this sort have been deemed infirm on constitutional grounds because of the undue restrictions they would place on users' free expression rights.[77]

In a sense, however, the barriers these laws placed on expression while they were in force could never, alone, be completely effective at achieving their stated public policy goals. Although the potential chilling effect in some cases was severe, these forms of legal regulation were almost always surmountable by users themselves, whether or not the user's intentions were legally valid. The threat of legal enforcement, standing alone, cannot achieve the law's purpose in the online context. Frequently, the users who are carrying out the illicit acts will be outside the threat's jurisdictional reach and can ignore the law completely, while others within the jurisdictional reach will transmit nonetheless. Millions of Americans have shown this to be true in the peer-to-peer context. Spammers, too, have flouted the dozens of laws that plainly deem their actions to be unlawful. Perhaps the most notable commonality among these

74. The CDA was challenged soon after its passage. *See* Rose Aguilar, *Two More Challenges to CDA Filed*, C|NET NEWS, Apr. 30, 1996, http://news.com.com/2100-1023-210802.html.

75. Ashcroft v. ACLU, 124 U.S. 2783 (2004).

76. 15 U.S.C. § 7704(a) (2000).

77. For instance, the Communications Decency Act was struck down in *Reno v. ACLU*, 521 U.S. 844 (1997), while the Child Pornography Protection Act was struck down in *Ashcroft*, 124 U.S. 2783.

regulatory measures is that none has been particularly effective in meeting its stated public policy goals.[78]

B. The Second Wave of Control

The second cluster involves state-mandated controls at or closer to the middle of the network. The two primary strategies within this cluster represent a greater impingement on the end-to-end principle. Each is more sophisticated from a regulatory perspective and more likely in the near-term to be effective at achieving its stated goals. Strikingly, these efforts have enjoyed much greater constitutional success and have become increasingly prominent over the last ten years.[79] In other countries, the trend is even clearer.[80]

1. State Encouragement of Private Action to Block Packets

In the first strategy of this sort, countries prompt private parties to block packets as they pass. An early example is section 230 of the CDA, which survived constitutional scrutiny and provides immunity from civil suit by an end user to a third-party intermediary for "any action voluntarily taken in good faith to restrict access to or availability of material that the [intermediary] considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[81] This provision grants nearly carte blanche to third-party intermediaries who choose of their own accord

78. In many cases, the provisions were held to be constitutionally infirm. In other instances, where the law remains on the books, the net effect of the legislation has not been to solve the problem it was intended to solve. For instance, the CAN-SPAM Act has been widely derided as the "You Can Spam Act." Most reports suggest that the number of spam messages sent and received in the United States since enactment of the CAN-SPAM Act has continued to rise. Grant Gross, *CAN-SPAM Law Seen as Ineffective*, COMPUTERWORLD NETWORKING, Dec. 24, 2004, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=98559&pageNumber=1.

79. As compared to statutes such as the CDA and the CPPA, the control methods described in this cluster have been less frequently challenged and rarely, if ever, declared to be constitutionally infirm.

80. Consider the frequently updated map of state-mandated Internet control of the sort contemplated herein at http://opennet.net/map (last visited Aug. 16, 2006).

81. 47 U.S.C. § 230(c)(2)(A) (2000).

to block content that a user has made available online, without fear of exposure to civil liability relative to that user's claims.

Perhaps the most (in)famous example of this strategy—the notice and takedown provisions of the DMCA, codified in section 512—grants another type of immunity for similar activity in the context of intellectual property protection.[82] Under this provision, a third-party intermediary who blocks content after receiving notice from a copyright owner gains immunity from a copyright infringement suit by the copyright owner so long as it follows a series of statutorily-defined steps.[83]

The Communications Assistance for Law Enforcement Act (CALEA),[84] part of the Telecommunications Act of 1996, offers an example by which the U.S. prompts private actors to assist in the monitoring of packets, rather than the blocking of them, as they flow through the network.[85] CALEA dictates that a telecommunications carrier has a duty to cooperate in the interception of communications for law enforcement purposes.[86] In practical terms, businesses, universities and others are expected to install equipment in private networks that enables law enforcement officers to listen to Internet-based traffic, much as in the context of a wire-tap in the traditional telephone setting.[87]

