

COMMENT

WHAT MAKES THE INTERNET SO SPECIAL? AND WHY, WHERE, HOW, AND BY WHOM SHOULD ITS CONTENT BE REGULATED?*

TABLE OF CONTENTS

I. INTRODUCTION.....	62
II. WHAT MAKES THE INTERNET SPECIAL?.....	64
III. WHY ALLOW CONTENT REGULATION IN THE FIRST PLACE?	67
IV. WHERE AND HOW IS CONTENT ON THE INTERNET REGULATED?.....	69
A. <i>Approaches to Internet Content Regulation</i>	70
1. <i>Regulating the Endpoints of the Network</i>	70
2. <i>Middle-of-the-Network Regulation</i>	71
3. <i>Current Legal Trends in Internet Content Regulation</i>	71
B. <i>Filtering: An Examination of Middle-of-the-Network Regulation</i>	72
1. <i>What Is Filtering and How Does It Work?</i>	72
2. <i>Positive Aspects of a Filtering Regime of Internet Content Regulation</i>	73
3. <i>Inherent Dangers of Filters</i>	74

* This Comment received the Jackson Walker LLP Award for the Best Paper in the Area of Media Law. The Author would like to thank his family and friends for their dedication and support—particularly his two sisters, Andrea and Jourdan, who are in his thoughts more than they could know. Thanks also to Professor Peter Linzer for his guidance and insight on earlier drafts of this Comment. Finally, thanks to the editors of the *Houston Law Review* for their tireless work.

V. IN WHOM SHOULD THE POWER TO REGULATE BE VESTED?78

A. *Congress’s Failed Attempts at Regulation*78

B. *Ceding the Task of Regulation to the ISPs: Section 230 of the Communications Decency Act of 1996*.....79

 1. *Objectives and Affirmation*80

 2. *Dangers of Section 230*82

C. *The State Action Doctrine*83

D. *The Negative Notion of First Amendment Freedoms*.....86

E. *ISPs: Publishers or Common Carriers?*87

VI. DANGERS OF THE “FREE MARKET” MODEL OF INTERNET CONTENT REGULATION89

A. *Direct Censorship*90

B. *Media Concentration and Lack of Meaningful Choice*92

C. *Profit Maximizing and Indirect Censorship*.....93

VII. SUGGESTIONS FOR A FREER INTERNET: APPLYING OUR MODEL OF INTERNET FREEDOM TOWARDS A SYSTEM OF USER-CONTROLLED INTERNET REGULATION.....96

A. *Prohibiting Private Censorship*96

B. *Allowing Civil Liability for Private Censorship*98

C. *Developing Technology and Educating End Users*98

D. *Addressing the Concerns of the ISPs*100

E. *Summary*.....101

VIII. CONCLUSION101

I. INTRODUCTION

In the wake of the rapid technological advancements of the past two decades, the Internet has emerged as the ultimate forum for public expression. Hailed as “the most participatory form of mass speech yet developed,”¹ the Internet’s potential to promote freedom of expression on a grand scale has been recognized since its inception. The Internet gives individuals the opportunity to broadcast their ideas to anybody willing to listen on a level far greater than at any other time in history. On the

1. *ACLU v. Reno (Reno I)*, 929 F. Supp. 824, 883 (E.D. Pa. 1996) (Dalzell, J., concurring).

flipside, anyone with a computer and an Internet connection has an unlimited wealth of information and ideas at his or her fingertips, a mere point and click away.

Vast and complex constitutional issues necessarily accompany these developments. The Framers of our Constitution clearly held dear the notion of freedom to express oneself publicly.² However, they could not possibly have foreseen innovations of this breadth and magnitude. This Comment focuses on the constitutional implications of regulating content on the Internet and the inherent dangers in various methods of regulating Internet content—both proposed and implemented. The Comment does not stress highly complicated technical considerations, but instead discusses the potential ramifications of these systems of regulation from a practical standpoint and suggests improvements to the current system.³

Beginning in the mid-1990s, Congress launched a series of legislative attempts to restrict access to Internet content in a variety of ways. In a succession of corresponding cases, however, the Supreme Court systematically struck down these statutes as unconstitutional under the First Amendment.⁴ In the wake of these cases, and perhaps recognizing the blatant unconstitutionality of government-imposed, content-based regulations, Congress sought to achieve its regulatory goals in a more indirect way. Essentially, through section 230 of the Communications Decency Act of 1996 (CDA)—which has survived constitutional scrutiny—Congress granted Internet service providers (ISPs) *carte blanche* to regulate as they see fit.⁵

2. See U.S. CONST. amend. I (“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”). For more on the Framers’ intent in enacting the First Amendment, see generally Stanley C. Brubaker, *Original Intent and Freedom of Speech and Press*, in *THE BILL OF RIGHTS: ORIGINAL MEANING AND CURRENT UNDERSTANDING* 82 (Eugene W. Hickok, Jr. ed., 1991).

3. See John G. Palfrey, Jr. & Robert Rogoyski, *The Move to the Middle: The Enduring Threat of “Harmful” Speech to the End-to-End Principle*, 21 WASH. U. J.L. & POL’Y 31, 38 n.29 (2006) (explaining that such a participation-centered, rather than technology-centered, approach to Internet discussion, while simplistic, is nevertheless conceptually useful). The purpose of this Comment is not to examine the intricacies of the various topics presented herein, many of which are unfortunately beyond its scope. Rather, the Comment seeks to alert the reader as to the existence of these issues from a broad, big picture standpoint. For a more technical discussion of these issues, see generally Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-To-End Debate*, 3 J. ON TELECOMM. & HIGH TECH. L. 23 (2004).

4. See *infra* Part V.A (analyzing congressional attempts to regulate Internet content).

5. See *infra* Part V.B (scrutinizing the Communications Decency Act of 1996

Given the endless possibilities for truly participatory expression that the Internet facilitates, however, this “free market” model of Internet content regulation is highly undesirable. Such an extraordinary concentration of power in the hands of such a small number of corporations poses an enormous risk for potential abuse. Regulatory abuses may manifest themselves in various ways, stemming from the lack of meaningful choice associated with Internet access and ranging from direct censorship to discrete, indirect censorship in the name of corporate profit maximization. Such disregard for the Internet’s capacity for promoting freedom of speech is patently inimical to the values embodied in the First Amendment. Therefore, the government should take a proactive role in promoting free expression by encouraging the development and implementation of transparent, user-controlled filtration software and by taking steps to expand public awareness of and involvement in these issues.

Part II of this Comment shows what makes the Internet a unique medium of expression deserving special protection from outside forces, both public and private. Part III explains why regulation, a notion that seems counterintuitive to the ideals of free expression embodied in the traditional concept of the Internet, nevertheless proves necessary in certain, albeit limited, circumstances. Part IV discusses the most important methods of regulation that have been implemented, and how they should be manipulated in order to best promote the values of freedom of expression protected by the First Amendment. Part V examines the extent to which various entities have been, and should continue to be, permitted to exercise control over these technologies. Part VI evaluates various dangers associated with the current regulatory scheme, and Part VII suggests potential improvements. Part VIII concludes this Comment.

II. WHAT MAKES THE INTERNET SPECIAL?

Since its inception, the Internet has been recognized as “the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen.”⁶ For the first time in history, nearly anyone can both have his or her voice heard by

(CDA), 47 U.S.C. § 230(c)(2)(A) (1996)).

6. *ACLU v. Reno (Reno I)*, 929 F. Supp. 824, 881 (E.D. Pa. 1996) (Dalzell, J., concurring).

2009] *WHAT MAKES THE INTERNET SPECIAL?* 65

an enormous audience and listen to the speech of millions of other individuals worldwide.⁷ Indeed,

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.”⁸

This participatory nature of the Internet is what makes it special and sets it apart from any other form of communication to come before it.

The potential for participation has only become more real as time has passed and developments have occurred. As web design software becomes more user friendly, it becomes easier for average individuals to design and host their own space on the web, allowing them to get their message—whatever that message may be—out to the world. Other recent developments, such as blogging and YouTube, make it even easier for individuals to express themselves, either in written or video format, to a massive audience.⁹ Similarly, user interfaces such as MySpace allow little-known musicians to be heard on a level that never would have been imaginable previously in the music industry, which until recently was dominated by large record labels.¹⁰ Social networking sites such as Facebook likewise provide a quick and easy way to stay in touch with friends across the globe.¹¹ Furthermore, Internet search engines have rapidly become the simplest, fastest, and most effective means of obtaining a seemingly limitless wealth of information.¹² E-mail represents yet another example of the Internet’s capacity as a

7. See 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, 3 (2004) (crediting the digital revolution with facilitating “widespread cultural participation and interaction that previously could not have existed on the same scale”).

8. *Reno v. ACLU (Reno II)*, 521 U.S. 844, 870 (1997) (quoting *Reno I*, 929 F. Supp. at 842).

9. See, e.g., YouTube, <http://www.youtube.com> (last visited Mar. 6, 2009) (allowing users to post and view streaming videos).

10. *The Internet: The Biggest Revolution in Music Since Punk?*, INTERNET ADVERTISING BUREAU, Mar. 9, 2006, <http://www.iabuk.net/en/1/na2006q1musicandmyspace.mxs>.

11. Facebook, <http://www.facebook.com> (last visited Mar. 6, 2009) (“Facebook helps you connect and share with the people in your life.”).

12. See Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 436–37 (2000) (“The Internet’s central value lies in providing a wealth of information in a fraction of the time that would be required to obtain the information offline.”); see also *infra* note 161 (noting the extensive power wielded by Google, the current leader in Internet search engines).

forum for the expression and exchange of ideas; indeed, the overall volume of e-mail has already far surpassed that of traditional “snail” mail.¹³ Truly, the variety of uses and the potency of the Internet as a form of mass communication are almost unlimited.

The extensive possibilities for participation created by the Internet arise from several factors that distinguish it from traditional media. The low cost of entry, lack of access barriers, and virtually limitless space on the Internet are fundamentally important. The Internet “drastically reduce[s]” these limitations generally associated with traditional print publication and broadcast media.¹⁴ Furthermore, the reduced costs of copying and distributing new ideas, as well as commenting on, building upon, and altering existing information, serve to further democratize speech.¹⁵ These factors also make it easier for content to cross cultural and geographical borders via the Internet than through traditional forms of communication.¹⁶ The unique characteristics of the Internet make it the ideal forum for freedom of personal expression on an unprecedented scale.¹⁷

In essence, the Internet’s primary benefit stems from its power to “allow[] mass culture to be appropriated by ordinary citizens and become, more than ever before, a truly popular culture.”¹⁸ Ideally, freedom of speech requires allowing people to both say what they want to say and hear what they want to hear. The Internet facilitates both of these aspects of free speech. First, it increases opportunities for the widespread distribution of ideas by opening avenues for individuals to disseminate information to the general public. Second, it expands the scope and power of those ideas by making them more readily available to be found and received.¹⁹ As such, the Internet’s potential as a democratizing force is undeniable.²⁰ Indeed, the unfettered

13. Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1122 (2005).

14. *Id.* at 1120.

15. See Balkin, *supra* note 7, at 7–9 (discussing the impact of the digital revolution on freedom of expression on the Internet); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1975, 1980 (2006) (addressing the Internet in terms of generativity, which “denotes a technology’s overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences”).

16. Balkin, *supra* note 7, at 7–8.

17. See Nunziato, *supra* note 13, at 1120 (examining the features of the Internet that give it “the potential to facilitate a true marketplace of ideas” and contrasting this with traditional media “dominated by a few wealthy speakers”).

18. Balkin, *supra* note 7, at 41.

19. *Id.* at 45–46.

20. Palfrey & Rogoyski, *supra* note 3, at 56 (noting the “democratizing potential” of

exchange of ideas and information that the Internet can provide is vital to the development, spread, and guarantee of free speech and human rights on a global scale in the twenty-first century.²¹ It seems only natural that we, as citizens of a powerful democratic nation, should pay particular attention to and exercise extreme caution in allowing the regulation of content on the Internet.

