REVISITING USER CONTROL: THE EMERGENCE AND SUCCESS OF A FIRST AMENDMENT THEORY FOR THE INTERNET AGE

JOHN B. MORRIS, JR. & CYNTHIA M. WONG*

INTRODUCTION

In 1995, when the popular, commercial Internet was just emerging, concerns about protecting children online were already on legislative agendas, and no one knew exactly what level of First Amendment protection courts would afford this new form of mass communication. That year, two public policy advocates, Jerry Berman and Daniel Weitzner, argued in the *Yale Law Journal* that the Internet's technical characteristics, including abundance of capacity and a high level of individual user control, meant that online speech should receive the highest level of protection under the First Amendment—protection comparable to print.[1]

In the years since then, the concept of user control—or "user empowerment"—has been central to numerous decisions protecting speech in the online environment, from the United States Supreme Court on down.[2] Under this theory, if technology

* The authors are, respectively, General Counsel and Ron Plesser Fellow of the Center for Democracy and Technology (CDT), a non-profit public interest organization that works to keep the Internet open, innovative, and free. The authors of the 1995 *Yale Law Journal* article discussed in this essay, Jerry Berman and Daniel Weitzner, were co-founders and initial leaders of CDT. Berman continues as Chair of CDT's Board of Directors.

1. Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L. J. 1619, 1626-29 (1995).

2. *See, e.g.*, Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 668-69 (2004) (holding that filtering software was a less restrictive method of protecting

can provide users (and parents) with the ability to control what they (and their children) access online, government regulation of content would be unconstitutional. Arguments against and criticisms of this constitutional theory have been advanced,[3] but the idea that users and parents—and not the government—should control what children access online remains the dominant rationale for courts to protect speech online. This essay looks at the origins and application of the "user control" theory in the online context and how the theory has fared the test of time. We conclude that "user control" on the Internet is as vital and important today as it was when Berman and Weitzner first advanced the theory fifteen years ago.

---

children from indecent material and that the government failed to prove the software was so deficient as to indicate otherwise); Reno v. ACLU (*CDA*), 521 U.S. 844, 879 (1997) (finding there were less restrictive means than content-based restrictions to protect children from indecent material, such as parental control filters); ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008) (same), *cert. denied*, 129 S. Ct. 1032 (2009); ACLU v. Gonzales, 478 F. Supp. 2d 775, 794-97 (E.D. Pa. 2007) (discussing the effectiveness of filtering software as a less restrictive method of protecting children from indecent material), *aff'd sub nom.* ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008); ACLU v. Reno*,* 31 F. Supp. 2d 473 (E.D. Pa. 1999) (preferring filtering software to the more restrictive provisions of the Child Online Protection Act), *aff'd,* 217 F.3d 162 (3d Cir. 2000), *aff'd and remanded sub nom.* Ashcroft v. ACLU, 542 U.S. 656 (2004).

3. For example, in defending the Child Online Protection Act (COPA), the government argued that user control tools (i.e., filtering software) are not an available effective alternative because such tools are not perfectly effective in that they both over- and under-block; not all parents use filtering tools; such tools can be circumvented; and such tools are already part of the "status quo" that Congress found ineffective at protecting minors. Brief for Appellant at 43-56, ACLU v. Mukasey, 534 F.3d 181 (3d. Cir. 2008) (No. 07-2539). *See also* Ashcroft v. ACLU (*COPA*), 542 U.S. at 669–70 (rejecting the government's argument that filtering software was less effective); ACLU v. Mukasey, 534 F.3d at 203–204 (same). We discuss criticisms of the user control theory in more depth in Part IV, *infra*.

I.THE "USER CONTROL" THEORY IN THE ONLINE CONTEXT

The First Amendment protects against overreaching by the government to censor or control content. A key concept underlying this protection has been that the listener—the "user"—should choose what content is worth the listener's time.[4] As the Supreme Court has explained, "[a]t the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence."[5] Under the First Amendment, "[c]ontent-based regulations are presumptively invalid"[6] and are subject to strict scrutiny:

> [A] content-based speech restriction . . . can stand only if it satisfies strict scrutiny. If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest. If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative. To do otherwise would be to restrict speech without an adequate justification, a course the First Amendment does not permit.[7]

Thus, under the First Amendment, the government is not free to substitute itself for listeners and decide what they should be able to hear.

---

4. *See, e.g.*, Cohen v. California, 403 U.S. 15, 24 (1971) ("The constitutional right to free expression . . . is designed and intended to remove governmental restraints from the arena of public discussion, putting the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity . . . .").

5. Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 641 (1994).

6. R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) (citations omitted).

7. United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813 (2000) (citations omitted).

But in *FCC v. Pacifica Foundation*,[8] the Supreme Court considered how the First Amendment would apply in the broadcast context. In that case, a plurality of the Court relied on the flip-side of this approach to *uphold* a governmental content regulation, based on its conclusion that listeners *lacked* control over what content they would receive.[9] In *Pacifica*, the plurality held that the Federal Communications Commission (FCC) could prohibit the radio broadcast of George Carlin's "Seven Dirty Words" monologue. The plurality was concerned that, given the nature of the broadcast medium of content delivery, content would "assault" a listener (or viewer) in his or her home.[10] It concluded that broadcast content had a "uniquely pervasive presence" that came into a person's home, and over which the person had no control.[11] Because of this asserted lack of control, the Court did not apply "strict scrutiny," and decided that the government could step in and regulate content in this narrow context.[12]

It was into this legal landscape—with the broadcast medium, because of its particular characteristics, receiving less First Amendment protection than the print medium—that the popular Internet emerged. And it was this landscape that Berman and Weitzner confronted in their 1995 essay, "Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media."[13]

In 1995, it was far from clear what First Amendment standards would apply to the emerging online environment. It was also equally unclear exactly what form the online world would

8. 438 U.S. 726 (1978).

9. *Id.* at 748–50. In a narrowly-drawn holding, a plurality of the Court upheld FCC sanctions against a broadcaster for airing indecent material because the listener could not be adequately protected from unexpected program content due to the "pervasive" nature of broadcast and because the broadcast medium was "uniquely accessible to children." *Id.*

10. *See id.* at 748-49.