2. Direct State Intervention

With the second type of control in this cluster, the state becomes actively involved in the blocking process, or some governmental entity itself blocks access to expression. Twists on this theme have involved using various state apparati to effect content blocking. Section 512(j) of the DMCA creates a process by which a court, under certain circumstances, can order a third-party intermediary to block content via an injunction. For example, a court can order a service provider to block access to a user's IP address, or order the

82. 17 U.S.C. § 512 (2000).
83. *Id.* § 512(c).
84. 47 U.S.C. § 1001 (2000).
85. *Id.* § 1002(a).
86. *Id.* § 1002(a)(3).
87. *Id.* §§ 1001–21.

removal of content posted by a user on the service provider's servers.[88]

Some state entities that are accessible by private citizens—notably libraries—have also decided on their own accord to block access to certain content by directly installing filtering software on their computers. For example, in 1997, the Board of Trustees of the Loudoun County Library in Virginia implemented this strategy as part of their sexual harassment policy. The Loudoun policy established, among other things, that "all library computers would be equipped with site-blocking software to block all sites displaying: (a) child pornography and obscene material; and (b) material deemed Harmful to Juveniles."[89] The unblocking of sites—an important factor, according to at least one Supreme Court Justice[90]—required a written request, review, and approval by library staff.

The Eastern District of Virginia deemed this direct blocking scheme to run afoul of the First Amendment.[91] The court first characterized library filtering as a "removal" decision based on content, rather than an "acquisition" decision, a distinction which, if reversed, otherwise might have saved the scheme.[92] The court determined that the library was a limited public forum, meaning that the content-based decision to limit speech was subject to strict scrutiny.[93] The Loudoun County filtering regime, not surprisingly, failed to pass muster under strict scrutiny in federal court.[94]

However, attempts to block in such a direct manner have since been enacted by Congress and upheld by the Supreme Court. In 2000, Congress passed the Children's Internet Protection Act (CIPA),[95]

88. 17 U.S.C. § 512(j).

89. Mainstream Loudon v. Bd. of Trustees, 24 F. Supp. 2d 552, 556 (E.D. Va. 1998).

90. Justice Kennedy, in his concurring opinion of *American Library Association*, the challenge to the constitutionality of the Children's Internet Protection Act, stated: "If, on the request of an adult user, a librarian will unblock filtered material or disable the Internet software filter without significant delay, there is little to this case." United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003) (Kennedy, J., concurring in the judgment). Justice Kennedy argued that if libraries did not unblock sites as requested by adult patrons, such a policy would give rise to a factual, "as-applied" challenge to the law in question. *Id.*

91. *Loudon*, 24 F. Supp. 2d 552.

92. *Id.* at 561.

93. *Id.* at 563.

94. *Id.* at 570.

95. 20 U.S.C. § 9134 (2000).

which combines both control strategies of the second cluster. At the national level, CIPA prevents public libraries from receiving federal funds for patron Internet access unless they install filtering software for pornography, obscenity, and other materials harmful to minors.[96] This regulation functions as a prod from one branch of government to another to block online expression between the nodes. As of January, 2005, approximately 59.5% of libraries had complied with CIPA, and 65% reported filtering at least some terminals.[97]

CIPA met with stiff constitutional resistance, but ultimately prevailed in the Supreme Court. According to the plurality opinion in *United States v. American Library Association*,[98] the federal government did not itself filter, but instead only exercised its spending power.[99] The question considered by the Court was whether libraries could filter in this manner in a way that was consonant with the First Amendment.[100] The Court held, narrowly, that implementing filtering software was analogous to a "selection" decision, and that full strict scrutiny was therefore not required.[101] Five Justices also agreed that concerns of over-blocking were dispelled because it was easy for library staff to disable the filtering software if needed.[102] Although a library using Loudoun's original blocking scheme would still be problematic, the Court offered clear guidance as to how libraries can block expression at a control point in the middle of the network in a manner that would pass muster under the First Amendment.

The Pennsylvania state legislature made a similar foray in 2002. In this third twist on state-mandated blocking, the Pennsylvania legislature granted the state Attorney General authority to obtain an order from a local court declaring that "probable cause" existed to block access to child pornography, as defined by the statute,

96. *Id.*

97. *See* Norman Oder, *Budget Report 2005-Tipping Point*, LIBRARYJOURNAL.COM, Jan. 15, 2005, http://www.libraryjournal.com/article/CA491143.html.

98. 539 U.S. 194 (2003).

99. *Id.* at 203.

100. *Id.* at 202–03.

101. *Id.* at 205–08, 216–17.