III. WHY ALLOW CONTENT REGULATION IN THE FIRST PLACE?

Given the extraordinary potential for the Internet to promote the exchange of ideas and expand democratic principles on a global scale, one may wonder: Why permit any individual, group, agency, or government to regulate it at all? As with any powerful innovation, however, the Internet itself has great potential for abuse. Consequently, several situations exist in which its regulation is not only necessary, but also desirable.²² Four main areas have emerged that merit the regulation of content on the Internet.²³

First, every society has an interest in protecting its commonly held moral values.²⁴ Protecting minors from potentially harmful materials represents the most prominent example of this regulatory impulse.²⁵ Second, national security and other political interests often drive the enforcement of regulations.²⁶ In the

the Internet).

21. See Susan Crawford, *Internet Freedom Must Never be Taken for Granted*, DETROIT FREE PRESS, Sept. 25, 2007, available at <http://www.mail-archive.com/discuss@isoc-nyc.org/msg00371.html> ("Every day brings more evidence that the Internet can shed light on human rights abuses and dramatically lower barriers to political activism. . . . We must not take for granted all of the empowerment, economic growth, free speech, and other benefits the Internet makes possible.").

22. See Palfrey & Rogoyski, *supra* note 3, at 37–38 (discussing problems associated with "harmful" online speech).

23. Kevin O'Keefe, John Palfrey & Wendy Seltzer, *Internet Filtering in the United States and Canada*, in ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 226, 226 (Ronald Deibert et al. eds., 2008); Palfrey & Rogoyski, *supra* note 3, at 37–38.

24. See Palfrey & Rogoyski, *supra* note 3, at 38–39 (noting the original problems that gave rise to a need to regulate the Internet dealt primarily with "offensive images, such as pornography, or text, such as hate speech"). Of course, what amounts to "commonly held moral values" worthy of government intervention is far from uncontroversial. This is particularly true in a nation such as the United States that prides itself on racial, ethnic, religious, and cultural diversity. Furthermore, social mores change as society's shared beliefs evolve over time. Still, at some point the line must be drawn between permissible and unacceptable expression. The inevitable question of who should determine where to draw that line is addressed *infra* in Parts V–VII.

25. See O'Keefe et al., *supra* note 23, at 227–30 (identifying congressional attempts to protect minors from explicit content on the Internet).

26. *Id.* at 232; see also Palfrey & Rogoyski, *supra* note 3, at 41–42 (detailing how

United States, this often takes the form of surveillance as opposed to outright blocking or filtering.²⁷ However, because the Internet can be a powerful tool for affecting political change, the latter methods are not uncommon in countries with more authoritarian regimes where state sponsored content regulation is prevalent.²⁸ Third, the Internet is often regulated in the name of protecting the intellectual property of copyright holders from those wishing to copy, modify, or redistribute copyrighted materials.²⁹ An intellectual battle over the proper scope of regulation has developed in this area.³⁰ Finally, computer security and commercial concerns about unwanted messages (in various forms of spam) or viruses comprise a fourth category of Internet activity necessitating regulation.³¹

These four areas constitute recognized circumstances in which commentators deem regulation necessary to *prevent* the end user browsing the Web on his personal computer from accessing certain content.³² In other words, they represent the limited instances in which the restriction of content is acceptable. This Comment suggests another context in which a different species of regulation seems necessary. Specifically, it maintains

political activists can use the Internet and attract the attention of governments). See generally ULRICH SIEBER & PHILLIP W. BRUNST, *CYBERTERRORISM—THE USE OF THE INTERNET FOR TERRORIST PURPOSES* (2007).

27. See O'Keefe et al., *supra* note 23, at 232 (suggesting that the United States may be among the most aggressive and sophisticated states in the world in terms of Internet surveillance and listening to online conversations); see also Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1002 (2000) (requiring private telecommunications carriers to assist in the monitoring, rather than blocking, of communications as they flow through the network).

28. State censorship of political content in Asian countries known for their mistrust of dissidents is commonplace. For example, the governments of China and Vietnam regularly engage in "pervasive filtering as a central platform for shaping public knowledge, participation, and expression," commonly blocking topics "spanning human rights issues, reform and opposition activities, independent media and news, and discrimination against ethnic and religious minorities." Stephanie Wang, *Internet Filtering in Asia*, in *ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING*, *supra* note 23, at 155, 155.

29. Palfrey & Rogoyski, *supra* note 3, at 40; see also Balkin, *supra* note 7, at 13–18 (assessing the Internet's value as a means of facilitating access to and innovation based upon copyrighted material).

30. See generally Tim Wu, *On Copyright's Authorship Policy*, 2008 U. CHI. LEGAL F. 335 (2008) (examining the logically defensible claims to copyright ownership held by numerous entities—including authors, distributors, publishers, and networks—in the digital era).

31. See O'Keefe et al., *supra* note 23, at 232 (discussing congressional attempts to remedy security concerns); Palfrey & Rogoyski, *supra* note 3, at 40 ("[T]he security threats to the network often borne by spam and other means of dissemination[] increase the potential damage of these activities.").

32. See O'Keefe et al., *supra* note 23, at 226 (discussing a need for and strategies for regulating the four areas of problematic content on the Internet).

that federal policy should protect end users from unacceptable content restrictions that do not fall into one of these four narrow categories. That is, Congress should seek to *promote* universal access by *providing* the end user with the fullest access possible, prohibiting any entity from enacting regulations that would run afoul of the First Amendment if enacted by a government actor.

Unfortunately, Congress has thus far taken the exact opposite approach—with the full blessing of reviewing courts—granting almost total editorial *carte blanche* to the private business entities that control most of the Internet's infrastructure and provide access to individual users.³³ As discussed below, the current legal model of Internet regulation in the United States poses various dangers to freedom of expression on the Internet.³⁴ First, however, some background information on Internet regulation in general will enlighten the discussion to follow.

IV. WHERE AND HOW IS CONTENT ON THE INTERNET REGULATED?

In very general terms, the Internet consists of four primary components: the end user, the Internet service or access provider, the host or content provider, and the communication networks linking the first three.³⁵ The Internet itself is actually a cooperative collaboration of thousands of individual networks, most of which are privately managed and funded by companies such as ISPs. Private companies are also largely responsible for building and selling access to Internet backbones, the high-capacity lines that make up the physical infrastructure of the Internet through which information flows.³⁶

33. See CDA, 47 U.S.C. § 230(c)(2)(A) (2000) (providing immunity from liability for ISPs for “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be . . . objectionable, *whether or not such material is constitutionally protected*” (emphasis added)); see also *infra* Part V.B (discussing the implications of Section 230). The courts have followed suit by giving broad deference to the legislature's position. See, e.g., *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330–31 (4th Cir. 1997) (interpreting Section 230 as providing complete immunity from tort liability to an ISP for content posted on its service).

34. See *infra* Part V.B (describing the current legal model); *infra* Part VI (examining the dangers of this model).

35. PRESTON GRALLA, *HOW THE INTERNET WORKS* 21 (Millennium ed. 1999).

36. *Id.* at 5. All of the different computers linked to the Internet are able to communicate with each other thanks to a unifying set of conventions known as TCP/IP. Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering*, in *ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING*, *supra* note 23, at 57, 57. Transmission Control Protocol, or TCP, breaks data being transmitted from a content provider into small packets of information and later recombines those

The Internet has often been described in terms of the end-to-end (e2e) principle.³⁷ Under this theory, the Internet should function much like a common carrier, simply serving as a neutral conduit for information flowing from the content provider, or “speaker,” on one end to the end user receiving the information, or “listener,” on the other end.³⁸ The e2e principle dictates that all data packets, or bundles of information, should be treated equally as they pass through the middle of the network, regardless of their content.³⁹ Accordingly, e2e embodies a notion of the Internet that comports perfectly with its characterization as a participatory forum promoting First Amendment freedoms.⁴⁰ This principle, however, is simply a theoretical approach to conceptualizing the Internet, and is not backed by the force of law. Consequently, various methods of Internet content regulation have developed, which are not always consistent with the e2e principle.⁴¹

A. *Approaches to Internet Content Regulation*

There are two major classifications of the methods by which Internet content is regulated, which are distinguishable based upon the location on the Internet where the regulation occurs. In the first classification, content is blocked at the endpoints of the network. In the second, data packets are filtered or reviewed as they pass through the middle of the network itself.⁴² These two general classifications are examined in greater detail below, followed by an assessment of their practical applicability.

1. *Regulating the Endpoints of the Network.* The first classification consists of three distinct methods of regulation. In the first, regulators stop content deemed “harmful” at its source;

packets into comprehensible data when it is received by an end user. Internet Protocol, or IP, is the method by which information is routed across the Internet backbone from the host to the user. GRALLA, *supra* note 35, at 14. Specialized computers called routers are responsible for directing the data packets as they flow through the Internet from one end to the other. Murdoch & Anderson, *supra*, at 57.

37. See generally LAWRENCE LESSIG, CODE: VERSION 2.0, at 44–45 (2006) (explaining end-to-end theory); J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS COMPUTER SYS. 277 (1984) (proposing end-to-end theory).

38. See LESSIG, *supra* note 37, at 44–45.

39. *Id.*

40. See *supra* Part II (explaining the participatory potential of the Internet).

41. Palfrey & Rogoyski, *supra* note 3, at 36–37 (noting the “tension between the desirability of the end-to-end principle and the desire to regulate certain behavior online”).

42. *Id.* at 33–35.

in effect, Internet speakers are prevented from disseminating their message in the first place.⁴³ Exactly the opposite occurs in the second method, in which regulators ban the possession or receipt of certain kinds of information contained in the data packets; essentially, listeners are prohibited from receiving specific content.⁴⁴ The third type of endpoint regulation requires that certain data packets be accompanied by some additional information in order to be sent or received.⁴⁵ Age verification systems, which prohibit the end user from accessing certain content unless and until the user proves that he or she meets the minimum age requirement, constitute a prime example of this third method.⁴⁶ All three regulatory methods in this category are consistent with the e2e principle, which “calls for intelligence to be located at the edges of the network,” thereby keeping the middle of the network as neutral as possible.⁴⁷ While endpoint regulation can certainly prove problematic for freedom of speech, regulating the middle of the network has the capacity to pose a much farther-reaching danger.

2. *Middle-of-the-Network Regulation.* Still, regulation of the middle of the Internet does occur, and may manifest itself in one of two ways, depending on who is in charge of the regulation. First, the government itself may play a direct role in reviewing and filtering information packets as they pass through the Internet backbone.⁴⁸ Alternatively, states may prompt private actors to block or monitor information being transmitted online as it passes through their network.⁴⁹

3. *Current Legal Trends in Internet Content Regulation.* The current trend in Internet regulation, much to the dismay of proponents of the e2e principle, indicates a move away from regulating the network endpoints and toward middle-of-the-network filtering.⁵⁰ This stems primarily from the fact that regulatory measures at the endpoints of the network have proven largely ineffective.⁵¹ Regulators therefore find midpoint

43. *Id.* at 33–34, 44–46.

44. *Id.* at 34, 46.

45. *Id.*

46. *Id.* at 46–47.

47. *Id.* at 32.

48. *Id.* at 35, 49–53.

49. *Id.* at 34, 48–49.

50. *Id.* at 35.

51. *See id.* at 35–36 (“[T]he relative effectiveness of regulations placing control closer to the center of the network will likely lead to more approaches of this kind . . .”). Peer-to-Peer (P2P) filesharing and spamming, which remain prevalent despite fervent

regulation attractive because it is more likely to help them achieve their regulatory goals.⁵² The effectiveness of midpoint regulation is closely tied to its efficiency. This makes sense because it is much easier to assert control over the relatively few network intermediaries through which information flows than to exercise authority over each of the billions of individual Internet speakers and listeners.⁵³

However, several drawbacks are also associated with this regulatory trend. First, the e2e principle, which has benefited the global society since the Internet's inception and which naturally aligns itself with the promotion of rights such as freedom of expression, is compromised by regulations at the middle of the network.⁵⁴ Furthermore, the shift toward having private ISPs and other access providers monitor and police the network can easily lead to unnecessary overregulation and encroachment on the civil liberties of individual Internet users.⁵⁵ Finally, regulating the middle of the network threatens the global character of the Internet—its great potential for spreading information cheaply and easily throughout the world—and thereby inhibits its capacity for promoting cross-cultural understanding and providing an international commercial market.⁵⁶

B. *Filtering: An Examination of Middle-of-the-Network Regulation*

Because middle-of-the-network filtering is quickly becoming the most common form of Internet content regulation, the process merits a discussion in some detail.