11. *See id.* at 749-50. In his dissent in *Pacifica*, Justice Brennan argued that the viewer indeed had control over access to content—the on/off switch—but that was not sufficient for the Court. *See id.* at 765 (Brennan, J., dissenting).

12. *Id.* at 748-50 (majority opinion).

13. Berman & Weitzner, *supra* note 1.

ultimately take. America Online (AOL) was rising as the leading path for consumers into the online environment, but it was only taking hesitant steps to allow its users to step outside of its "walled garden" of content to access the Internet directly. Other online services—such as CompuServe and Prodigy—competed with AOL, and pure Internet access (as is common today) was still used mainly by academics and more technically advanced users.[14]

In their article, Berman and Weitzner pursued two simultaneous goals: first, to urge courts (and policymakers) to bestow the highest level of First Amendment protection on the new media, and second, and of equal importance, to urge the architects of the new media to build into new media technical characteristics that would make it deserving of that full constitutional protection. As the authors noted, they were offering "a First Amendment wish list for the age of interactive media."[15]

Berman and Weitzner focused their arguments on two critical factors—abundance and user control:

> In order for interactive media to develop with the diversity-enhancing characteristics of a medium such as print—and to win strong First Amendment protections from regulation like those accorded to print—their architecture must have two key characteristics. First, the architecture must be open and decentralized, promoting a true abundance of information and communication opportunities. Second, there must be sufficient user control to enable users to choose what information they want to receive, and what they want to keep out, thus eliminating the rationale for government to

14. Indeed, in their article, Berman and Weitzner seldom used the term "Internet," focusing instead on broader terms "interactive media" and "new media." *See* Berman & Weitzner, *supra* note 1, at 1619 n.1. This distinction becomes all the more important today as digital content is increasingly available across a wide array of interactive platforms and devices, a development with which both policymakers and the market for user control tools must contend.

15. *Id.* at 1635.

> step in and protect various parts of society with intrusive content regulations.[16]

Their first point—that the new media must be open, decentralized, and abundant—remains a critical concern today, and those goals lie at the heart of ongoing battles about "network neutrality" and the risk that access providers will act as bottlenecks and gatekeepers over users' online choices. A loss of openness or neutrality would pose serious challenges to free speech online,[17] but to date, these factors have not been a significant focus of courts in analyzing First Amendment claims in the online context.

In contrast, Berman and Weitzner's second focus—user control—has been a central issue in many of the leading First Amendment cases about the Internet. Laying the groundwork for those cases, they argued that "[i]nteractive media differ from mass media in that they offer users a great degree of control over the content that users and their children receive,"[18] and they describe a range of emerging filtering and other technologies that could provide robust user controls.[19] As Berman and Weitzner explain:

> User-control technologies enable customers (in particular, parents) to limit access to certain kinds of material on their . . . PCs. With such control mechanisms within the practical reach of parents, the goal of indecency regulations—the protection of children—could be achieved without intrusive government restrictions. In interactive media, the reasoning of *Pacifica* . . . would not justify content regulation at all, whether it is regulation of sexual expression,

16. *Id.* at 1621.

17. *See generally* John B. Morris, Jr. & Jerry Berman, *The Broadband Internet: The End of the Equal Voice?*, *in* PROCEEDINGS OF THE TENTH CONFERENCE ON COMPUTERS, FREEDOM & PRIVACY: CHALLENGING THE ASSUMPTIONS 119 (2000), *available at* http://www.cdt.org/publications/broadbandinternet.pdf (discussing free speech risks posed by a loss of open and neutral access).

18. Berman & Weitzner, *supra* note 1, at 1629.

19. *Id.* at 1632-34.

> violence, commercial speech, or other controversial materials.[20]

Berman and Weitzner were concerned, though, that "political pressures [would] threaten to introduce draconian regulations into these new media before user-control mechanisms have a chance to take hold."[21] They were particularly concerned about the "Exon Amendment" (named after its lead sponsor, Senator James Exon), which ultimately passed as the Communications Decency Act of 1996 (CDA) and was signed into law early in that year.[22] The CDA and the resulting legal challenges to it would prove to be the first significant test of the user control theory in the online context.

II.USER CONTROL IN THE COURTS

The Communications Decency Act (CDA) was signed into law in January 1996 and was challenged immediately in a suit filed in Philadelphia by the American Civil Liberties Union (ACLU).[23] Congress, anticipating that the CDA would draw a constitutional challenge, had provided that a three-judge district court panel would hear the case, with direct review by the Supreme Court.[24]

The CDA criminalized the dissemination of "indecent" material in a way that rendered such material "available" to minors.[25] But, because speakers on the Internet had no way to screen out minors, and thus all content was "available" to them, the practical effect of the CDA would have been to reduce online content to a level appropriate for a child.

As Berman and Weitzner had anticipated, the need to determine what First Amendment standard should be applied to the Internet arose immediately in the *CDA* case—in the very first

---

20. *Id.* at 1634.

21. *Id.*

22. Communications Decency Act of 1996, Pub. L. No. 104-104, § 505, 110 Stat. 133, 142 (1996).

23. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).

24. 47 U.S.C. § 561 (2006).

25. *Id.*

filing made by the U.S. Department of Justice to defend the law.[26] Opposing a motion for a temporary restraining order against enforcement of the CDA, the Department of Justice argued that the case presented "compelling parallels" to the *FCC v. Pacifica Foundation* decision, which applied a lower level of constitutional protection to the broadcast medium.[27] The government argued that the Internet was pervasive and readily available to children (as the Supreme Court had noted about broadcast in *Pacifica*).[28] In later briefing, the government reiterated its *Pacifica* argument:

> The approach Congress enacted [in the CDA] is constitutional under *Pacifica*. Like broadcast stations, the Internet is establishing an increasingly "pervasive presence" in the lives of Americans. . . . Like indecency presented on broadcast stations, indecent material presented over the Internet "confronts the citizen in the privacy of the home." Like broadcast stations, the Internet "is uniquely accessible to children."[29]

The district court granted the ACLU's motion for a temporary restraining order against enforcement of the CDA.[30] Soon thereafter, a second lawsuit was filed in the same court challenging the CDA, and both cases were consolidated for trial. A key purpose of the second suit was to emphasize the user control arguments against the CDA—and against the application of *Pacifica* to the Internet.[31]

---

26. *See* Defendant's Opposition to Plaintiffs' Motion for a Temporary Restraining Order, ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996) (No. 96-963), *available at* http://www.eff.org/legal/cases/EFF_ACLU_v_DoJ/960214_doj_opposition.brief.