102. *Id.* at 208–09, 216–17. These five Justices arrived at the same conclusion as to the statute's constitutionality by various means, with Justice Breyer joining the plurality after asserting that heightened scrutiny should be applied to what is ultimately a "selection" matter.

accessible through an ISP's service.[103] The Attorney General could then direct the local ISP—a private sector third-party intermediary—to block access to child pornography from the middle of the network, subject to a criminal penalty for failing to do so.[104] Section 7622 of the Pennsylvania Criminal Code specifically provides:

> An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.[105]

Despite the glaring constitutional issues raised by the Pennsylvania statute, a year-and-a-half transpired before a constitutional challenge was filed in Pennsylvania district court.[106] By this time, opponents of the blocking statute had amassed evidence of over 1.5 million wrongly blocked sites.[107] The court reviewing the matter found two distinct First Amendment violations, as well as a violation of the dormant Commerce Clause. The court noted:

> Based on the evidence presented by the parties at trial, the Court concludes that, with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment. In addition, the procedures provided by the Act are insufficient to justify the prior restraint of material protected by the First Amendment and, given the current design of the Internet, the

103. 18 PA. CONS. STAT. § 7621-30 (2002).

104. For the most comprehensive review and analysis of the Pennsylvania legislation and court struggle, see generally Zittrain, *supra* note 3.

105. 18 PA CONS. STAT. § 7622 (2002).

106. For a timeline and extensive review of this matter, see Ctr. for Democracy & Tech., Pennsylvania Web Blocking, http://www.cdt.org/speech/pennwebblock/ (last visited May 16, 2006).

107. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 611 (E.D. Pa. 2004).

Act is unconstitutional under the dormant Commerce Clause because of its effect on interstate commerce.[108]

Although there are presently relatively few examples of blocking from the middle of the network in the United States, there has been a dramatic upswing of such efforts around the world during the last five years.[109] Most of these efforts are best characterized as Internet filtering, carried out either directly by states or via intermediaries, such as ISPs licensed by the state to provide Internet access to citizens.

IV. INCREASING CONTROL IN THE NETWORK: INTERNET FILTERING AND THE ROLE OF THE CORPORATION

The bloom is off the rose of the Internet. In the late-1990s, as Internet use grew rapidly in the United States and other highly developed countries, the mantra that less regulation is necessary to protect the growth of the network kept intermediaries from being regulated.[110] Much of the early legislation regulating Internet usage, such as section 230 of the CDA and section 512 of the DMCA, expressly exempted ISPs and certain other intermediaries from liability.[111] The primary argument prevailing in such debates was that the economic benefits to be derived from the growth of Internet commerce was sufficient to offset any injustice associated with preferential treatment of firms doing business or otherwise acting online.[112] This presumption in favor of a techno-libertarian approach to the regulation of Internet-based activity seems to have run its course, especially when considered from an international perspective.[113]

---

108. *Id.*

109. For a catalog of known, state-based Internet filtering regimes, see http://opennet.net/map (last visited Aug. 16, 2006).

110. Tim Clark, *Private Sector Should Lead Net*, C|NET NEWS, Oct. 28, 1997, http://news.com.com/Private+sector+should+lead+Net/2100-1017_3-204745.html (last visited Aug. 16, 2006).

111. The relevant provisions of the Communications Decency Act are found at 47 U.S.C. § 230 (2003). The relevant provisions of the Digital Millenium Copyright Act are found at 17 U.S.C. § 512 (2003).

112. *See* Clark, *supra* note 110.

113. Not all states fit this trend. Governments sometimes agree with the technologists who

Controls at the end-points of the network, whether voluntary or mandated by states, have not succeeded in purging the Internet of problems.[114] Alternative strategies—such as seeking peer production of Internet regulation, a more active market, or technical controls—have yet to work, or, more likely, to be fully pursued.[115] The net effect is that pressure to allow intermediaries, such as ISPs and e-commerce companies, to have a free ride in the interest of growing the network is no longer such a substantial political impulse, at least in the most developed nations.