1. *What Is Filtering and How Does It Work?* Middle-of-the-network filtering consists of a two-part process whereby various

attempts at regulating them, are two of the most blatant examples of the overall inefficacy of this type of regulation. *Id.* at 54.

52. For example, the Record Industry Association of America (RIAA) recently shifted its legal strategy away from the classic endpoint regulatory method of prosecuting individuals suspected of online music piracy. Instead, the RIAA has joined forces with major ISPs in an effort to monitor filesharing and regulate it in the middle of the network by slowing or cutting off service to repeat offenders. Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1.

53. *See id.* (noting the tens of thousands of lawsuits brought by the RIAA in the past five years “ultimately did little to stem the tide of illegally downloaded music” and asserting that ISPs are “increasingly cutting content deals of their own with entertainment companies”).

54. Palfrey & Rogoyski, *supra* note 3, at 36–37.

55. *Id.* at 37.

56. *Id.*

content on the Internet is first assigned labels and then sorted according to those labels.⁵⁷ Content providers and independent rating organizations review Internet content based on previously determined standards for offensiveness and label the content according to the existence and degree of such offensiveness.⁵⁸ The filtering entity may then choose how it wants to sort the labeled content by selecting and adjusting its filtering software and rating system based on the type or degree of content it wants filtered out.⁵⁹ Thus, although the process is controlled at the endpoints of the network by those labeling the content and adjusting the level of filtration, the content is actually blocked in the middle of the network as it tries to pass from the content provider to the would-be receiver.

2. *Positive Aspects of a Filtering Regime of Internet Content Regulation.* Filters appear to provide an attractive alternative to universal restrictions at the source because, by their very nature, filters restrict content less than blanket endpoint prohibitions.⁶⁰ They exclude content more selectively and are often controlled at the receiving end by the user seeking to access the information. Thus, filters do not preemptively block speakers from expressing themselves, and listeners may gain access to any content not blocked by the restrictive software. Under this type of filtering regime, authorized users may freely gain access to speech without having to identify themselves or otherwise prove their identity.⁶¹ Moreover, this level of control allows adult users to access constitutionally protected adult-oriented speech while simultaneously blocking children from viewing that same content.⁶²

Furthermore, the Supreme Court has already suggested that Congress may mandate the use of filters as a means of

57. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 177 (1999).

58. *Id.*; see also Family Online Safety Institute, About ICRA, <http://www.fosi.org/icra> (last visited Mar. 6, 2009) (listing broad categories of content considered potentially offensive, such as the presence of foul language, nudity, or sexual content, or depictions of violence, drugs, alcohol, or gambling).

59. LESSIG, *supra* note 57, at 177; Family Online Safety Institute, *supra* note 58 (“Users . . . can then use filtering software to allow or disallow access to web sites based on the information declared in the label. . . . ICRA does not rate internet content—the content providers do that, using the ICRA labeling system.”).

60. See *Ashcroft v. ACLU*, 542 U.S. 656, 667 (2004) (striking down the prohibition of commercial transmission of “harmful material” to minors as unconstitutionally overbroad under the First Amendment and suggesting filters as a narrower—and therefore constitutionally acceptable—approach).

61. *Id.*

62. *Id.*; see also *Ginsberg v. New York*, 390 U.S. 629, 636–37 (1968) (recognizing that there is a class of speech that adults have a right to access but children do not).

regulating, at least indirectly, the content available to Internet users.⁶³ Specifically, the Court has asserted that “Congress can give strong incentives to schools and libraries” to filter the content accessible from their Internet connections.⁶⁴ The Court has also maintained that Congress may attempt to promote the industry’s development of better filtering technology and encourage parents to use filters to protect their children from content they deem inappropriate.⁶⁵ Thus, it is evident that filters possess many positive attributes in terms of regulating certain types of content while simultaneously allowing access to everything else, particularly when end users control the filters that affect their own Internet experiences.

3. *Inherent Dangers of Filters.* There certainly exist, however, serious drawbacks to using filters as a means of regulating content on the Internet.⁶⁶ Two of the problems most commonly associated with filtering systems are underblocking and overblocking.⁶⁷ Due to inherent design flaws and technological incompetencies, filters may block some harmless or desirable material (overblocking) while failing to detect other material deemed inappropriate (underblocking).⁶⁸ The shortcomings of filtering software manifest themselves in a variety of ways because both levels of the filtering process—the labeling and the blocking of content—are complex tasks that are continually tested by the ever-changing technologies inherent in this system.⁶⁹

Opponents of filtering as a method of regulation also argue that user-initiated filters are ineffective. For example, they

63. See *Ashcroft*, 542 U.S. at 669 (“[T]he argument that filtering software is not an available alternative because Congress may not require it to be used . . . carries little weight, because Congress undoubtedly may act to *encourage* the use of filters.” (emphasis added)); see also *United States v. Am. Library Ass’n*, 539 U.S. 194, 214 (2003) (upholding a requirement that filters be used in public libraries).

64. *Ashcroft*, 542 U.S. at 669.

65. *Id.*

66. See LESSIG, *supra* note 57, at 178 (describing problems associated with vertical neutrality).

67. *Am. Library Ass’n*, 539 U.S. at 222 (Stevens, J., dissenting).

68. *Id.*; see also *Murdoch & Anderson*, *supra* note 36, at 59 (noting that compiling the list of resources to block is “a considerable challenge and a common weakness” in filtering systems).

69. See LESSIG, *supra* note 57, at 179 (suggesting that both levels of the regulatory scheme have the potential for mistake or abuse); Anthony Niccoli, Comment, *Least Restrictive Means: A Clear Path for User-Based Regulation of Minors’ Access to Indecent Material on the Internet*, 27 J. LEGIS. 225, 235 (2001) (discussing the “glitches in the accuracy of protective software and the confusion over how the development of the next generation of software should proceed”).

maintain that filters do not actually prevent children from viewing inappropriate content because the software is imprecise to begin with and totally worthless unless actually used.⁷⁰ Hence, in situations where parents are either ignorant or indolent, their children may still access objectionable material.⁷¹ Nevertheless, the lack of absolute precision in filtering software does not absolve parents of their responsibility to protect their own children. Instead, placing the onus on parents to understand and implement filtering technology facilitates and reinforces their parental duty.⁷² As it should be, Congress is unlikely to force parents to implement filtering software on their home computers. However, if parents act in a responsible manner to protect their own children to the extent they view as appropriate then it makes governmental regulation unnecessary, prevents violations of the First Amendment, and allows the legislature to spend its time on other, more important issues.⁷³ Furthermore, technology advances rapidly and software developers are constantly striving to produce more accurate filtering systems.⁷⁴ Therefore, concerned parents have no excuse for neglecting to take the simple step of educating themselves about filters and installing the programs on their home computers, rather than waiting around for the legislature to act.⁷⁵

Still, this lack of precision makes filtering software extremely dangerous when controlled by someone other than the end user—it prevents access to constitutionally protected speech sought by adult Internet users. Outside of the context of restricting children’s access to adult-oriented content, it does not appear that Congress can force private individuals to implement filtering software on their personal computers.⁷⁶ This limitation on Congress’s ability to impose a broad filtering scheme seems

70. See *Ashcroft*, 542 U.S. at 668 (noting that filtering “is not a perfect solution” because “[i]t may block some materials that are not harmful to minors and fail to catch some that are”).

71. See *id.*

72. See Niccoli, *supra* note 69, at 235 (“[T]he decision to use legislative regulation versus self-regulation should not rise or fall on the indolence of parents.”).

73. See *id.* at 233–35 (“Protective software . . . presents a viable alternative to the dangers of Congressional regulation.”).

74. See *id.* at 235 (discussing government support and the free market economy as appropriate means for the development of better filtering software).

75. The proper role for Congress, then, is to encourage these software developers and provide information to parents. See *infra* Part VII.C (suggesting alternatives to filtering systems controlled by entities other than end users).

76. See LESSIG, *supra* note 57, at 175–78 (noting that Congress may only regulate speech that is “harmful to minors,” and that filters may block a broader range of content); see also *Ashcroft*, 542 U.S. at 669–70 (asserting that Congress could take steps to promote the use of filters by parents).

highly desirable. However, such a limitation is likely an artificial one, due in large part to the ISPs' broad power to filter even adult users' access to constitutionally protected content without their knowledge.⁷⁷

The most serious concern associated with regulation through filtering schemes is that end users may not even realize that content is being blocked.⁷⁸ Herein lies great potential for abuse by the entities that provide Internet service and access.⁷⁹ Filtering systems lack any internal checks on possible abuses,⁸⁰ a characteristic that stems in part from the fact that labeling systems, by their very nature, rely on ambiguous terms and arbitrary definitions to function.⁸¹ Who defines, for example, what constitutes a "mild" as opposed to a "moderate" expletive or what type of content "sets a bad example for young children"?⁸² Clearly, one person's notion of inappropriate content may be very different from another's. Vague notions of "inappropriate" content permeate all filtering software; however, someone must

77. LESSIG, *supra* note 57, at 178 (warning of the potential for abuse of filtering technology); *see also infra* notes 112–22 and accompanying text (examining Congress's grant of immunity to ISPs for filtering even constitutionally protected content online without fear of civil liability).

78. *See* *United States v. Am. Library Ass'n*, 539 U.S. 194, 224 (2003) (Stevens, J., dissenting) ("Until a blocked site or group of sites is unblocked, a patron is unlikely to know what is being hidden and therefore whether there is any point in asking for the filter to be removed."); LESSIG, *supra* note 57, at 179 ("If you cannot see the content, you cannot know what is being blocked."). Of course, this lack of user awareness is a benefit of filtering when the goal is to keep children away from inappropriate content. Accordingly, the following discussion of this danger should be considered solely in the context of a knowing adult Internet user.

79. *See* LESSIG, *supra* note 57, at 179–81 (discussing the dangers of a filtering regime of regulation); The Open Net Initiative, About Filtering, <http://opennet.net/about-filtering> (last visited Mar. 6, 2009) ("[B]ecause the filters are often proprietary, there is often no transparency in terms of the labeling and restricting of sites."). To make matters worse, Congress has provided total immunity from civil suit for these entities. *Infra* Part V.B.

80. If end users do not even recognize that something is being censored—which, by the nature of filters, they would not—then they cannot attempt to seek redress. When end users are kept in the dark in this manner, and the censor is left free to block content without any fear of reaction, the potential for abuse reaches its peak. *See* The Open Net Initiative, *supra* note 79 (emphasizing the potential for abuse of filters). This general proposition provides the underlying rationale for the Supreme Court's outright rejection of prior restraints. *See* *Near v. Minnesota*, 283 U.S. 697, 722 (1931) (discussing the "serious public evil [that] would be caused by authority to prevent publication"). The same logic applies with equal—if not greater—force in the Internet context for the reasons discussed in *supra* Part II.

81. *See* LESSIG, *supra* note 57, at 178 (noting that vague notions of "the norms of a community" are built into filtering software).

82. To illustrate this point, the reader can open Microsoft Internet Explorer 6, go to the Tools menu, click on Internet Options, go to the Content tab, and explore the Content Advisor, which lists the various types and degrees of content that can be filtered out.

ultimately decide where to draw the line.⁸³ The danger, of course, lies in the risk that ISPs or other creators of filtering software will impose their views of morality on their unknowing customers.⁸⁴

This risk is only minimally mitigated when users select their own filter settings. Although the user may configure the filter to block a predefined category of content, he or she nevertheless “has no way of knowing the criteria used by the [filtering] software developers to select which websites fall into this category, nor which websites will actually be found to fall within this category.”⁸⁵ Thus, even purportedly user-controlled filtering systems have inherent flaws that may lead to unwanted content blocking.

This concern is particularly salient—and even more unsettling—when a third party filters the content available to an adult Internet user without the user’s consent or, even worse, without the user’s knowledge. The concern is also very real because “[f]iltering can occur at any level in the distributional chain—the user, the company through which the user gains access, the ISP, or even the jurisdiction within which the user lives.”⁸⁶ If third parties may filter out material they deem objectionable before it ever reaches an adult user’s computer, unconstitutional censorship may go undetected and, consequently, unchecked.⁸⁷ Filtering software thus has even greater potential for speech-stifling censorship when it is not controlled by the end user, but instead by the ISP or access provider.⁸⁸ Indeed, this constitutes the ultimate form of unacceptable censorship and is a manifestation of the absolute power that rating and filtering companies can flex over the end user’s Internet experience.