27. *Id.*

28. *Id.*

29. Brief for the Appellants, Reno v. ACLU (*CDA*), 521 U.S. 844 (1997) (No. 96-511), 1997 WL 32931 (citation omitted).

30. ACLU v. Reno, 929 F. Supp. 824, 838-42 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

31. *See, e.g.*, Plaintiffs' Memorandum of Law in Support of Their Motion for a Preliminary Injunction at 72, American Library Association v. U.S. Dep't

In the course of that lawsuit, the three-judge district court panel received extensive evidence of user control tools and capabilities, including both parental empowerment options built into leading online services such as AOL, and stand-alone software programs such as "CYBERsitter" and "Net Nanny."[32] In striking down the CDA as unconstitutional, the court included extensive findings of fact concerning such user empowerment tools and concluded: "Despite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available."[33]

One judge explained: "As we learned at the hearing, parents can install blocking software on their home computers, or they can subscribe to commercial online services that provide parental controls. It is quite clear that powerful market forces are at work to expand parental options to deal with these legitimate concerns."[34]

In upholding the judgment that the CDA was unconstitutional, the Supreme Court specifically acknowledged the significance of "user-based" tools that allow parents to control

---

of Justice, 929 F. Supp. 824 (E.D. Pa. 1996) (No. 96-963), *available at* http://w2.eff.org/legal/cases/EFF_ACLU_v_DoJ/ala_030196_injunction.brief (emphasizing "user-based tools that empower parents to control their children's online activities based on the parents' views of what is appropriate for their children").

Berman and Weitzner, early proponents of the "user control" approach, were also instrumental organizers of the second lawsuit, which was filed on behalf of the American Library Association, America Online, and many other leading online companies and organizations. Berman and Weitzner's group, the Center for Democracy & Technology (CDT), coordinated the second suit and retained Jenner & Block LLP to represent the plaintiffs. One of this article's authors, John Morris—then at Jenner & Block—served with his partners, Bruce Ennis and Ann Kappler, as lead counsel in the case.

32. *See Reno*, 929 F. Supp. at 838-42 (detailing extensive evidence of user control technology).

33. *Id.* at 842.

34. *Id.* at 883.

access to content.[35] Although the Court did not focus much attention on user control technology, it did squarely reject the *Pacifica* "lack of control" rationale for governmental regulations. Writing for the Court, Justice Stevens held that the "factors [found in *Pacifica*] are not present in cyberspace," and specifically that "the Internet is not as 'invasive' as radio or television. The district court specifically found that '[c]ommunications over the Internet do not '"invade'" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content '"by accident.'"[36]

In two subsequent cases, the Supreme Court has more directly confronted and squarely validated the user control theory. First in a case involving cable television regulation, and then in a legal challenge to the "son of CDA," the Child Online Protection Act (COPA),[37] the Court has made plain that promoting user- and parental-empowerment technology is a constitutionally "less restrictive alternative" to government regulation of content.

In *United States v. Playboy Entertainment Group, Inc.*,[38] the statute required a cable company to block access by *all* households to lawful sexual content during certain hours of the day in an effort to protect children. The crucial fact in the case was that wholly independent from (and as an alternative to) the system-wide prohibition challenged in the case, parents could direct the cable company to block the entire channel, just for their individual house. The Supreme Court struck down as unconstitutional the mandated blocking requirement because individual parents had the means (a "less restrictive alternative") to protect their children without any burden on the rights of willing adults to access the sexual content. The Court reasoned that "even where speech is indecent and enters the home, the objective of shielding children does not suffice to support a blanket ban if the protection can be accomplished by a

35. *See* Reno v. ACLU (*CDA*), 521 U.S. 844, 877 (1997) (citation omitted).

36. *Id.* at 868-69 (citation omitted).

37. 47 U.S.C. § 231 (2006).

38. 529 U.S. 803 (2000).

less restrictive alternative."[39] The *Playboy* Court made clear that if there exists a targeted capability for parents and individual users to control access to content, government regulation to control the content more broadly cannot stand:

> Simply put, targeted blocking is less restrictive than banning, and the Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests. This is not to say that the absence of an effective blocking mechanism will in all cases suffice to support a law restricting the speech in question; but if a less restrictive means is available for the Government to achieve its goals, the Government must use it.[40]

Four years later, the Supreme Court returned to the topic of user control—this time squarely in the Internet context—and in a five-Justice majority decision, emphatically endorsed the promotion of filtering software as a constitutionally less restrictive alternative to government content regulation. In *Ashcroft v. ACLU* (*COPA*),[41] the Court reviewed and upheld a preliminary injunction against enforcement of COPA, which was Congress's mild revision to the CDA following the *Reno v. ACLU* decision (striking down the CDA).

In the *COPA* majority opinion, Justice Kennedy, joined by Justices Stevens, Thomas, Ginsburg, and Souter, specifically agreed that user-based filtering software was a less restrictive alternative to content regulation:

> The primary alternative considered by the District Court was blocking and filtering software. Blocking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them. . . .

39. *Id.* at 814.
40. *Id.* at 815.
41. 542 U.S. 656 (2004).

> Filters are less restrictive than COPA. They impose selective restrictions on speech at the receiving end, not universal restrictions at the source. Under a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information. Even adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers. Above all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished.[42]

The Court upheld the preliminary injunction but sent the case back to the district court to bring the evidentiary record on the effectiveness of filters up to date.