The most persistent issues that give rise to regulation at the mid-points of the network relate to Internet security. The initial concerns to which online life gave rise, such as sexually explicit content, spam, and illicit trade of intellectual property, persist. New online threats—with scary names such as phishing, pharming, viruses, and network terrorism—have emerged at the front of the list.[116] More recently, politically subversive speech plays an increasingly important role in prompting state-based regulation on the grounds of national security.[117]

Internet filtering regimes, which block citizen access to certain sites on the Internet either directly or through intermediaries, are becoming more sophisticated and more commonplace around the world as the Internet becomes a greater means of communication, a forum for doing business, and a hotbed of political activism.[118] We are witnessing a cat-and-mouse game being played between states

---

prefer adherence to end-to-end principles. For instance, the general position of the Polish government is that, despite the ongoing problems related to the Internet (such as international digital divide, cyber crime, and intellectual property violations), "the unfettered exchange of information and free flow of ideas" is important to the development and guarantee of human rights. Michal Kleiber, Minister of Scientific Research & Info. Tech., Republic of Pol., Statement at the World Summit on the Information Society (Dec. 11, 2003), *available at* http://www.itu.int/wsis/geneva/coverage/statements/poland/pl.doc.

114. Spam is the simplest example. Despite dozens of laws at multiple levels of government, the spam problems continue to get worse, by nearly all accounts.

115. *See* Johnson, *supra* note 25.

116. Zittrain, *supra* note 28.

117. *See, e.g.*, OPENNET INITIATIVE, THE INTERNET AND ELECTIONS: THE 2006 PRESIDENTIAL ELECTION IN BELARUS (AND ITS IMPLICATIONS) 36 (2006), *available at* http://www.opennetinitiative.net/studies/belarus/ONI_Belarus_Country_Study.pdf (describing the legal, and potentially technical, Internet-related controls established on the grounds of state security).

118. The OpenNet Initiative, http://www.opennetinitiative.net/ (last visited Aug. 16, 2006).

seeking to control the information environment and citizens seeking to speak freely online. Filtering technologies, and how they are implemented, are becoming more sophisticated with each passing year.[119] In many places, there is also a corresponding increase in terms of the legal mechanisms of control and surveillance.[120]

The examples of China and Burma best tell this story of the increasing technological and legal sophistication of filtering and surveillance regimes. In China, the OpenNet Initiative's research from 2002 through 2005 shows a country that continues to find more and more effective ways to control online speech and track the movements of its citizens, even as technologies to evade these controls become more sophisticated as well.[121] Similarly, Burma, controlled by its army, appears to have gone from an open source technology (DansGuardian) to a proprietary one (Fortinet) in 2005.[122] Most indicators show that Burma's filtering regime, along with its legal regime, are growing more restrictive.[123]

A third example is Saudi Arabia, which has had a relatively transparent filtering regime for years that is narrowly tailored, mostly to pornography.[124] However, recent reports note that access to the entire set of blogs hosted on Blogger, a popular weblog hosting service, has been shut down—a step that plainly leads to over-inclusive blocking of speech that meets none of the state's criteria for censorship.[125]

Uzbekistan is a fourth example, in which the president has claimed publicly that the country does not have the resources to filter the Internet.[126] Nevertheless, the OpenNet Initiative's research shows

---

119. China is the most salient example of this trend. *See* OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004–2005: A COUNTRY STUDY (2005), *available at* http://www.opennetinitiative.net/china/.

120. *See id.*

121. *See id.*

122. *See* OPENNET INITIATIVE, INTERNET FILTERING IN BURMA IN 2005: A COUNTRY STUDY (2005), *available at* http://www.opennetinitiative.net/burma.

123. *See id.*

124. *See* OPENNET INITIATIVE, INTERNET FILTERING IN SAUDI ARABIA IN 2004 (2004), *available at* http://www.opennetinitiative.net/saudi/.

125. *See* Posting of Jemima Kiss to http://www.journalism.co.uk/news/story1539.shtml (Oct. 5, 2006).

126. The OpenNet Initiative has a draft report on Uzbekistan that has yet to be published (on file with author).

that Uzbekistan is likely the central Asian country with the most extensive filtering system, especially of political speech.[127]

Burma may be the canary in the mine. Burma demonstrates how a developing country that has an overall repressive ideology can extend that viewpoint to the information environment as its citizens come online. If the Internet in Burma is introduced as a restrictive environment in which one's actions are blocked and tracked by the state, the state has a much better chance of keeping a lid—at least for a while—on the Internet's democratizing potential.