If the government permits these entities to exercise control over what the public can access, they may potentially exercise complete control: telling users what they are allowed to perceive and, ultimately, what they should believe. The relevant issue,

83. See O’Keefe et al., *supra* note 23, at 230 (noting that defining vague terms such as “obscene” and “harmful to minors” is “beyond the capacity of filters and inherently subject to the normative and technological choices made during the software design process”).

84. See *id.* (“[I]t is developers first, and users second, who determine what gets filtered when such software is implemented.”).

85. Nunziato, *supra* note 13, at 1152.

86. LESSIG, *supra* note 57, at 178.

87. See *id.* (describing the invisibility of filtering as inherent in the design).

88. See *id.* at 179 (warning that filters may be used without a user’s knowledge or consent).

then, concerns whom we should trust with this broad power to regulate content on the Internet.

V. IN WHOM SHOULD THE POWER TO REGULATE BE VESTED?

One of the most important questions for the end user in the Internet regulation debate concerns what entity should have the power to regulate accessibility to content on the Internet. At least three major players should be considered as viable candidates to take the reins in the Internet regulation game: the government, private electronic media corporations,⁸⁹ and the end user. Congress itself initially sought to regulate Internet content, but the Supreme Court repeatedly struck down its legislation as violating the First Amendment.⁹⁰ Subsequently, and despite the existence of two remaining alternatives, Congress, with the full support of the courts, resoundingly answered that this formidable power should be vested almost exclusively in private business entities, controlled only by the invisible hand of the free market.⁹¹

A. Congress's Failed Attempts at Regulation

Beginning in the early 1990s, Congress sought to regulate Internet content on several occasions, primarily in the name of protecting minors from harmful content.⁹² The majority of these regulatory regimes, however, were struck down by the Supreme Court as unconstitutional violations of the First Amendment.⁹³ Time and time again, the Court made it clear that it would apply

89. In this Comment, "private electronic media corporations" and similar terms refer to the companies that supply Internet service and access, predominantly in the form of ISPs, such as AOL-Time Warner and Comcast, or access providers such as Google and MySpace.

90. See *infra* note 93 (listing cases in which the Supreme Court struck down congressional legislation).

91. See *supra* note 33 and accompanying text (discussing Section 230 (granting regulatory immunity to ISPs) and the Supreme Court case upholding its constitutionality); *infra* Part V.B (same).

92. See, e.g., CDA, 47 U.S.C. § 223 (2000 & Supp. 2005) (prohibiting the transmission of "indecent" material and the display of "patently offensive" content and communications to minors); Child Online Protection Act (COPA), 47 U.S.C. § 231 (2000) (regulating the commercial distribution of materials deemed "harmful to minors"); see also CAN-SPAM Act of 2003, 15 U.S.C. § 7701 (2006) (outlining congressional findings in relation to unsolicited mass e-mail).

93. See, e.g., *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004) (striking down COPA as unconstitutionally overbroad under the First Amendment); *Reno v. ACLU (Reno II)*, 521 U.S. 844, 874 (1997) (finding a portion of the CDA unconstitutional on First Amendment grounds because "less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve").

the highest level of judicial scrutiny to legislation seeking to regulate content on the Internet, requiring that it be narrowly tailored to serve a compelling governmental interest and that there be no less restrictive alternative available.⁹⁴

Assuming the government has a compelling interest in implementing some narrowly tailored content regulation,⁹⁵ the remaining issue concerns what manner of regulatory scheme constitutes the least restrictive means of achieving that goal.⁹⁶ The Supreme Court determined that the types of regulations initially sought by Congress violated the spirit and essence of the democratic guarantees of freedom of expression embodied in the First Amendment. Rather than accept the notion that the Internet should remain a free and open forum for public discourse, however, Congress simply passed the content regulation torch to private electronic media corporations. Because these corporations are technically beyond the reach of the First Amendment, they can potentially engage in massive regulation of Internet content that would be patently unconstitutional if carried out by Congress itself.⁹⁷

B. Ceding the Task of Regulation to the ISPs: Section 230 of the Communications Decency Act of 1996

In the wake of its failed attempts to regulate content on the Internet, Congress left the task almost entirely up to the corporations who own and operate the Internet's physical infrastructure. The government did not sit idly by as this regulatory power became concentrated in the hands of a few

94. *Ashcroft*, 542 U.S. at 665–66 (applying strict scrutiny and finding blanket speech restrictions under COPA unconstitutional because effective, less restrictive alternatives were available); *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 827 (2000) (striking down the Telecommunications Act, 47 U.S.C. § 561 (1994 & Supp. 1996), for the same); *Reno II*, 521 U.S. at 874 (finding portions of the CDA unconstitutional because they were not narrowly tailored to serve a compelling governmental interest and because less restrictive means of achieving the goal existed).

95. *See supra* Part III (discussing legitimate reasons to regulate Internet content).

96. Much like the Court has consistently held that only the least restrictive federal regulations will survive constitutional scrutiny, this Comment suggests that *any* entity seeking to regulate access to content should be required to do so in the least restrictive manner possible. *See infra* Part VII (arguing that a system of user-controlled regulation would support such a standard).

97. *See infra* note 116 and accompanying text (noting the inapplicability of First Amendment guarantees to private actors). *But see infra* Part V.C (suggesting state action in promoting content regulation by private corporations should subject that private action to constitutional scrutiny).

large corporations; rather, Congress actively encouraged them to take on this role.⁹⁸

1. *Objectives and Affirmation.* Section 230 of the Communications Decency Act (CDA) supplies the most blatant example of state sponsorship of private regulation, giving ISPs immunity from civil suits stemming from their choices regarding content regulation. It provides in relevant part:

No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.⁹⁹

On its face, Section 230 appears to simply protect ISPs from any liability for *restricting* access to content.¹⁰⁰ Nevertheless, in practice it has been applied primarily in the defamation context, immunizing ISPs from liability for allegedly *providing* defamatory content.¹⁰¹ Though seemingly counter to the plain language of the statute, this construction of Section 230 as giving ISPs immunity for content they choose *not* to restrict is supported by both Congress's legislative intent and subsequent judicial interpretation.¹⁰²

Thus, through Section 230, Congress sought to advance freedom of expression online "by minimizing the government's role in regulating Internet expression, [and] handing over the

98. See *infra* Part V.B.1–2 (examining the grant by Section 230 to ISPs of immunity for any content restrictions).

99. CDA, 47 U.S.C. § 230(c)(2) (2000).

100. *Id.*

101. See, e.g., *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997) (upholding Section 230 as necessary to prevent ISPs from simply removing any allegedly defamatory content from their network for fear of liability).

102. For example, Congress cited such policy justifications for the CDA as "promot[ing] the continued development of the Internet," "preserv[ing] the vibrant and competitive free market . . . for the Internet," and "encourag[ing] the development of technologies which maximize user control over what information is received." 47 U.S.C. § 230(b) (2000). Similarly, the courts have asserted that providing such immunity for ISPs is necessary to preserve freedom of speech on the Internet. See Raymond Shih Ray Ku, *Irreconcilable Differences? Congressional Treatment of Internet Service Providers as Speakers*, 3 VAND. J. ENT. L. & PRAC. 70, 77 (2001) (discussing the court's finding in *Zeran* that Section 230 was necessary in the defamation context to prevent ISPs from simply taking down any challenged content for fear of liability); see also *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843, 850 (W.D. Tex. 2007) ("[S]ection [230] reflects Congress's recognition that the potential for liability attendant to implementing safety features and policies created a disincentive for interactive computer services to implement any safety features or policies at all.").

reins . . . to private actors.”¹⁰³ In particular, Congress refused to open the nation’s courts to individuals who are offended by content on the Internet and seek redress by suing the ISP or access provider.¹⁰⁴ According to this logic, holding media corporations liable for the content they provide would simply impose too great a burden, not only because the Internet serves as a medium of mass expression, but also because of the extremely large volume of content continually posted on the Internet.¹⁰⁵ As the *Zeran* Court noted, Congress probably worried that ISPs, fearing suit over objectionable material, would simply choose to remove any and all content complained of as inappropriate without actually investigating each claim individually, due to the enormous number of potential claims.¹⁰⁶ Inevitably, this would have resulted in the removal of content that was not necessarily inappropriate, thereby stifling free speech.¹⁰⁷ When viewed in this manner, Congress’s decision to grant immunity to ISPs for liability based on their choices in providing access to content seems understandable.

Several federal courts have dealt with Section 230 in the context of users distressed by their ISP’s failure to censor Internet content that they found offensive. Most of these cases “involved attempts to hold an interactive computer service liable for its publication of third party content or harms flowing from the dissemination of that content.”¹⁰⁸ For example, the courts have: refused to impose liability on an ISP for allegedly defamatory content it posted;¹⁰⁹ held that Section 230 barred lawsuits against ISPs for all decisions regarding “whether to publish, withdraw, postpone or alter content”;¹¹⁰ and even found AOL immune from a defamation suit for content published on a blog called the Drudge Report, even though the ISP was actively

103. Nunziato, *supra* note 13, at 1129.

104. *See id.* (“In Section 230 of the CDA, Congress sought to encourage the proliferation of a free market in Internet speech; a market in forums for expression that would be largely unfettered by government intervention and defined predominantly by private actors’ speech choices.”).

105. *See Ku, supra* note 102, at 77 (discussing the *Zeran* court’s finding that Section 230 immunity was necessary to preserve freedom of expression on the Internet by preventing this “impossible burden” from being placed on ISPs by “the sheer number of postings” (quoting *Zeran*, 129 F.3d at 333)).

106. *Zeran*, 129 F.3d at 333.

107. *Id.*

108. *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007).

109. *Ben Ezra, Weinstein, & Co. v. Am. Online, Inc.*, 206 F.3d 980, 986 (10th Cir. 2000).

110. *Zeran*, 129 F.3d at 330.

involved in employing, promoting, and editing it.¹¹¹ Thus, Section 230 has more often been used to protect ISPs from liability for hosted third party content, which, in keeping with Congress's asserted intention, serves to *promote* free speech. While this goal is certainly desirable, it runs contrary to the plain meaning of Section 230, which implicates an immense potential for sweeping detrimental effects on freedom of expression online.

2. *Dangers of Section 230.* Providing ISPs with such broad immunity from liability is unnecessary, illogical, and counterproductive to Congress's stated intent.¹¹² By providing that "any action" taken to "restrict access to or availability of" content on the Internet is immune from civil liability,¹¹³ Congress eliminated the threat of retributive legal action. This thereby gave ISPs a green light to implement any form of censorship they could conjure. The "good faith" requirement does little to limit the freedom of ISPs to restrict content access, given the slippery nature of the definition of the term.¹¹⁴ Nor does the laundry list of adjectives describing the type of content that may be restricted limit its potential for abuse, because nearly any content could qualify as "otherwise objectionable" under this utterly subjective test as long as the ISP "considers" it to fall within that broad category.¹¹⁵

Section 230 effectively encourages private ISPs to do what Congress itself could not do: restrict access to content that, although constitutionally protected, is deemed "objectionable" to some individuals.¹¹⁶ It does more than "recognize the private

111. *Blumenthal v. Drudge*, 992 F. Supp. 44, 51–53 (D.D.C. 1998).

112. *See* *Ku*, *supra* note 102, at 77 ("While Congress may have paid lip service to the values of free expression in the CDA, the statute itself threatens rather than promotes freedom of speech.")

113. CDA, 47 U.S.C. § 230(c)(2)(A) (2000).

114. *See id.* (requiring that ISPs exercise "good faith" in restricting content availability); Laureano F. Guiterréz Falla, *Good Faith in Commercial Law and the UNIDROIT Principles of International Commercial Contracts*, 23 PENN ST. INT'L L. REV. 507, 508 (2005) ("[G]ood faith is a slippery expression that reflects the changing points of view of generations and succeeding societies.")

115. *See* CDA, 47 U.S.C. § 230(c)(2)(A) (2000) (immunizing ISPs for content they find "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable"). It is worth noting that the "otherwise objectionable" language in the statute would almost certainly be found unconstitutional if it applied to government action. *Cf. supra* notes 92–93 (listing statutes struck down by the Supreme Court that sought to limit material found to be "harmful to minors," "indecent," or "patently offensive").