As we discuss in greater detail in the next section, the district court answered the Court's question of whether filtering tools have become more effective and available in the intervening years with a resounding "yes."[43] On remand, the lower court permanently enjoined COPA, holding that the law would not be effective at protecting children and that the government had failed to show that filtering technology is not a less restrictive alternative to advance the government's goal.[44] Importantly, the district court issued a broad affirmation of the user control approach after an extensive review of the diversity, availability, cost, ease of use, and effectiveness of filtering technologies.[45] The Third Circuit Court of Appeals affirmed the lower court's conclusions and, in January

---

42. *Id.* at 666-67.

43. ACLU v. Gonzales, 478 F. Supp. 2d 775, 793–94 (E.D. Pa. 2007).

44. *Id*. In fact, the district court concluded that although filters are not perfect, evidence shows they are "at least as effective, and in fact, are more effective than COPA in furthering Congress' stated goal for a variety of reasons." *Id.* at 815.

45. *Id.* at 789–95.

2009, the Supreme Court declined to hear the government's appeal—bringing to an end this ten-year stage of the battle over how best to protect children online.[46]

Taken together, these cases directly validate the user control approach advanced by Berman and Weitzner to protect children online without sacrificing First Amendment principles. From the Supreme Court down, these courts have affirmed the notion that if end users are empowered to choose what speech they wish to access or block online, then such a user-controlled approach is fundamentally less restrictive than universal restrictions imposed at the source. Since COPA was passed, four major online safety task forces and commissions in the United States have reached the same conclusion, deciding that education and voluntary technology tools are the most effective way to protect kids online.[47] In the next section, we will examine how effective and ubiquitous user control technologies have become.

III.USER CONTROL AS DEPLOYED IN THE MARKET

As the Supreme Court noted in COPA's second appearance before the Court, the Internet and other interactive media

---

46. ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, 129 S. Ct. 1032 (2009).

47. *See* INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES (Dec. 31, 2008), *available at* http://cyber.law.harvard.edu/pubrelease/isttf/; COPA COMMISSION, FINAL REPORT TO CONGRESS (Oct. 20, 2000), *available at* www.copacommission.org/report; POINTSMART.CLICKSAFE TASK FORCE, TASK FORCE RECOMMENDATIONS FOR BEST PRACTICES FOR CHILD ONLINE SAFETY (July 2009), *available at* http://www.pointsmartreport.org/; COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD OF THE NATIONAL RESEARCH COUNCIL, YOUTH, PORNOGRAPHY AND THE INTERNET (Dick Thornburgh & Herbert S. Lin eds., Nat'l Academies Press, 2002), *available at* http://www.nap.edu/html/youth_internet/. For a summary of the findings in all four reports, see Adam Thierer, The Progress & Freedom Found., *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation are the Answer*, PROGRESS ON POINT, July 2009, http://www.pff.org/issues-pubs/pops/2009/pop16.13-five-online-safety-task-forces-agree.pdf.

technologies develop and transform at unprecedented speeds.[48] The *CDA* and *COPA* cases illustrate the practical challenges of using static laws to attempt to control a rapidly changing environment.

In contrast, the market for user empowerment tools has flourished alongside new media developments as parents and caregivers seek sensible strategies to protect children in an increasingly networked world.[49] Reviewing COPA on the merits at the direction of the Supreme Court, the district court's extensive findings of fact documented many of these advancements. Both the district court and Third Circuit on appeal relied heavily on these findings in concluding that user empowerment tools are both more effective and far less restrictive than COPA in advancing Congress's interest.[50]

Filtering software and other tools have become increasingly sophisticated, allowing parents to tailor a variety of options to suit the values and needs of each particular household. The district court found that many filtering software tools are highly customizable by "enabling parents to choose which categories of speech they want to be blocked . . . and which age setting they want the product to apply."[51] Many tools also enable parents with multiple children to set up different accounts for each child, allowing parents to adjust settings according to age and maturity.[52] The filters themselves can be further fine-tuned to the household's

48. Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 671 (2004).

49. *See, e.g.*, ADAM THIERER, THE PROGRESS & FREEDOM FOUND., PARENTAL CONTROLS & ONLINE CHILD PROTECTION (Summer 2009), www.pff.org/parentalcontrols (surveying available online tools and methods of filtering online content).

50. *See Mukasey*, 534 F.3d at 198–204 (quoting the district court's findings of fact extensively).

51. ACLU v. Gonzales, 478 F. Supp. 2d 775, 791 (E.D. Pa. 2007). For example, parents can specifically block or allow access to content based on categories such as sexually explicit material, illicit drug information, information on violence and weapons, and hate speech. *Id. See also* GetNetWise, Tools for Families: Filtering and Blocking, http://kids.getnetwise.org/tools/filters (providing a searchable database of filters that allow blocking by category of speech).

52. *Gonzales*, 478 F. Supp. 2d at 791.

values by allowing parents to create customized "black" or "white" lists of websites the parents would like the filter to block or allow (respectively), notwithstanding the other categories that they have preset.[53]

In addition, many user empowerment tools aid parents in enforcing a variety of house rules that go beyond simply what content their children should be able to access. To help enforce computer usage rules, "[s]ome filters can also restrict Internet access based on time of day, day of week, how long the computer has been connected to the Internet, or which user is logged onto a computer."[54] Other tools can block use of Internet applications or protocols other than HTTP (either in whole or only for certain uses), including e-mail, instant messaging, chat, peer-to-peer file sharing, streaming video and audio, Internet television, and voice over Internet protocol (VoIP).[55]

For example, a parent can configure a filtering tool to block a child's use of chat rooms completely or simply filter out inappropriate words within a chat session. Many tools also allow parents to block transmission of certain sensitive information to strangers, including address and credit card information, over a variety of applications.[56] Finally, many tools now enable parents to monitor children's Internet activities, either remotely in real time, or by providing a report after the fact.[57]

The district court also assessed the availability and cost of filters. Because of robust competition in this market, the court found user control tools to be affordable and widely available.[58] Many Internet Service Providers (ISPs) and at least one major operating system offer filters and other parental control tools to customers for free.[59] In addition, the court found that filtering programs are "fairly easy to install, configure, and use and require