Contrast Burma with Saudi Arabia, for instance, in which the state did not introduce the Internet until it developed the Internet Services Unit. This approach to filtering announced to the Saudi people that the state would censor the net, but also take suggestions as to how to block and unblock sites.[128] Many of the gatekeepers who run countries have recently turned away from allowing open environments to flourish online.[129] Instead, they seek to shape what citizens do and say online, in part by literally blocking sites, in part by encouraging or requiring intermediaries to block sites, and in part by creating a culture of fear through laws and social norms.[130]

Perhaps the trickiest ethical problem to emerge from this trend is the role of corporations, based in places such as the United States, in the filtering and surveillance regimes of other countries. The OpenNet Initiative's research shows that the technology developed by at least three United States companies is being used by other countries to block Internet access and potentially to listen in on their citizens' Internet activities.[131] Setting aside the particulars of which company's technologies are used in which regime, it is plain that this creates a lurking "Oppenheimer" problem, in which there is buried a

127. *Id.*

128. *See* Internet Services Unit, http://www.isu.net.sa/ (last visited May 16, 2006).

129. GOLDSMITH & WU, *supra* note 2.

130. The series of OpenNet Initiative research reports, *see* http://opennet.net, collectively make this case.

131. In most cases, such as in Burma, when researchers contacted the United States-based company, they refused to confirm or deny their involvement. The ONI researchers found other ways to demonstrate the involvement of these companies, such as finding that the Myanmar state has put out a web page talking about it, procuring a "block page" that citizens view when they seek to access a forbidden destination on the Internet that has hallmarks of Fortinet's system, and hearing from people on the ground that such a new system is being implemented.

complex set of ethical quandaries.[132] This problem becomes one step further removed when the United States company does not directly profit from making the filtering regime itself work.

In the case of content and service providers, such as Yahoo!, Microsoft, and others, who seek to compete in markets such as China, the question of whether and how to comply with the foreign state's rules—such as a requirement to turn over personal information of a journalist or to remove an allegedly subversive blog—remains vexing to the company's leadership. A third class of equipment companies—providers such as Cisco and Nortel Networks—are also brought into the act when their apparently general-use technologies, such as switches and routers, are used for Internet filtering and surveillance.[133] In the current environment, certain countries rely on private actors, often not based in their jurisdiction, to act in a manner that is inconsistent with the conception of freedom of expression in the private actors' home markets.[134]

United States courts and legislators show very little inclination to stand in the way of such a trend, either at home or abroad. Flexible filtering regimes, in which intermediaries are required to play a more active role in sorting which packets should pass, may well be more efficient in the constitutional sense than rules that ban certain activities at the nodes. As geo-location and other technical means of determining a person's online identity improves, these techniques by intermediaries will only become more effective at achieving their public policy goals. This will, in turn, strengthen their constitutional position.[135] Meanwhile, the end-to-end technological principle

132. *See* Derek Bambauer, *Cool Tools for Tyrants*, LEG. AFFAIRS, Jan.-Feb. 2006, *available at* http://www.legalaffairs.org/issues/January-February-2006/feature_bambauer_janfeb06.msp.

133. *See id.*; *see also* Nart Villeneuve, *Internet Censorship Explorer: Censorship Is in the Router*, June 3, 2005, http://ice.citizenlab.org/?p=113.

134. China, once again, is the most obvious example, insofar as the state's strategy relies heavily upon prompting private actors to carry out censorship and surveillance measures, which are well-documented. These measures have given rise to a series of public hearing in Congress in 2006 as well as the proposed Global Online Freedom Act of 2006, shares with the authors in draft form by the office of Congressman Christopher Smith. An unofficial version of the bill, as of February 14, 2006, has been posted to the Internet at http://rconversation.blogs.com/rconversation/files/SMITNJ_094_XML.pdf (last visited Aug. 16, 2006).

135. *See* Andrew Turner, *Geolocation by IP Address*, LINUX JOURNAL, Oct. 5, 2004, http://www.linuxjournal.com/article/7856.

continues to hold no sway in courts' analyses. Abroad, U.S. corporations seeking to compete in markets that filter and tap Internet conversations are conscripted without recourse to any appellate body or support from their home trade representatives. It may also be that the United States itself values the efficacy of turning to corporations as partners in the task of regulating activity online.[136]

V. DANGERS OF THE MOVE TO THE MIDDLE

A. Technical Innovation and Competition

To the extent that the trend in legal Internet regulation has moved away from regulation at the edges of the network and toward regulation that involves control closer to the center, the grip of the end-to-end principle as the dominant design feature of the Internet has been loosened, largely through law and policy. The arguments in favor of the end-to-end principle are well-developed in the legal and technical literature. The primary argument relates to innovation. For example, Lawrence Lessig and Mark Lemley argued:

> While the End-to-End design principle was first adopted for technical reasons, it has important social and competitive features as well. End-to-end expands the competitive horizon, by enabling a wider variety of applications to connect and use the network. An End-to-End network creates a maximally competitive environment for innovation.[137]

The basic ideas behind the hypertext mark-up language (HTML) and the World Wide Web were proposed on several occasions before they became a reality in the end-to-end environment.[138] Because of the open nature of the architecture, HTML emerged from the Internet

136. BATTELLE, *supra* note 36, at 13–14 (discussing the "interesting questions about privacy, security, and our relationship to government and corporations").

137. Written Ex Parte of Professor Mark A. Lemley and Professor Lawrence Lessig, *In re* Application for Consent to the Transfer of Control of Licenses MediaOne Group, Inc. to AT&T Corp., CS Docket No. 99-251, *available at* http://cyber.law.harvard.edu/works/lessig/filing/lem-les.doc.html.

138. Markus Fischer, *Introduction in HTML 3.2*, http://www.itb.uni-stuttgart.de/training/bioinformatics00/Session2.pdf (last visited Aug. 16, 2006) (discussing the origins of HTML at IBM in the 1960s).

backdrop and propagated at a wild rate without top-down coordination.[139] Similarly, the idea behind e-mail existed long before it blossomed as a social resource.[140] The end-to-end design helped to allow participants at the nodes to rapidly set up shop, improve existing e-mail applications, and begin sending messages. This fostered a network effect that made e-mail communication attractive as a general form of communication. More recently, the end-to-end design has continued to support the proliferation of an array of new technologies, such as peer-to-peer networks (P2P), Internet Relay Chat (IRC), and the syndication and aggregation technologies fueling Web 2.0.

B. Democratic Culture

Innovation has not been limited to technological underpinnings, however, as end-to-end design has also fostered cultural innovation on a grand scale. Cultural innovation requires much more than the development of new modalities of communication, such as wikis and VOIP, new cultural icons and fads, or new artistic genres. As Jack Balkin argued:

> Democracy is far more than a set of procedures for resolving disputes. It is a feature of social life and a form of social organization. Democratic ideals require a further commitment to democratic forms of social structure and social organization, a commitment to social as well as political equality. And the forces of democratization operate not only through regular elections, but through changes in institutions, practices, customs, mannerisms, speech, and dress. A 'democratic' culture, then, means much more than democracy as a form of self-governance. It means democracy as a form of social life in which unjust barriers of rank and privilege are dissolved, and in which ordinary people gain a greater say over the

139. *See* Replication and Caching Position Statement, http://www.w3.org/Propagation/Activity.html (last visited Aug. 16, 2006) (describing, in part, the means of propagation of HTML and related technologies in the 1990s).

140. A list of early Internet mail systems is included in RFC 808, Summary of Computer Mail Services Meeting, http://rfc.sunsite.dk/rfc/rfc808.html (last visited Aug. 16, 2006).

> institutions and practices that shape them and their futures. What makes a culture democratic, then, is not democratic *governance* but democratic *participation*. A democratic culture includes the institutions of representative democracy, but it also exists beyond them, and, indeed undergirds them. A democratic culture is the culture of a democratized society; a democratic culture is a participatory culture.[141]

In this passage and elsewhere, Balkin has argued that the purpose of free expression is to promote democratic culture, including both traditional democratic processes and semiotic democracy—collective participation in cultural meaning-making.[142] It is important in a society that values individual liberty and autonomy to include semiotic democracy in the equation for two key reasons. First, culture is an important source of identity. Democratic culture gives individuals a role in shaping the forces that produce them. Second, individual cultural innovators produce their own culture. They "exercise and perform their freedom and become the sort of people who are free. That freedom is something more than just choosing which cultural products to purchase and consume; the freedom to create is an active engagement with the world."[143] Balkin further argued that developments in digital technologies change democratic culture.[144] New digital technologies alter the social conditions for expression, producing new opportunities for democratic participation—both cultural and political expression—and for control.

Reconsider library filtering in the context of Balkin's view of democratic culture. The overblocking or underblocking of sites in a given filtering regime is a fact, well-established by the work of the OpenNet Initiative and demonstrated in court in a variety of filtering cases, among other venues.[145] Supporters of CIPA claim that

---

141. Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 35 (2004).