116. *See* Nunziato, *supra* note 13, at 1126–27 ("Because [an ISP] is a private entity, the determinations that it makes regarding the types of expression allowed within its property are not subject to scrutiny under the First Amendment."); *see also* Jose I. Rojas, *Liability of ISPs, Content Providers and End-Users on the Internet*, in 507 PRACTICING

editorial rights of ISPs” and protect them from prosecution for exercising those rights.¹¹⁷ Indeed, by immunizing ISPs from all liability for their editorial decisions, it effectively creates “an environment for unrestrained and irresponsible censorship.”¹¹⁸ By its very terms, Section 230 intimates that the individuals responsible for making the judgment call as to whether a particular piece of content is “objectionable” are none other than the “provider[s] or user[s]” themselves.¹¹⁹ Essentially, privately owned ISPs may make the determinations as to what speech they will or will not host on their networks, and thus what speech the end user accessing the Internet may send or receive. Because Internet users gain access almost exclusively through these private companies, ISPs effectively become the final arbiter of what content may be accessed on the Internet.¹²⁰ As such, for “the great majority of Internet speakers” and listeners, their ISP’s subjective notion of how far free speech should extend, rather than the First Amendment, defines the boundaries of protection afforded to Internet expression.¹²¹ Consequently, ISPs wield an enormous amount of power in regard to online censorship.¹²²

C. *The State Action Doctrine*

At first glance, the notion of government-sponsored private censorship embodied in Section 230 appears to rise to the level of state action.¹²³ According to the state action doctrine, the conduct

LAW INST., PATENTS, COPYRIGHTS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 1009, 1019 n.25 (1998) (“[A] private ISP . . . is not precluded by the First Amendment from blocking email ‘spamming’ by its customers on the reasoning that there is no ‘state action’ where a private company takes such action.” (citing *Cyber Promotions, Inc. v. Am. Online Inc.*, 948 F. Supp. 436 (E.D. Pa. 1996))).

117. Ku, *supra* note 102, at 77.

118. *Id.*

119. CDA, 47 U.S.C. § 230(c)(2)(A) (2000).

120. See Nunziato, *supra* note 13, at 1123 (“[T]he vast majority of Internet access and service providers, which are privately owned, assert and exercise substantial control over the expression that flows through their Internet places.”); see also Jon Perr, *Google’s Gag Order: An Internet Giant Threatens Free Speech*, PERSPECTIVES, June 20, 2004, http://www.perspectives.com/articles/art_gagorder01.htm (“Google is on the verge of becoming the Internet arbiter of the First Amendment.”).

121. Nunziato, *supra* note 13, at 1127.

122. See Ku, *supra* note 102, at 71 (“ISPs are capable of exercising absolute control over the information that appears on their networks and who may access that information.”); Palfrey & Rogoyski, *supra* note 3, at 48–49 (“[Section 230] grants nearly carte blanche to third-party intermediaries who choose of their own accord to block content that a user has made available online, without fear of exposure to civil liability relative to that user’s claims.”).

123. See Ku, *supra* note 102, at 83 n.92 (“By immunizing ISPs for any effort to censor material on their networks ‘whether or not it is constitutionally protected,’ the CDA potentially elevates private censorship to state sponsored censorship of speech

of private actors may constitute state action—subject to the constitutional restraints on government—based on a number of theories. Generally, a sufficient nexus between the two must be shown such that the private actor's conduct can be fairly attributed to the state.¹²⁴ For example, private actions fulfilling a traditionally exclusive public function may be characterized as state action.¹²⁵ Alternatively, state authorization or encouragement of private action may trigger the application of constitutional scrutiny against the private entity.¹²⁶ Thus, the argument goes, because of the government's affirmative role in facilitating censorship by private ISPs, the ISPs should in turn be held to the First Amendment standards typically reserved for state actors.¹²⁷

However, given the extent to which the Supreme Court has sought to limit this doctrine in recent years, the Court seems unlikely to find that private censorship by an ISP constitutes state action.¹²⁸ For example, in *Cyber Promotions, Inc. v. American Online, Inc.*, a federal district court found that, absent state action, AOL had the right to block unsolicited e-mails from reaching its customers.¹²⁹ The court specifically refused to find that the popular ISP's provision of e-mail accounts was an exclusive public function, even though AOL maintained complete control over access to its members' accounts and despite the

inconsistent with the First Amendment.” (quoting 47 U.S.C. § 230(c)(2)(A)).

124. See, e.g., *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982) (holding that to invoke the state action doctrine, there must be “a sufficiently close nexus between the State and the challenged action . . . so that the action of [the private entity] may be fairly treated as that of the State itself”).

125. See, e.g., *Marsh v. Alabama*, 326 U.S. 501, 506 (1946) (subjecting the activities of a company town to state regulation because “their operation [was] essentially a public function”). More recently, however, the Court has severely limited this analysis, requiring exclusivity in the state's reservation of a function. See, e.g., *Flagg Bros., Inc. v. Brooks*, 436 U.S. 149, 158 (1978) (“While many functions have been traditionally performed by governments, very few have been ‘exclusively reserved to the State.’” (quoting *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 352 (1974))).

126. See, e.g., *Reitman v. Mulkey*, 387 U.S. 369, 380–81 (1967) (striking down legislation found to authorize racial discrimination in the housing market). The Court has since retreated from the application of this doctrine, insisting that state involvement with the private conduct must be significant to constitute authorization. See, e.g., *Moose Lodge No. 107 v. Irvis*, 407 U.S. 163, 176–77 (1972) (rejecting a claim that a private club's racial discrimination was unconstitutional state action simply because the club held a state liquor license).

127. *Ku*, *supra* note 102, at 83 n.92.

128. See *Nunziato*, *supra* note 13, at 1135–42 (surveying the Supreme Court's application of the state action doctrine and concluding that it is unlikely to be successfully ascribed to private Internet regulation); *supra* notes 125–26 (noting the Court's reluctance to expand the exclusive public function or state authorization models of state action).

129. *Cyber Promotions, Inc. v. Am. Online, Inc.*, 948 F. Supp. 436, 437 (E.D. Pa. 1996) (mem.).

importance of e-mail to public discourse and free speech.¹³⁰ Furthermore, the court rejected the suggestion that the government participated in AOL's conduct by virtue of the ISP's use of the court system to validate its actions.¹³¹

Although the case law has consistently suggested against a finding of state action, that precedent may—and should—be poised to change. Even the court in *Cyber Promotions* specifically limited its ruling based on the fact that “AOL has never sought to control the exchange of ideas and communications over the Internet itself. Rather, AOL has sought to control its own pathway or channel leading to the Internet in order [to] protect its own private property, reputation and subscribers”¹³² Thus, if an ISP attempts to block content flowing through the Internet itself—as permitted by Section 230—such conduct may qualify as state action if a court finds that the promotion of the free exchange of ideas online is traditionally an exclusive public function.¹³³ The *Cyber Promotions* court also conceded that “[t]he Internet may indeed some day be found to be a critical pathway of communication.”¹³⁴ This intimates the court's recognition that the Internet had the potential to rise to the level of a public function if it became a vital channel for communication, as it has in the decade since that decision.¹³⁵

The reasoning employed in *Cyber Promotions* is easily distinguishable from the statutory authorization of private regulation of Internet content today. The primary difference is that the government's involvement in an ISP's content regulation through Section 230 is unquestionably greater. Indeed, the statute provides actual authorization to the ISPs, as opposed to

130. *Id.* at 441–43.

131. *Id.* at 444.

132. *Id.* at 454–55 (mem. on reconsideration).

133. The distinction between an ISP regulating its own pathways and regulating the Internet at large is addressed in *MySpace v. Wallace*, 498 F. Supp. 2d 1293 (C.D. Cal. 2007). In *Wallace*, the court denied the access provider's proposed injunction insofar as it would have prohibited an end user from referencing MySpace in connection with any e-mail or advertisement whatsoever on the Internet. However, the court upheld the injunction insofar as it prohibited the user from accessing or manipulating the MySpace website specifically. *Id.* at 1307. Thus, because Section 230 does not limit ISP immunity to content restrictions on its own pathways, courts should be more receptive to arguments against permitting this broad level of content regulation. Interestingly, the *Wallace* court did not discuss the state action doctrine, even though MySpace asserted authority for the injunction based on the federal CAN-SPAM Act and similar state codes. Instead, the court determined the proper scope of the injunction solely in terms of the defendant's First Amendment rights. *Id.* at 1307–08.

134. *Cyber Promotions*, 948 F. Supp. at 454 (mem. on reconsideration).

135. The rise of the Internet as a forum for participatory communication is discussed in *supra* Part II.

mere post hoc ratification by the courts, of the regulation in question. Furthermore, the Internet's role in providing access to information and promoting the free exchange of ideas has increased dramatically in recent years. Therefore, the state action issue merits reconsideration in relation to Section 230.

D. The Negative Notion of First Amendment Freedoms

Congress and the Supreme Court have adopted a negative construction of their role in protecting First Amendment freedoms. Under the negative theory, "[T]he primary purpose of the First Amendment is to insulate private individuals' speech decisions from government interference."¹³⁶ Therefore, a free market for speech, along with market-driven regulations of speech, completely conforms to the ideals of freedom of expression and requires no intrusion on the part of the government, even to protect speech. In the context of the Internet, as long as the barriers to entry into the speech market remain low, private decisions with regard to speech made in private online forums will adequately protect First Amendment rights. Accordingly, the free market renders affirmative government involvement in the regulation of Internet speech unnecessary.¹³⁷ This negative conception of the government's role in protecting First Amendment freedoms, however, is inappropriate.

The affirmative theory, on the other hand, maintains that the government should take an affirmative role in protecting freedom of speech because the private market cannot adequately determine what speech to permit and what speech to restrict.¹³⁸ Rather, the free market system necessarily fails because the values embodied in the First Amendment are not meant to reflect an aggregate of existing private preferences, but instead are meant to incorporate a set of collective values, which an unregulated market will not necessarily recognize.¹³⁹ In particular, "dissenting and other disfavored or unpopular speech [may] be foreclosed" if the government does not take some action to protect it.¹⁴⁰ Furthermore, the affirmative conception of

136. Nunziato, *supra* note 13, at 1143.

137. *Id.*

138. *Id.* at 1143-44.

139. *Id.*

140. *Id.* at 1144; *see also* Balkin, *supra* note 7, at 42 ("In a world dominated by mass media controlled by a relative handful of very wealthy corporations, it seems important to make sure that dissenting views get a word in edgewise, [and] that serious issues are not driven out by the media's never-ending quest for profits . . .").

freedom of expression comports with First Amendment jurisprudence, which clearly asserts an individual's right to both speak and be heard.¹⁴¹

Therefore, ensuring that each citizen has the opportunity to express him or herself meaningfully may require government involvement in the market to protect free speech.¹⁴² Specifically, the "minimally adequate opportunity for the exercise of certain freedoms" that the government may be required to provide should include a degree of constitutional protection of online speech.¹⁴³ The ability of every individual to have his or her voice heard is essential to our system of democratic self-government;¹⁴⁴ furthermore, the Internet provides the perfect platform for realizing this goal because it facilitates individual expression more than any other medium in history.¹⁴⁵ Thus, government involvement is particularly necessary in this context because of the Internet's ability to provide the ideal interface for public discourse¹⁴⁶ as well as the potential for abuse by the private corporations who control its physical infrastructure.¹⁴⁷

E. ISPs: Publishers or Common Carriers?

Another relevant concern in determining who should wield regulatory power over Internet content stems from whether the

141. It has long been established that freedom of speech under the First Amendment includes not only the freedom to speak but also the freedom to receive speech. *See, e.g.*, *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes . . . the right to distribute, the right to receive, the right to read . . . and freedom of inquiry, freedom of thought, and freedom to teach . . ."); *Martin v. City of Struthers*, 319 U.S. 141, 146–47 (1943) (noting that the freedoms to distribute and receive information are "clearly vital to the preservation of a free society" and, therefore, "must be fully preserved"). Indeed, this notion has become entrenched in our nation's impression of freedom of expression. *See, e.g.*, *Bd. of Educ. v. Pico*, 457 U.S. 853, 866 (1982) (asserting that the role of the First Amendment deals with both "fostering individual self-expression" and "affording the public access to discussion, debate, and the dissemination of information and ideas" (quoting *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 783 (1978))); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas. . . . regardless of their social worth.").