53. *Id.* at 790.
54. *Id.*
55. *Id.*
56. *See, e.g.*, GetNetWise, *supra* note 51.
57. *Gonzales*, 478 F. Supp. 2d at 792.
58. *Id.* at 793.
59. *Id.*

only minimal effort by the end user to configure and update."[60] Surveys suggest a very high level of user satisfaction with available software.[61]

Finally, as the Supreme Court requested on remand, the district court examined the effectiveness of filtering tools and found that available tools are remarkably effective for their purpose—and for Congress's goal of preventing minors from accessing sexually explicit material on the Internet—blocking around ninety-five percent of sexually explicit material on the Internet.[62] In assessing whether user filtering is at least as effective as COPA, both the district court and Third Circuit Court of Appeals contrasted this ninety-five percent blocking rate with evidence showing that COPA would not even address availability of substantial amounts of sexually explicit material on the Internet since around fifty-five percent (and growing) of such sites are hosted abroad.[63]

As Berman and Weitzner suggested, with such a diversity of effective and feasible user control mechanisms within practical reach of parents, the goal of protecting children from pornography and other potentially harmful material on the Internet and other interactive media can be achieved without heavy-handed government restrictions. The courts have unmistakably affirmed this notion: When faced with a choice between a one-size-fits-all speech restriction and a specific user-controlled technological solution available for parents to use, courts have made clear that a blanket speech restriction cannot survive strict scrutiny absent a showing that the technological solution is not as effective.

60. *Id.*

61. *Id.* at 794.

62. *Id.* at 795; ACLU v. Mukasey, 534 F.3d 181, 201 (3d Cir. 2008). The *COPA* district court found that these tools had improved quickly due to a robust competitive market and technological advances. *Gonzales*, 478 F. Supp. 2d at 794–97.

63. *Gonzales*, 478 F. Supp. 2d at 789, 815; *Mukasey*, 534 F.3d at 202–03.

IV.CRITIQUES OF THE USER CONTROL THEORY

The user empowerment jurisprudence is not without its critics—most significantly Justice Breyer and a minority of the Supreme Court. These critics have raised a number of challenges to the idea that filtering and user empowerment software should be considered a less restrictive alternative to governmental regulation. The critiques do not, however, undercut the strength of user empowerment tools, either as important components of any effort to protect minors online, or as constitutional alternatives to more burdensome government action.

A. User Empowerment Tools are Not Perfectly Effective

A key criticism is that filtering software is not perfect. As Justice Breyer notes—accurately—"filtering is faulty, allowing some pornographic material to pass through without hindrance."[64] The *COPA* district court found that filtering software blocks access to as much as ninety-five percent of sexual content online—but that means that five percent or more of such content is *not* blocked.[65]

The applicable standard, however, is not perfection, or even near-perfection. To be a constitutionally less-restrictive alternative, something must simply be *as or more* effective than the government action that is being challenged. As the Supreme Court explained in *ACLU v. Reno*, a restriction on speech is "unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[66] In *COPA*, the district court concluded that filtering tools clearly met this standard because the statute would be ineffective in thwarting overseas websites (and thus would be much less effective than filters).[67]

---

64. Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 685 (2004) (Breyer, J., dissenting).

65. *See Gonzales*, 478 F. Supp. 2d at 795.

66. Reno v. ACLU (*CDA*), 521 U.S. 844, 874 (1997).

67. *See Gonzales*, 478 F. Supp. 2d at 789, 815; *see also COPA*, 542 U.S. at 667 ("COPA does not prevent minors from having access to . . . foreign

B. Not All Parents Use Filtering and Control Tools

In defending COPA, the government argued repeatedly that filtering and control tools are not effective because not all parents use them. Justice Breyer agreed, noting that "filtering software depends upon parents willing to decide where their children will surf the Web and [being] able to enforce that decision. As to millions of American families, that is not a reasonable possibility."[68] He also noted that not all families can afford filtering software, even if they wanted to use such tools.[69] According to this argument, user control tools would be ineffective at protecting, for example, minors left at home without supervision or those who have unfiltered Internet access on computers outside the home.[70]

Determining how to raise children is a quintessentially parental responsibility, including how and when to restrict access to sexually explicit material. Many parents recognize that it is impractical and unrealistic to try to monitor all media consumption of their children (especially older minors) at all times. This practical reality is perhaps one reason why the most recent studies of online child safety place an increasing emphasis on the role of digital media literacy and education as a vital component of any strategy to protect minors online.[71]

Importantly, recent surveys demonstrate that parental guidance and other non-technological approaches also play a critical role in protecting minors online.[72] Most parents take an

---

harmful materials. That alone makes it possible that filtering software might be more effective in serving Congress' goals.").

68. *COPA*, 542 U.S. at 685.

69. *Id.*

70. *Id.* at 685–86.

71. *See* INTERNET SAFETY TECHNICAL TASK FORCE, *supra* note 47; POINTSMART.CLICKSAFE TASK FORCE, *supra* note 47.

72. *See, e.g.*, THIERER, *supra* note 49, at 25–44 (describing the many non-technological methods parents use to protect children from harmful material); AMANDA LENHART & MARY MADDEN, TEENS, PRIVACY AND ONLINE SOCIAL NETWORKS v-vi (Apr. 18, 2007), http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx (summarizing the non-technical means by which parents monitor children's use of the internet and other media).

active role in guiding their children's Internet experience through a variety of methods that may not involve technological tools, including setting house rules for Internet and mobile device usage, monitoring such usage, placing computers in common rooms, and educating their children to make informed media choices.[73] In fact, a recent Pew Internet & American Life Project study found that at least eighty-five percent of American parents use technological user control tools, non-technological approaches, or some combination of the two.[74]

In affirming the user control approach, courts have explicitly acknowledged the variety of parental preferences and approaches to protecting minors online. In enjoining COPA, the Third Circuit Court of Appeals cited studies showing that "the primary reason that parents do not use filters is that they think they are unnecessary because they trust their children and do not see a need to block content."[75] The Supreme Court has recognized in two separate cases that if some parents do not block adult content, it does not necessarily follow that they do not know how to do so or, alternatively, that promoting the use of blocking technology would not be an effective alternative to a blanket speech restriction.[76] Indeed, in endorsing the user control approach, these courts have affirmed that families—not the government—should choose for themselves what content should be accessed in the home, consistent with fundamental First Amendment values.