142. *Id.* at 33–35 n.56; *see also* BENKLER, *supra* note 51, at 15.

143. Balkin, *supra* note 141, at 35, 42–43.

144. *Id.* at 42–47.

145. *See, e.g.*, Benjamin Edelman, *Sites Blocked by Internet Filtering Programs*, http://cyber.law.harvard.edu/people/edelman/mul-v-us/ (last visited Aug. 16, 2006).

overblocking is a red herring.[146] For example, as Justice Kennedy opined in *American Library Association*, if a librarian could quickly unblock a site or disable the filtering software upon the request of an adult user, "there is little to this case."[147]

This apparently simple technical solution to a thorny social problem involves a series of questionable assumptions and ignores the cultural context of the use of the Internet in a public space. Consider the case most favorable to filtering software given current technology—that whenever something is blocked by filtering software, it will be flagged as blocked, thereby making the user aware of its status. This is not how all filtering software works, but all filtering software could likely be modified to function in this manner. In some cases, a user that enters a URL for a particular site, such as http://usembassy.state.gov (blocked by one software program because of the word "ass" embedded in the URL), will know that the hosted content is legitimate and should be unblocked.[148] However, a user who accesses a previously unknown, foreign, or vaguely identified site through a hyperlink or search result will not have such knowledge.

Justice Kennedy's apparently simple solution to the library filtering problem assumes too much. It assumes that the user has expert knowledge—legal knowledge that it is appropriate or even possible for filtering software to be deactivated and technological knowledge that filtering software and the libraries that utilize it are fallible (i.e., that a site might have been wrongly included in a list of blocked sites). Moreover, Justice Kennedy's solution ignores the role of normative pressure on the individual. A library patron who wishes to have the blocking technology deactivated must resist the normative pressure to comply with the authority that imposes the technology; she must also be willing to take the social risk of deactivating software intended to block only obscenity. She must gamble that the unknown site that she wishes to unblock does not contain harmful

146. United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 209 (2003) (citing the Solicitor General's argument rebutting the critique of CIPA on overblocking grounds).

147. *Id.* at 196.

148. *See* Open Net Initiative Advisory 001, Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran, http://opennetinitiative.net/advisories/001/ (last visited May 16, 2006).

content to which she does not want to be exposed, or which would embarrass her if displayed at a public terminal.[149]

The upshot is that unknown numbers of library Internet users, in some cases individuals who do not have sufficient resources to gain Internet access in any other way, are denied an equal opportunity to participate in democratic culture. This harm flows directly from the impingement of the end-to-end principle because third party intermediaries place barriers between participants at the nodes. A democratic society may decide that this cost is acceptable in light of the benefits derived from the blocking regime—in Justice Kennedy's words, "[t]he interest in protecting young library users from material inappropriate for minors is legitimate, and even compelling, as all Members of the Court appear to agree"[150]—but the cost should be acknowledged and fully calculated into the equation.[151]

C. Semiotic Oligarchy?

The harms that result from impingement of the end-to-end principle extend beyond a straightforward reduction of opportunities for individuals to participate fully in a democratic culture. Moving away from the end-to-end principle also facilitates semiotic "oligarchy," presuming that it is the alternative to semiotic democracy. In the copyright context, William W. Fisher III argued that because the copyrights that cover a substantial portion of our society's cultural products are in the hands of a relatively modest number of large corporations, these corporations are positioned to assert control over public participation involving the copyrighted material.[152] Moving away from the end-to-end principle becomes another mechanism by which this transfer of cultural power can take place. By moving control of the network from the nodes to the conduits, third parties gain the ability to control content at the

149. By way of rebuttal to this argument, the plurality opinion noted that "the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment." *Am. Library*, 539 U.S. at 209.

150. *Id.* at 196.

151. *Id.*

152. WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT (2004).

expense of democratic values. The institutionalization of private prejudices about what is permissible for the public to view, in the library filtering context, is one subtle example of how moving away from the end-to-end principle facilitates semiotic oligarchy.

The DMCA's notice and takedown provisions present another example. Both the notice and takedown and injunction provisions of the DMCA result in situations in which third party intermediaries are positioned to block information in the space between users at the nodes.[153] The former involves a nudge from the state that gets the ball rolling; the latter pushes with a court order. In situations involving duplicates of copyrighted material, such as mp3-encoded music files, the cultural effect of this departure from end-to-end is intentional—the point is to allow copyright owners to control access to their works. However, as with other departures, this purpose brings with it unintended consequences.