142. Nunziato, *supra* note 13, at 1144.

143. *Id.* (quoting LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* 964 (2d ed. 1988)).

144. *Id.*

145. *See* Crawford, *supra* note 21 ("The Internet is unlike anything we've seen before; it's the largest idea-generating, participatory communications medium in history.").

146. *See supra* Part II (evaluating the Internet's natural propensity to be a forum for individual expression on a massive scale).

147. *See infra* Part VI (examining the potential for abuse by private content regulators). Of course, grave dangers are also associated with government overregulation. Thus, government oversight must be limited as discussed in *infra* Part VII.

ISPs are identified as common carriers or as publishers. Although the e2e principle assumes the Internet should serve as a common carrier, this assertion is far from a given.¹⁴⁸ Courts have long recognized that each medium of expression presents its own unique First Amendment problems and deserves individualized analysis.¹⁴⁹ Generally speaking, courts acknowledge two main types of media: publishers and common carriers. The rules that relate to these two groups are very different; therefore, the yet undecided question of which category the Internet falls into is very important.

Courts are very deferential to the editorial discretion of private publishers and broadcasters. The underlying belief is that the First Amendment rights of publishers as speakers are violated if they are not allowed decisionmaking authority over what information to disseminate.¹⁵⁰

On the other hand, common carriers such as telephone and telegraph companies are typically required to provide open access. In this context, the thinking is that the service provider merely serves as a conduit for the expression of others. Thus, the First Amendment rights of the providers are not implicated, because they are not speakers in any real sense. Therefore, the rights of their users must be given priority.¹⁵¹

148. See *supra* notes 37–41 and accompanying text (discussing the e2e principle).

149. See, e.g., *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 502–03 (1952).

150. The Supreme Court originally upheld the “fairness doctrine,” which—based on the right of the listening public to be informed—holds broadcasters responsible for providing the public with a balanced representation of issues of public importance. *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 390 (1969) (“It is the right of the viewers and listeners, not the right of the broadcasters, which is paramount.”). Indeed, radio broadcasting has historically “received the most limited First Amendment Protection.” *FCC v. Pacifica Found.*, 438 U.S. 726, 748 (1978). However, the Court in *Reno* specifically distinguished the Internet from radio. *Reno v. ACLU (Reno II)*, 521 U.S. 844, 869 (1997) (noting that the Internet is less “invasive” than radio or television and that Internet users are unlikely to accidentally encounter objectionable content).

Furthermore, without so much as a mention of *Red Lion*, the Court severely limited the fairness doctrine a mere five years after it was set forth. See *Miami Herald Publ’g Co. v. Tornillo*, 418 U.S. 241 (1974). In *Tornillo*, the Court struck down a Florida statute requiring newspapers to allow public officials attacked in their publication the opportunity to respond to the allegations in a subsequent issue. In determining that a state-mandated “right of reply” is unconstitutional, the Court reasoned that the newspaper had a First Amendment right to the “exercise of editorial control and judgment” over what it printed. *Id.* at 257–58. Similarly, the Court has found that neither the public interest nor the First Amendment requires television stations to accept paid editorial advertisements because broadcasters have editorial discretion over what they air. *Columbia Broad. Sys., Inc. v. Democratic Nat’l Comm.*, 412 U.S. 94, 121–22 (1973).

151. See *Denver Area Educ. Telcomm. Consortium, Inc. v. FCC*, 518 U.S. 727, 739 (1996) (“[I]n respect to leased [or public access cable] channels, [cable companies’] speech interests are relatively weak because they act less like editors, such as newspapers or television broadcasters, than like common carriers, such as telephone companies.”).

The Internet has traits in common with both models. For example, in many instances ISPs serve as both service and content providers.¹⁵² Ultimately, however, the Internet should be regarded as a common carrier. As discussed above, the primary benefit of the Internet arises from its function as a system connecting content providers and content seekers.¹⁵³ This speaker–listener dichotomy is more in line with the common carrier paradigm. Furthermore, characterization as a common carrier is consistent with the e2e principle that has been prominent since the Internet’s inception. Hence, the First Amendment rights of end users must trump the editorial decisions of ISPs.

VI. DANGERS OF THE “FREE MARKET” MODEL OF INTERNET CONTENT REGULATION

Congress deliberately chose to allow the “free market” model to reign supreme over regulation of expression on the Internet.¹⁵⁴ It accomplished this by allowing ISPs and other private access providers to restrict access to free expression that the providers, at their sole discretion, find undesirable.¹⁵⁵ Essentially, Congress determined that letting the market run its course, “unfettered by Federal or State regulation,”¹⁵⁶ best promoted innovation and development during the infancy of the technological revolution.¹⁵⁷

The invisible hand of the market has received a great deal of deference concerning Internet content regulation for a long time; however, the Internet cannot survive as the ultimate public forum for individual expression if private businesses continue to reign unchecked in this manner.¹⁵⁸ Due to the unique nature of the Internet,¹⁵⁹ this “free market” concept of regulation proves

152. For further discussion of media concentration, see *infra* note 175 and accompanying text.

153. See *supra* Part II.

154. See *supra* notes 103–07 and accompanying text (discussing Congress’s desire to facilitate private regulation of content on the Internet by enacting Section 230).

155. See *supra* notes 112–22 and accompanying text (scrutinizing the statutory language of Section 230).

156. CDA, 47 U.S.C. § 230(b)(2) (2000).

157. As Michael Powell, then-acting Chairman of the FCC, asserted, “Government regulation of the terms and conditions of private contracts is probably the most fundamental intrusion on the free market. This intrusion is particularly destructive where innovation and experimentation are hallmarks of an emerging service.” Michael K. Powell, *Preserving Internet Freedom: Guiding Principles for the Industry*, 3 J. ON TELECOMM. & HIGH TECH. L. 5, 10 (2004).

158. See Balkin, *supra* note 7, at 20–22 (arguing that the “capitalist theory of freedom of speech” is misplaced in the Internet context).

159. See *supra* Part II (describing the participatory potential of the Internet).

undesirable for several reasons. Among the most important are: the nature of both direct and indirect censorship in the Internet context, the lack of meaningful choice in the ISP and access provider markets, and the model's overall incompatibility with the character and purpose of the Internet itself.

A. *Direct Censorship*

Concerns about private businesses abusing the extreme power granted to them by Congress are not merely hypothetical, but rather are very real.¹⁶⁰ The policies of Google, a company that has emerged in recent years as the clear leader among Internet search engines and is responsible for an enormous share of the nation's access to content online, represent a glaring example of corporate abuse of regulatory power.¹⁶¹ Besides providing links to websites corresponding to search terms, Google searches also provide "sponsored links," or advertisements related to the search terms entered by the user, that appear alongside the initial search results.¹⁶² Due to Google's dominant position in the search engine market, and because most users typically do not look beyond the first page or two of search results, obtaining a sponsored link from Google has become a crucial method of expression for anyone actively seeking to disseminate information on the Internet.¹⁶³ Unfortunately, Google has taken advantage of this power to determine which Internet speakers

160. See, e.g., Nunziato, *supra* note 13, at 1121 ("The extent of such private speech restrictions is staggering."). Proponents of the "free market" system of Internet regulation argue that these concerns are unjustified because of the lack of more concrete examples of improper censorship. See *Overcoming Mythology in the Debate over Media Coverage: Hearing Before the S. Comm. on Commerce, Science, and Transp.*, 108th Cong. 1 (2004) (statement of Adam Thierer, Director of Telecommunication Studies, CATO Institute) ("While critics of media liberalization have had great success employing heated rhetoric and extremely emotional rationales for . . . regulation, claims about a lack of 'diversity,' the end of 'localism,' or the supposed 'death of democracy' simply do not equate with reality."). However, the very nature of middle-of-the-network content filtering is such that abuses may easily go undetected. See Wang, *supra* note 28, at 162; *supra* notes 78–88. As a result, mainstream empirical data concerning the actual prevalence of this activity remains nonexistent. The fact that such data is not readily quantifiable alone gives cause for concern and reinforces the need for a user-controlled system, as discussed in *infra* Part VII.C.

161. See Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, 2008 U. CHI. LEGAL F. 263, 263 n.1 (2008) (stating that Google, with a 67% share of U.S. Web searches in September 2007, "is the most dominant search engine" in the United States). Google's "iconic status" has even risen to the level that a new verb has become part of the English language: "To Google" someone or something has become synonymous with using the Internet to find information, images or news." Perr, *supra* note 120.

162. Nunziato, *supra* note 13, at 1123.

163. *Id.*

are heard by refusing to accept many sponsored links simply because they fit Google's broad category of content constituting "advocacy against any individual, group, or organization."¹⁶⁴ Pursuant to this policy, Google has refused to host many political, religious, or socially critical advertisements as well as the websites to which these advertisements link.¹⁶⁵ Google has thereby effectively, if not actually, silenced a great deal of Internet speech.

Although preventing certain types of content from being used as sponsored links does not remove the content from the search results, it nevertheless presents dangerous implications. Given Google's powerful status with regard to Internet users' ability to speak out, enlist the like-minded, and promote goods and services; and given users' reliance, trust, and confidence in Google, it should not be permitted to take on the role of censor.¹⁶⁶ This problem is of even greater importance because of the nature of the content restricted by Google; political, religious, and otherwise unpopular ideas are exactly the types of speech the Framers sought to protect by enacting the First Amendment.¹⁶⁷

The "terms of service" employed by all of the major ISPs represent another example of the potential for censorship at the hands of private corporations. Each ISP creates and enforces its own terms of service, giving itself the contractual right to prohibit the expression of certain types of speech that it subjectively finds inappropriate.¹⁶⁸ The First Amendment would protect much of the content prohibited by the ISPs' terms of

164. Google, Google AdSense Program Policies, <http://www.google.com/adsense/policies> (last visited Mar. 6, 2009).

165. Nunziato, *supra* note 13, at 1124–25 (discussing Google's censorship of sponsored links to websites promoting, among other things, a book about Guantanamo detainees and Abu Ghraib, criticism of President George W. Bush, and the Church of Scientology).

166. Perr, *supra* note 120. This notion applies with equal force to all private electronic media corporations who play a role in Internet users' access to information:

In a democratic society, those who control access to information have a responsibility to support the public interest. By dint of their power over such an important resource, these gatekeepers must assume an obligation as trustees of the greater good. Indeed, barring some clear showing that they are bearing this burden voluntarily, government should impose it upon them.

ANDREW L. SHAPIRO, *THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW* 225 (1999) (emphasis omitted).

167. See Brubaker, *supra* note 2, at 89–90 (discussing the importance the Framers of the Constitution placed on the freedom of political speech in promoting democratic self-government).

168. Nunziato, *supra* note 13, at 1121.

service¹⁶⁹ if the government attempted to regulate that same content directly. However, despite enjoying full endorsement by the federal government,¹⁷⁰ ISPs reserve the right to regulate speech at their “sole discretion” under the guise of private action.¹⁷¹ ISPs may even “refuse to transmit or post” or “remove or block” any form of expression they find objectionable, “regardless of whether this material or its dissemination is unlawful.”¹⁷² Thus, ISPs enjoy freedom to block speech that is both constitutionally protected and otherwise lawful.¹⁷³ Furthermore, as discussed above, the end user is typically not even aware that such censorship is taking place.¹⁷⁴ The concentration of the Internet market in the hands of a few large electronic media corporations results in a lack of meaningful choice among ISPs, magnifying the speech-stifling effects of these terms of service.

B. Media Concentration and Lack of Meaningful Choice

The urgency of this situation is compounded by the paucity of options available to end users seeking Internet service. Indeed, in recent years mergers and market forces have resulted in only a few ISPs remaining as viable options for most users.¹⁷⁵ This means that a very large amount of power to control the middle-of-the-network region of the Internet rests in the hands of a very small number of private electronic media companies.

The fact that similar conditions appear in every major ISP’s terms of service further diminishes the force of the “free market”

169. *Id.*

170. *See supra* notes 116–22 and accompanying text (describing the congressional grant of immunity from liability to ISPs for the content they host).