---

73. *See* THIERER, *supra* note 49, at 25–44.

74. LENHART & MADDEN, *supra* note 72.

75. ACLU v. Mukasey, 534 F.3d 181, 203 (3d Cir. 2008).

76. United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 824 (2000) ("A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act."); Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 670 (2004) ("COPA presumes that parents lack the ability, not the will, to monitor what their children see. By enacting programs to promote use of filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties.").

C. Parental Use of Empowerment Tools Is Not a Governmental Action

Another key criticism argues that mere use of filtering and control tools is not really a governmental act, and thus cannot be considered an alternative legislative approach under strict scrutiny analysis, much less a "less restrictive alternative." In his dissenting opinion in *COPA*, Justice Breyer characterized the problem Congress sought to address as protecting children exposed to harmful material, *despite* the availability of filtering software.[77] For Justice Breyer, the presence of user control tools was merely part of the backdrop against which Congress enacted COPA. Congress may not require that parents use filters, the argument goes, and so parental use of such tools is not a governmental act—and "'doing nothing' does not address the problem Congress sought to address."[78]

But, as the Supreme Court stated clearly in *Playboy*, the existence of "targeted blocking enables the Government to support parental authority without affecting the First Amendment interests of speakers and willing listeners."[79] The courts and online safety task forces have identified many concrete ways in which governments may act to protect minors online.[80]

Congress can, for example, promote parental use and awareness of such tools. As the *COPA* district court concluded, "the government may promote and support their use by, for example, providing further education and training programs to parents and caregivers."[81] One recent blue ribbon task force recommended expanding online safety education programs to empower parents and teachers to prepare minors to navigate the

77. *COPA*, 542 U.S. at 685 (Breyer, J., dissenting).

78. *Id.*

79. *Playboy*, 529 U.S. at 815.

80. *See COPA*, 542 U.S. at 669–70 ("Congress undoubtedly may act to encourage use of filters . . . . By enacting programs to promote use of filtering software, Congress could give parents [the ability to monitor use] without subjecting protected speech to severe penalties.") (internal citations omitted).

81. ACLU v. Gonzales, 478 F. Supp. 2d 775, 814 (2007).

Internet and other new media.[82] The same task force recommended increased government funding for professional development for teachers, curriculum development and implementation for students, public awareness campaigns, and research to identify and promote best practices for digital literacy and online safety.[83]

To address cost concerns, Congress could act by "giving incentives or mandates to [ISPs] to provide filters to their subscribers, directing the developers of computer operating systems to provide filters and parental controls as a part of their products, [and by] subsidizing the purchase of filters for those who cannot afford them."[84] Congress could also subsidize the use of filters on computers accessible to minors in schools and libraries.[85] Finally, Congress could take steps to promote the development and ease of use of tools by performing further studies and developing recommendations and best practices to improve these tools.

As courts have recognized, all of these options are governmental acts that represent less restrictive alternatives to a one-size-fits-all restriction on online speech. That filtering technology is something that parents must implement—if they decide they want to filter—does not diminish the fact that the promotion of user empowerment can be a less restrictive alternative to government regulation.

82. POINTSMART.CLICKSAFE TASK FORCE, *supra* note 47, at 7.

83. *Id.* at 7–8.

84. *Gonzales*, 478 F. Supp. 2d at 814.

85. Congress passed the Children's Internet Protection Act (CIPA) in 2000, which strongly incentivizes use of Internet filters in libraries and schools by conditioning certain federal funding on their use. Pub. L. No. 106-554, § 1(a)(4), 114 Stat. 2763 (codified at 20 U.S.C. §§ 6801, 6777, 9134 (2003); 47 U.S.C. § 254 (2003)). While CIPA was ultimately upheld by the Supreme Court in *United States v. Am. Library Ass'n, Inc.*, 539 U.S. 194, 199 (2003), this approach raises a number of First Amendment concerns: filters can be a useful—though imperfect—tool when used voluntarily by parents; government-mandated filters, however, would result in the blocking of lawful websites and otherwise constitutionally protected speech, for both adults and minors.

D. Filtering Represents the Status Quo on Which Congress Can Legislate

Ultimately, Justice Breyer's most fundamental objection in the *COPA* case to user empowerment being a less restrictive alternative is his assertion that filtering software is "part of the status quo . . . against which Congress enacted [COPA]."[86] Justice Breyer essentially asserts that Congress might have passed COPA based on a theory that filtering tools were not good enough. There are a number of flaws with Justice Breyer's analysis, including the lack of significant evidence that Congress was focused on the effectiveness of filtering software when it passed COPA in 1998.

More critically, Justice Breyer's COPA analysis is inconsistent with how the "less restrictive alternative" analysis has been implemented under the Supreme Court's First Amendment jurisprudence. In one seminal case, *Sable Communications of California, Inc. v. FCC*,[87] the Court overturned a law prohibiting "dial-a-porn" by holding some prior FCC regulations were a less restrictive alternative to the newly passed law.[88] Indeed, the new law repealed statutory provisions on which the prior regulations were based.[89] In other words, the "less restrictive alternative" found by the *Sable* Court was *precisely* the "status quo" that existed prior to the passage by Congress of the law held to be unconstitutional.

The facts in *United States v. Playboy Entertainment Group, Inc.*,[90] further illustrate the difficulty raised by Justice Breyer's "status quo" analysis. In that case, one section of an act (§ 505) was held to be unconstitutional because another section of the same act (§ 504) was found to be a "less restrictive alternative."[91] But hypothetically, had § 504 been passed a brief time *before* § 505,

---

86. Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 684 (2004) (Breyer, J., dissenting).

87. 492 U.S. 115, 117 (1989).

88. *Id.* at 128-29.