First, the corpus of copyright law covering highly transformative derivative works, parody, and fair use—cultural innovation instead of simple copying—is far from clear to most end users. While arguably a good idea as a general policy matter when all factors are weighed, this lack of clarity is bad from the perspective of encouraging creative re-use of digital materials. Second, media companies hold copyrights in a large number of important works that comprise a vast swath of the content found online. The owners of these copyrights believe that they have a strong economic incentive to protect their rights to the full extent allowed by law and, in at least one case, beyond.[154] As a result, the parties at the other end of the barrel have a strong incentive not to fight back. ISPs generally have no business interest in a privately created derivative work that would outweigh the risk of a lawsuit. Individual creators with a personal stake in their works will often lack the resources or savvy necessary to litigate. As a result, free expression is chilled and control over democratic culture is consolidated far beyond what those who drafted the law may have intended.

153. 17 U.S.C. § 512 (2003).

154. *See, e.g.*, Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

D. Many Internets, Less Cross-Cultural Understanding

A final harm that may result from this departure from the end-to-end principle is the development of a balkanized, fractured Internet. The development of a China Wide Web, a Saudi Wide Web, an Uzbek Wide Web, and so forth may protect certain cultural values, but stunt the growth of others. The power of the Internet to foster cross-cultural understanding at extremely low cost may be sacrificed. The collaborative, international establishment of semiotic democracy—the promise of which is expressed both via large-scale experiments, such as Wikipedia, and small-scale trading of mash-ups via e-mail or BitTorrent—is far less likely to come to fruition.

VI. CONCLUSION

Technological innovation, participatory democracy, cultural development, generativity, and other wonderful things could no doubt continue to develop without the Internet. These interests can plausibly be vindicated in ways other than by upholding the end-to-end principle of network design. It would be a drastic overstatement to contend that any given incremental online legal control means the end of free expression on the Internet. A reasonable legislator or judge might find in favor of potentially more effective ways of solving the problems of online life—whether dealing with sex, commerce, culture, or politics—than with the benefits of end-to-end.

Information technology continues to evolve rapidly and to bring with it new and complicated puzzles. The job of the policy-maker, who must set rules in a time of such "quicksilver technological innovation," is challenging, if not unenviable.[155] In such a fast-moving environment, adherence to the end-to-end principle is a consistently safe bet. However, it is a bet that is not easily draped in language that has legal force, other than insofar as end-to-end solutions themselves tend to support and foster greater expression online. Jonathan Zittrain has forcefully argued that the better rhetorical framework may be to emphasize those technical designs—

155. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1174 (9th Cir. 2004).

and corresponding legal, market, and social designs—that favor generativity.[156]

If history is any guide, the preservation of an end-to-end network will mean the promotion of a flourishing democratic culture, potentially on a global scale—cultural innovation in an unusually rich, empowering sense that should be the goal of the policy-maker and technologist alike. The trend away from legal controls consistent with the end-to-end principle and toward those that block content from the middle of the network works against innovation, the development of democratic institutions, and the aspiration of semiotic democracy. In a particularly worrisome development, intermediaries—such as technology service and content providers—are increasingly being required to carry out some of the most egregious of these proprietary controls as a condition of competing in highly attractive emerging markets.

As the online regulatory environment continues to shift toward more control at intermediate points in the network, the job of the technologist must be to articulate better the aspects of the threatened network designer—whether translated as "net neutrality," "generativity" or other monikers—that must be preserved. The job of non-profits and universities, as Charles Nesson argued, is to express the power and the possibilities of the network in its least encumbered form.[157] The job of the legislator, the regulator, and the judge should be to listen carefully to the technologists and to determine how to preserve those essential elements of the end-to-end principle to protect the public interest.

The most difficult job may ultimately prove to be the challenge facing the technology company caught in the cross-hairs of state regulation. Their challenge, if one accepts their likely fate as the locus of state regulation, is to shape and adhere to a set of best practices for participating in markets in which repressive regimes mandate excessive proprietary control at mid-points in the network.

---

156. *See* Zittrain, *supra* note 28.

157. *See* Charles Nesson, *Eon: Law Professor Blogging*, http://cyber.law.harvard.edu/nesson/blog/?p=174 (last visited Aug. 16, 2006).