171. America Online, Agreement to Rules of User Conduct, <http://www.aol.com/copyright/rules.html> (last visited Mar. 6, 2009).

172. Comcast, Comcast High-Speed Internet Acceptable Use Policy, <http://www.comcast.net/terms/use> (last visited Mar. 6, 2009).

173. Nunziato, *supra* note 13, at 1121–22; *see also* CDA, 47 U.S.C. § 230(c)(2)(A) (2000) (precluding ISPs from civil liability for restricting access to certain material “whether or not such material is constitutionally protected”).

174. *See supra* notes 78–84 and accompanying text.

175. *See* Press Release, Time Warner, America Online and Time Warner Complete Merger to Create AOL Time Warner (Jan. 11, 2001), *available at* <http://www.timewarner.com/corp/newsroom/pr/0,20812,668364,00.html> (detailing the creation of “the world’s first Internet-powered media and communications company”). For more on the concentration of the media and the resulting bias in coverage, *see generally* the many works of journalist and commentator Bill Moyers. *E.g.*, Bill Moyers, Closing Address at the National Conference on Media Reform: Take Public Broadcasting Back (May 15, 2005), *available at* <http://www.commondreams.org/views05/0516-34.htm>; Bill Moyers, Keynote Address to the National Conference on Media Reform (Nov. 8, 2003), *available at* <http://www.commondreams.org/views03/1112-10.htm>.

model.¹⁷⁶ Concerns about government intervention into the terms of private contracts¹⁷⁷ carry much less weight when one considers the lack of bargaining power that individual end users have relative to the ISPs that provide them with Internet access. An end user cannot simply suggest a less restrictive counteroffer if he or she does not like an ISP's contract terms; users truly have no choice but to accept the terms and conditions offered by the ISP or forego Internet access completely.¹⁷⁸ In our increasingly technologically driven society, the latter is not a very plausible alternative. Consequently, most Internet users are simply forced to accept the terms of service as offered.

Thus, the ability to choose among a handful of ISPs' strikingly similar terms does little to allay end users' fears of potential abuse created by the broad terms of their contracts. Furthermore, most Internet users do not even bother to read an ISP's terms of service, much less choose one ISP over another because of a preference among these conditions.¹⁷⁹ No doubt recognizing this, ISPs are incentivized to compete based on price and product quality rather than on the terms of use that bind the customer.¹⁸⁰

Hence, the invisible hand of the market has not resulted in any real differences among ISPs in terms of access to content. This utter lack of meaningful choice, coupled with the nonexistence of any possibility for bargaining, shows that the "free market" forces at work here do not benefit the consumer interested in freedom of expression.¹⁸¹ Similarly, the inherent self-interest associated with "free market" forces further motivates ISPs to exercise their discretion at the expense of truly free speech.

C. Profit Maximizing and Indirect Censorship

Indirect censorship poses perhaps an even greater concern than the direct filtering of content inherent in this "free market" model of Internet regulation. Indirect censorship occurs in two

176. See Nunziato, *supra* note 13, at 1121–22 (noting the similarity of restrictions on speech imposed by different ISPs).

177. See Powell, *supra* note 157, at 10 (arguing that government regulation of private contracts "is probably the most fundamental intrusion on the free market").

178. See Netanel, *supra* note 12, at 437 (observing that users "have only the choice of accepting or rejecting the terms, not negotiating changes").

179. Cf. *id.* at 435 (noting that most Internet users do not read a website's conditions of use nor choose one website over another based on a preference among these conditions).

180. *Id.* at 437.

181. Compare Powell, *supra* note 157, at 10 (suggesting that the "free market" should rule), with Balkin, *supra* note 7, at 20 (arguing that such a system "subordinates freedom of expression to the protection and defense of capital accumulation").

ways. Both stem from the fact that ISPs are often also content providers, or at least affiliated with content providers.¹⁸² This, in turn, creates incentives for ISPs to favor their own content over that of others. First, ISPs may give preferential treatment to certain content as it flows through the network itself, creating a virtual “fast lane” for material coming from the ISP or its affiliates, while slowing down or even outright blocking content coming from competitors or other independent Internet speakers.¹⁸³ Second, a related—and even more important for the current discussion—concern is that ISPs may direct users through a maze of links in which the ISP’s subsidiaries and affiliates are given high priority.¹⁸⁴

Essentially, ISPs may create “walled gardens” or “managed content areas” limiting users’ access to content provided by the ISP and its partners.¹⁸⁵ Cisco Systems, for example, has

182. See Balkin, *supra* note 7, at 21 (“[T]elecommunication enterprises are hybrids of content providers and conduits for the speech of others.”).

183. *Id.* A voluminous amount of literature discusses the arguments associated with the government compelling free access to the privately owned infrastructure of the Internet, commonly known as the “net neutrality” debate. See, e.g., LESSIG, *supra* note 37, at 236, 255–56 (arguing the “architecture of cyberspace is the real protector of speech [in cyberspace]” and that publicly required filters are less expensive and less overinclusive than private filters, and therefore better at protecting free speech); Peter Linzer, *From the Gutenberg Bible to Net Neutrality—How Technology Makes Law and Why English Majors Need to Understand It*, 39 MCGEORGE L. REV. 1, 22–24 (2008) (outlining the debate between groups calling for legally enforced net neutrality and those advocating free market based net neutrality, and warning of previous government blunders in regulating communication); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 145–46, 165–68 (2003) (arguing that net neutrality is needed for innovation and proposing an antidiscrimination rule to achieve net neutrality by “forbid[ding] broadband operators, absent a showing of harm, from restricting what users do with their Internet connection”); Yoo, *supra* note 3, at 46 (“The impossibility of technologically neutral government intervention undercuts claims that imposing the end-to-end argument as a regulatory mandate represents the proper way to show humility about the future of the Internet.”); see also JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 69–73 (2006) (demonstrating that, despite early expectations that the Internet would render territorial governments obsolete, governments can effectively restrict Internet content across the globe by controlling local intermediaries such as ISPs). While this Comment will not attempt to assert a position in this highly technical, highly controversial dispute, it is worth mentioning as an aspect of the very real danger presented by the “free market” system described above. See *supra* Part V.B.

184. Balkin, *supra* note 7, at 21–23 (describing the ISPs’ profit maximizing interests in indirect censorship).

185. *Id.* at 21. Tim Berners-Lee, the man credited with inventing the World Wide Web, described the problem in terms of an ISP that did not regulate content as compared to an ISP owned by a cable company seeking to promote its own agenda: “[U]sers through an [unbiased] ISP can access independent movies on any site that offers them By contrast, a cable TV company acting as an ISP could block such access, because it wants subscribers to select the pay-per-view movies it alone offers.” John Cox, *Web Guru Berners-Lee Warns Against “Walled Gardens” for the Mobile Internet*, NETWORKWORLD.COM,

attempted to control the end user's Internet experience by creating "captive portals," which, in the company's own words, give the ISP "the ability to advertise services, build its brand, and *own the user experience*."¹⁸⁶ This means the ISP directs the end user to link after link of content that is comparable to what he or she was looking for, though not necessarily precisely what the user would have chosen if given total free choice.¹⁸⁷ In this manner, ISPs can effectively control "who gets to see what programming and under what terms."¹⁸⁸ The ISP's "goal is not simple ideological censorship," but rather diverting users "into a continuous series of offers to consume goods and services from which the [ISP] will glean profits."¹⁸⁹ Unfortunately, these systems may actually be growing in popularity, as it was recently announced that even "Google is embracing the 'walled garden' approach."¹⁹⁰

Because most Internet users are unaware of these settings or simply do not have the technical know-how to change them, the software giants can easily get away with these abuses in connection with the majority of their customers.¹⁹¹ Lack of knowledge and consent makes indirect censorship potentially far more dangerous than direct censorship. End users are even more unlikely to recognize that they are being prevented from accessing the exact content they are looking for, as opposed to what the ISP and its affiliates have to offer, however similar that content may be. The issue is particularly problematic because, in the "free market" state that presently exists on the Internet, media corporations will naturally "seek to limit forms of participation and cultural innovation that are inconsistent with their economic interests."¹⁹² Therefore, smaller content providers are less likely to have their voices heard by virtue of being

Nov. 14, 2007, <http://www.networkworld.com/news/2007/111407-berners-lee-mobile-internet.html>.

186. Balkin, *supra* note 7, at 22 (emphasis added) (quoting Data Sheet, Cisco 6400 Service Selection Gateway, http://sysdoc.doors.ch/CISCO/c6510_ds.pdf).

187. *See* Balkin, *supra* note 7, at 22.

188. *Id.*

189. *Id.* This concept is of particular concern as more and more Internet users access the web through ISPs owned by cable television and cellular telephone providers. The danger lies in the fact that such providers necessarily have other interests that are not always compatible with unrestricted Internet access. Therefore, they often set up their systems so that "subscribers can only use devices authorized by the carrier, and can only access content and services authorized by the carrier." Cox, *supra* note 185.

190. Billy Marshall, Cloud Computing Casts Shadow on Walled Gardens, <http://web2.sys-con.com/node/558455> (Aug. 16, 2008, 17:00 EST).

191. *See* Netanel, *supra* note 12, at 435 (describing typical Internet users' failure to assess and compare such regulatory regimes).

192. Balkin, *supra* note 7, at 22.

unaffiliated with a major corporation providing Internet service or access, and their rights as speakers are thereby violated.¹⁹³ Furthermore, ISPs complicate end users' ability to access content, thus also violating the users' rights as listeners.¹⁹⁴

VII. SUGGESTIONS FOR A FREER INTERNET:
APPLYING OUR MODEL OF INTERNET
FREEDOM TOWARDS A SYSTEM OF
USER-CONTROLLED INTERNET REGULATION

In articulating the government's position on net neutrality, then-FCC Chairman Michael Powell issued a challenge to the broadband network industry to preserve four fundamental "Internet Freedoms."¹⁹⁵ The first essential freedom he cited, and the most relevant to the present discussion, is the "Freedom to Access Content."¹⁹⁶ While asserting that all "legal content" should be made available to users, he nevertheless noted that ISPs sometimes must include "reasonable limits" in their service contracts in order to "manage their networks and ensure quality experiences."¹⁹⁷ But, Powell conceded, "[S]uch restraints should be clearly spelled out and should be as minimal as necessary."¹⁹⁸ As discussed above, the limits included in most ISPs' service contracts are neither "reasonable" nor "as minimal as necessary." Rather, their terms provide for the ISPs' sole discretion over a myriad of matters that they may find subjectively inappropriate, regardless of whether the content is constitutional or otherwise lawful.¹⁹⁹ The government therefore must implement some regulatory controls over the ISPs and empower individual Internet users to control their own access to content.

A. *Prohibiting Private Censorship*

In order for true freedom to access content to exist, access must be universal in nature. In other words, to fully realize the government's stated goal of free access, the content available on the Internet must be unfettered by restrictions, public or private,

193. See *supra* note 141 and accompanying text (discussing First Amendment rights to speak and listen).

194. See *supra* note 141 and accompanying text.

195. Powell, *supra* note 157, at 11.

196. *Id.* The other three are the Freedom to Use Applications, the Freedom to Attach Personal Devices, and the Freedom to Obtain Service Plan Information. *Id.* at 11–12.

197. *Id.* at 11.

198. *Id.*

199. See *supra* notes 168–81 and accompanying text (discussing the broad discretion ISPs give themselves in their nonnegotiable service contracts to regulate content).

except where absolutely necessary.²⁰⁰ This notion is fundamentally at odds with the government's provision of total immunity for ISPs filtering content as expressed in Section 230.²⁰¹ If Congress had indeed been motivated by a desire to protect freedom of expression on the Internet,²⁰² it should have provided immunity only to ISPs that exercised their discretion to *host* constitutionally protected, though otherwise objectionable, material. Instead, Congress granted immunity to ISPs exercising their discretion to *remove* material that they find objectionable, irrespective of its constitutional status. As such, Section 230 gives ISPs an unprecedented—and unnecessary—level of power in controlling the content accessible to end users online.²⁰³ This obvious disregard for the Internet's potential as a democratizing, participatory mechanism of free speech clearly goes against both the stated goal of Section 230 and the values embodied in the First Amendment.²⁰⁴ Therefore, Section 230 should be amended to reflect Congress's stated intent of promoting freedom of expression online.