89. *Id.* at 122-23.

90. 529 U.S. 803 (2000).

91. *Id.* at 823.

Justice Breyer would presumably argue that § 504 was the "status quo" on which Congress passed § 505 (and thus § 504 could not be a less restrictive alternative). Yet that would upend the constitutional analysis based solely on the timing of the Congressional enactment—thus upholding (using Justice Breyer's analysis) a speech-burdening provision when a less burdensome *and* more effective alternative was readily available.

Moreover, Justice Breyer's overriding focus in 2004 on what the "status quo" was when Congress enacted COPA in 1998 would seem to preclude *any* later development of a less restrictive alternative. *Whatever* the state of filtering software was when Congress enacted COPA in 1998, if by 2004 filtering was both constitutionally less restrictive and more effective than COPA, the statute should not have stood. And the *COPA* majority appears to have reached this same conclusion, remanding the case for further factfinding by the trial court. As the Supreme Court noted:

> [T]he factual record does not reflect current technological reality—a serious flaw in any case involving the Internet. The technology of the Internet evolves at a rapid pace. Yet the factfindings of the District Court were entered in February 1999, over five years ago. Since then, certain facts about the Internet are known to have changed. *It is reasonable to assume that other technological developments important to the First Amendment analysis have also occurred during that time.* More and better filtering alternatives may exist than when the District Court entered its findings.[92]

Contrary to Justice Breyer's focus on the "status quo" in 1998, the majority appropriately placed the focus of the First Amendment analysis on the present day. As the *COPA* district court found on remand, user empowerment technology has proven to be a far more effective—and less constitutionally burdensome—

92. Ashcroft v. ACLU (*COPA*), 542 U.S. 656, 671 (2004) (internal citations omitted) (emphasis added).

alternative to heavy-handed governmental regulation.[93] After thirteen years of litigation—starting in 1996 with the *Reno v. ACLU* challenge to the CDA, up to the Supreme Court's 2009 denial of a third appeal of the COPA challenge—the courts have well established that user controls are the constitutionally best approach to address concerns about minors' access to online content.

V.USER CONTROLS IN THE WEB 2.0 AGE

The Internet has not, however, stood still during the thirteen years of CDA and COPA litigation. On the contrary, we have seen a dramatic explosion of innovation in "user-generated" content on sites such as YouTube and Wikipedia and interactive communications on blogs and social networks such as Facebook. These "Web 2.0" sites have transformed how users relate to online content and to each other over the Internet and have become a (if not *the*) dominant way that young people connect with each other.

Much of the success of Web 2.0 platforms is due to a provision of the U.S. Code that was enacted at the same time as the Communications Decency Act in 1996. With what is known simply as "Section 230," Congress acted to foster innovation and growth in the online environment.[94] To this end, § 230 provides immunity to

---

93. Another way to analyze the First Amendment issue today is that the wide availability of free or low-cost user empowerment tools, and the high level of effectiveness of such tools, *see supra* Section III, call the governmental interest into question. These tools, plus the fact that many parents do not consider it to be necessary to block sexually explicit material because they prefer to educate their children about media consumption (and trust in that education), *see supra* Section IV.B and notes 68-74, may suggest that the governmental interest in protecting minors from sexually explicit material online may not be as compelling as assumed. Although protecting children (from any number of risks, on- and off-line) is of course a compelling *societal* interest, protecting them from online content may no longer be a significant *governmental* interest.

94. 47 U.S.C. § 230 (2006). Technically, § 230 was enacted as a part of the CDA. Although the Supreme Court struck down the CDA's indecency provisions in *Reno v. ACLU* in 1997, the remainder of that Act (including § 230) was not challenged and remains good law today. By enacting § 230, Congress sought to advance three important legislative goals: 1) to promote

ISPs or intermediaries from most civil suits (and some criminal charges) based on the content created by their users (and others).[95] These protections from liability have enabled social networking and other interactive sites that rely on user-generated content to flourish. Consequently, these sites are the vibrant platforms for freewheeling expression at the heart of Web 2.0.

But § 230 had another specific goal, that of promoting user control technology. As Congress declared: "It is the policy of the United States . . . to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer service[s] . . . ."[96]

Among other provisions, § 230 insulates ISPs, websites, and technology creators from liability for making or offering user control technology to help users and parents control their Internet experiences.[97]

Using the term to mean more than just "parental control," the Web 2.0 environment represents a new high point for "user control": Users are now able to shape many different aspects of their online experience, customizing websites and services to meet their exact interests. Facebook, Pandora, and myriad other interactive services enable highly granular degrees of control over what content a user will see or hear. And because many Web 2.0

---

the continued rapid and innovative development of the Internet (and other interactive media); 2) to remove disincentives to voluntary self-screening of content by service providers; and 3) to promote the development of user control technologies. For an analysis of the legislative history and intent behind § 230, see Brief for Anti-Spyware Coalition, et al. as Amici Curiae Supporting Appellee, Zango, Inc. v. Kaspersky Lab, Inc., 569 F.3d 1169 (9th Cir. 2009) (No. 07-35800) at 4–15, *available at* http://www.cdt.org/privacy/spyware/20080505amicus.pdf.

95. *See* 47 U.S.C. § 230(c)(1). If ISPs, web hosts, and websites were instead made potentially liable for content posted by others, they would be forced to assume content gatekeeper roles and would be more reluctant to host controversial (though lawful) speech. Without § 230, entry barriers for new Internet services and applications would be much higher, dampening the innovation we have witnessed heretofore in interactive media.

96. *Id.* § 230(b)(3).

97. *Id.* § 230(c)(2)(A)-(B).

applications rely on user-generated content—and, therefore, active, engaged users—such applications are all the more responsive to user input and demands for user empowerment tools than their Web 1.0 predecessors. As one example of these new levels of user control, the experience of listening to music today is quite different from the way it was thirty years ago, when *FCC v. Pacifica Foundation*[98] was decided. Today, instead of being subjected to whatever songs or other content a radio station chooses to broadcast, you can now use sites such as Pandora.com to assemble a stream of music precisely to your tastes. To go a step further, you can take your own library of music with you using MP3 players.