Under the current regulatory scheme, ISPs have few incentives to provide free access to content because they boast immunity from civil suit,²⁰⁵ and the market forces that would otherwise control them are essentially null and void in this context.²⁰⁶ Thus, in order to promote freedom of expression on the Internet, Congress should require ISPs to provide access to the full range of content available on the Internet. In other words, Congress should mandate that ISPs provide access no more narrowly than the First Amendment would permit if the Internet were owned and operated by the government. Absent an express agreement by the end user to forego this level of access, it is not the place of private companies to limit the user's ability to send or receive Internet speech.²⁰⁷

200. See *supra* Part III (outlining necessary regulations of content).

201. See *supra* Part V.B (examining the congressional grant of immunity to ISPs under Section 230).

202. See *supra* Part V.B.1 (noting legislative intent and judicial interpretation of Congress's goal of promoting free expression through Section 230).

203. See *supra* Part V.B.2 (identifying the dangerous level of deference granted to ISPs).

204. See *supra* Part II (assessing characteristics of the Internet that promote freedom of expression).

205. See *supra* Part V.B.2 (analyzing implications of congressional grant of immunity to ISPs under Section 230).

206. See *supra* Part VI (illustrating inability of free market to constrain regulatory measures implemented by ISPs).

207. Of course, many users may not want to be exposed to a great deal of the content available online, and they should be free to contract away this level of access.

The potential danger of the government completely taking over the market is no less ominous. However, by mandating access only to the extent required of public actors by the First Amendment, the government can rein in the problem of market concentration while at the same time maintaining a free market for online speech. Still, less drastic measures may be more realistic and almost as effective.

B. Allowing Civil Liability for Private Censorship

While regulation per se may not necessarily be the answer, Congress should implement no less than a retraction of the previous affirmative steps it has taken to encourage private restriction of constitutionally protected speech. In particular, Congress should discourage ISPs from censoring content on the Internet, either directly or indirectly, without the user's knowledge and consent: Failure to obtain such informed consent before restricting access should subject ISPs to civil liability. Thus, Section 230 should, at the very least, be limited in scope to include a clear, obvious, and understandable user-notice provision. An exception to immunity from suit should then apply to violations of the notice provision. A touchstone of this proposal is the judicial review afforded by liability. Far from blanket immunity for ISPs, the real key to promoting free speech online is subjecting ISPs' censorship decisions to reasoned review by impartial courts.

C. Developing Technology and Educating End Users

Furthermore, federal Internet policy would be better served if geared more toward promoting transparent user-controlled filtration software and widespread public knowledge of the problems inherent in filtering.²⁰⁸ Regulations of this nature comport better with Congress's stated purpose of "maximiz[ing] user control over what information is received."²⁰⁹ Similarly, this would help advance the FCC's goal of providing end users "Freedom to Access Content" on the Internet²¹⁰ much more effectively than the current policy, which allows the private

Nevertheless, the sensibilities of a few must not be permitted to dictate the extent of the freedom of many. *See* *Cohen v. California*, 403 U.S. 15, 21 (1971) (asserting that people offended by certain content "could effectively avoid further bombardment of their sensibilities simply by averting their eyes").

208. *See supra* note 65 and accompanying text (addressing the Supreme Court's endorsement of such strategies in *Ashcroft v. ACLU*, 542 U.S. 656 (2004)).

209. CDA, 47 U.S.C. § 230(b)(3) (2000).

210. Powell, *supra* note 157, at 11.

corporations in charge of the Internet's infrastructure to do whatever they want without any fear of consequences for abuses.²¹¹

This is not to suggest that content restrictions are undesirable under all circumstances. Certainly, parents should have the power to prevent their underage children from viewing content on the Internet that they deem inappropriate. But parents must determine what constitutes "objectionable" content rather than deferring the decision to some private electronic media corporation. Parental censorship, therefore, constitutes a superior substitute and prevents ISPs from imposing their conception of morality onto children.²¹² Absolutely, end users should be made aware of their options to protect themselves from content they do not wish to encounter. Furthermore, users should not need a degree in computer science to understand these options and achieve this goal. But the more knowledgeable, mature, and thick-skinned users should not have a minority view of what constitutes "inappropriate" content imposed on them in the name of protecting the ignorant.

In order to achieve these objectives, federal policies must seek to promote user awareness and disseminate public information about new technologies associated with the Internet. The fact that many Internet users are ignorant of the capacity for self-imposed regulation, or are insufficiently computer savvy to carry it out, does not justify allowing corporations such as ISPs and other access providers to perform this task in their stead.²¹³ On the contrary, Internet illiteracy is largely disappearing as a new generation of Internet users grows up experiencing the effects of the technological revolution on a daily basis. Software has become increasingly user friendly and the excuses for failing to monitor one's own (or one's children's) activities online are rapidly disappearing. Federal policy, therefore, must endeavor to further this progression in end user competency, rather than continue with the tired notion that ISPs are the only ones

211. See *supra* notes 112–22 and accompanying text (discussing Section 230's provision granting total immunity to ISPs for content restrictions).

212. See *Reno v. ACLU (Reno II)*, 521 U.S. 844, 878–79 (1997) (striking down portions of the CDA in part because the government's blanket content restrictions took the power to decide what constitutes "indecent" or "patently offensive" content to minors out of the hands of parents); *Ginsberg v. New York*, 390 U.S. 629, 639 (1968) ("[T]he parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society."); cf. Powell, *supra* note 157, at 16 (noting the importance of balancing the role of parental versus governmental control).

213. See Netanel, *supra* note 12, at 435 (observing lack of computer literacy typical of many Internet users).

capable of protecting users from “inappropriate” Internet content.²¹⁴

D. Addressing the Concerns of the ISPs

The ISPs pushing for freedom from government regulation in any form often claim the “free market” system is necessary to promote innovation.²¹⁵ While continual innovation is certainly of vital importance in the realm of technology, this goal may be pursued without the risk of sacrificing access to content, which inheres in the uncompromising “free market” approach.²¹⁶ This goal could be better served, for example, through incentive programs or government subsidies for private research and development of appropriate filtering software to companies who prove themselves dedicated to freedom of expression on the Internet. In this manner, the government could further its objective of facilitating user control over the information accessible on the Internet,²¹⁷ while at the same time avoiding the negative consequences of allowing filtering technology developers to go unchecked.²¹⁸

From a freedom of expression standpoint, such a strategy would serve a dual role. First, it would promote positive regulatory growth by facilitating the development of less intrusive, more user-friendly filtering software, which in turn would help restore power to the hands of the end user. Second, it would provide a stronger nexus between government and industry for purposes of the state action doctrine, thereby making it more likely that the judiciary would afford First Amendment protections to both the Internet content providers and the users potentially subjected to such filters.²¹⁹

214. Such user-education programs are not only practical, but also feasible. In Australia, for example, the government recently announced a plan to provide free filtering software to any family that wanted to use it on their home computer. See Patrick Gray, *Australia to Give Away Porn-Filtering Software*, CNET NEWS.COM, June 21, 2006, http://news.cnet.com/Australia-to-gove-away-pron-filtering-software/2100-1028_3-6086259.html. Such a plan could easily be implemented in the United States and is far preferable to permitting ISPs to regulate what content those home computers may access.

215. See Linzer, *supra* note 183, at 22–23 (noting that ISPs argue government regulations would “restrict progress”).

216. See *supra* Part VI (describing dangers of the “free market” system in the Internet context).

217. See CDA, 47 U.S.C. § 230(b) (2000).

218. See *supra* notes 160–81 and accompanying text (discussing negative consequences of allowing media corporations free rein with regard to the Internet).

219. See *supra* Part V.C (analyzing the state action doctrine); see also *Cyber Promotions, Inc. v. Am. Online, Inc.*, 948 F. Supp. 436, 442 n.2 (E.D. Pa. 1996) (recognizing the existence of an elaborate financial or regulatory relationship between the

E. Summary

In order for the Internet to achieve its potential as a democratizing, participatory communication medium, dissenting opinions must not be censored simply because they are unpopular.²²⁰ The government must not allow ISPs to have free rein, but rather should urge ISPs to use their extreme power and market share to develop better technologies that will help end users who desire a level of content filtering to impose it upon themselves.²²¹ Government programs, in turn, should seek to encourage the development of this type of software, not merely in a nominal sense, but in a meaningful and practical way.

Thus, by enacting legislative and administrative policies that promote popular participation in the design of communication technologies geared towards facilitating decentralized control, the government may play an affirmative role in achieving its stated policy ambitions.²²² This in turn will give the judiciary the tools it needs to recognize and combat unnecessary restriction of access to content online, and ultimately promote the goal of a truly free Internet.²²³

VIII. CONCLUSION

The Internet is a permanent force in our society and must be handled carefully and effectively. Now more than ever it is imperative that measures be taken to ensure that the public is aware of the vast power at its fingertips, as well as the various methods of regulating content available to them. In this way, the power to define what constitutes “objectionable” or “inappropriate” content can be retained by the individual, rather than simply passed off to corporations who have shown that they are more interested in maximizing profits than promoting public welfare.²²⁴

state and the private actor as a factor in the state action analysis).

220. See *ACLU v. Reno (Reno I)*, 929 F. Supp. 824, 881 (E.D. Pa. 1996) (Dalzell, J., concurring) (describing the Internet as “the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen”); Balkin, *supra* note 7, at 3 (discussing the “promise of the digital age for the realization of a truly participatory culture”); *id.* at 47 (“Dissent is central to . . . free speech.”); Palfrey & Rogoyski, *supra* note 3, at 56 (noting “the Internet’s democratizing potential”).

221. See *supra* Part VI.B (discussing the extreme power of ISPs due to lack of meaningful choice).

222. See CDA, 47 U.S.C. § 230(b) (2000) (outlining Congress’s goals of promoting technologies that maximize user control over content and empower parents to restrict children’s access to objectionable material).

223. See Balkin, *supra* note 7, at 51 (discussing legislative, administrative, technological, and judicial means of promoting freedom of expression).

224. See *supra* Part VI (identifying the dangers of granting media corporations the

Current federal policies run counter to their own stated goals.²²⁵ While these goals seem admirable on their face, they are no more than lip service if the actual effect of the policies does not reflect their intended purpose.²²⁶ This is exactly the case with the current system, which purports to promote freedom of access to and personal control of the Internet experience, while in reality simply deferring to the private corporations in charge of the Internet as the final arbiters of Internet content regulation and, ultimately, of our national sense of what is acceptable.²²⁷ The primary danger of the current system is the potential for both direct and indirect censorship at the hands of unconstrained private ISPs. This problem is magnified by the fact that most Internet users have no idea when content is being blocked. The lack of meaningful choice for end users in selecting a company from which to acquire Internet access further renders the “free market” model of regulation ineffective.

Because of the great potential for abuse by private entities concerned with maximizing profits, the government should take affirmative steps to protect freedom of speech on the Internet. This could be accomplished in a number of ways. For example, a statute forbidding ISPs from restricting access to content that would otherwise be protected by the First Amendment would promote consumer access to online speech. At the very least, the ISPs should be required to inform their customers when they block access to certain content. Failure to do so should subject them to civil liability. Finally, federal policies should encourage software developers to make unrestrictive, user-friendly filtering programs, and provide parents with the information necessary to effectively implement such programs vis-à-vis their children. Strategies such as these will facilitate the realization of the Internet’s long-recognized potential as “the most participatory form of mass speech yet developed.”²²⁸

Nicholas P. Dickerson

freedom to regulate content at their will).

225. See *supra* note 112 and accompanying text.

226. See *supra* notes 112–22 and accompanying text (disparaging terms of Section 230 as inconsistent with congressional policy goals stated therein).

227. See CDA, 47 U.S.C. § 230(b) (2000) (outlining Congress’s policies); Powell, *supra* note 157, at 11 (asserting the FCC’s goal of promoting Freedom to Access Content on the Internet); see also *supra* notes 116–22 and accompanying text (arguing that immunizing ISPs from all liability facilitates unrestrained censorship of constitutionally protected speech).

228. *ACLU v. Reno (Reno I)*, 929 F. Supp. 824, 883 (E.D. Pa. 1996) (Dalzell, J., concurring).