In turn, the innovation in interactive media has spurred innovation in more traditional parental and user control tools. User controls remain key for helping parents protect children in the Web 2.0 world. Filters can block in their entirety social networking sites such as MySpace or Facebook that may not be appropriate for children under thirteen. To aid parents of older minors, the market is responding with tools that allow parents to monitor a range of online activities, including children's use of social networks, and to facilitate discussion and guidance around a range of online safety concerns that go beyond mere accessibility of sexually explicit content.[99] Some of the leading social networks are themselves providing parental control tools and taking other steps to promote online child safety.[100]

---

98. 438 U.S. 726 (1978).

99. *See, e.g.*, OnlineFamily.Norton, https://onlinefamily.norton.com/familysafety/loginStart.fs (marketing a set of tools for parents to use to monitor and control their children's Internet usage). These tools aim to help parents not only monitor online activity, but also to foster dialogue between parents and children about a range of online safety concerns. *See also* Press Release, Symantec, Symantec Launches New, Unique OnlineFamily.Norton Service for Free Through 2009 (Apr. 27, 2009), http://www.symantec.com/about/news/release/article.jsp?prid=20090427_01 (addressing "online predators and cyberbullies").

100. *See* INTERNET SAFETY TECHNICAL TASK FORCE, THE BERKMAN CENTER FOR INTERNET AND SOCIETY, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES 24-26, *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (Dec. 31, 2008) (summarizing child safety actions and services of social networks).

In addition, as content migrates beyond personal computers onto a variety of mobile and wireless devices, the industry has worked to keep pace by meeting the demand for parental controls of such devices.[101] Parents now have multiple options to help control content their children can access on cell phones and other wireless devices.[102] The range and diversity of user control tools makes plain the power of the market to respond quickly to rapidly changing platforms.

On top of the increasing number and diversity of content and service offerings on the Internet is the increasing globalization of online content. The number of non-U.S. Internet users has grown rapidly over the past decade,[103] and these users have fully embraced the interactive nature of Web 2.0.[104] In response, blogging platforms, social networking websites, and other user-generated content sites increasingly offer localized versions of their services to cater to users from all over the world.[105] These and other factors have resulted in a significant increase of web content hosted and originating outside of the United States, and a shift away from English as the dominant online language.[106]

---

101. *See* THIERER, *supra* note 49, at 103–12 (providing an updated survey of parental control tools that have developed for mobile devices).

102. *Id.*

103. *See* Internet World Stats, Internet Usage Statistics: World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm (last visited Oct. 12, 2009).

104. *See Social Networking's New Global Footprint*, NIELSON WIRE, Mar. 9, 2009, http://blog.nielson.com/nielsonwire/global/social-networking-new-global-footprint.

105. For example, YouTube, Facebook, Blogger, and Wikipedia all offer localized or local language versions of their platforms. *See, e.g.*, Blogger Language Selection, https://www.blogger.com/language.g (last visited Oct. 12, 2009) (allowing customized language settings for Blogger); Facebook, http://www.facebook.com (last visited Oct. 12, 2009) (displaying a list of available language versions on the bottom of the homepage); YouTube India, http://www.youtube.com/index?gl=IN (last visited Oct. 12, 2009) (offering localized content); Wolna Encyklopeida, http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna (last visited Oct. 12, 2009) (Wikipedia Poland).

106. *See generally* Daniel Sorid, "Writing the Web's Future in Numerous Languages," N.Y. TIMES, Dec. 30, 2008, at B1 (highlighting the creation of

Collectively, this global body of users is creating vast amounts of diverse content, with over twenty hours of video uploaded every minute by a worldwide user base to YouTube alone.[107]

The volume and diversity of content—and the great global diversity of societal perspectives about what content is appropriate, and what content can be regulated—suggest that it is highly unlikely that there will ever be global consensus on content regulation, or that a one-size-fits-all speech restriction could ever address the diversity of speech represented in such a fast-paced global environment. These trends only strengthen Berman and Weitzner's argument that voluntary, client-side user empowerment tools—which can be tailored to each country, culture, and even household—are the most effective way to protect users and minors from unwanted content without chilling speech.

VI.CONCLUSION

As the Supreme Court has observed, "[t]echnology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us."[108] As technology progresses, user empowerment tools have become increasingly ubiquitous across a broad range of platforms. Without a doubt, it is becoming clear that a robust market for user empowerment tools can adjust to rapid changes in technology far more effectively than legislation passed by Congress.

Indeed, user control tools are also seeping *back* up the technological spectrum. There is now a diversity of tools available to help parents control what their children can view over broadcast television, and these tools are undercutting the validity of the case that Jerry Berman and Daniel Weitzner were originally seeking to

---

applications and services that allow users to create and read content in South Asian languages).

107. Posting of Ryan Junee to Broadcasting Ourselves ;): The Official YouTube Blog, http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html (May 20, 2009).

108. U.S. v. Playboy Entm't Group, Inc., 529 U.S. 803, 818 (2000).

ward off—*FCC v. Pacifica Foundation.*[109] As the Second Circuit observed about *Pacifica* in a broadcast indecency case, "technological advances may obviate the constitutional legitimacy of the FCC's robust oversight" under *Pacifica.*[110] And certainly as media (including content from broadcast networks) converge into the Internet realm, the strong user control tools available online will provide effective "less restrictive alternatives" to government censorship.

Berman and Weitzner concluded their 1995 analysis with a "hope that Congress and the courts will recognize the unique nature of interactive media and choose to regulate them accordingly," and with an exhortation for industry "to move forward with the task of building open networks that maximize abundance, diversity, and user control."[111] Looking back, we can see that both the courts and industry have moved in the right direction: by placing empowerment tools in users' hands so they can shape their online experience, we collectively have built a solid foundation for an open and uncensored Internet.

109. 438 U.S. 726 (1978).

110. Fox Television Stations, Inc. v. FCC, 489 F.3d 444, 466 (2d Cir. 2007).

111. Berman & Weitzner, *supra* note 1, at 1637.