2008

Protecting Minors from Online Pornography without Violating the First Amendment: Mandating an Affirmative Choice

Robert A. Gomez

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation
Available at: https://scholar.smu.edu/scitech/vol11/iss1/2

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu
Protecting Minors From Online Pornography Without Violating the First Amendment: Mandating an Affirmative Choice

Robert A. Gomez*

Abstract: In view of Congress’ failed efforts to prevent children from viewing pornography and other indecent and harmful materials on the Internet, this article proposes that Congress pass a law which requires all new personal computers to come equipped with blocking and filtering software that requires the activating user to make an affirmative choice, during the computer’s initial setup, regarding the computer’s filter settings for each account on the computer.

I. INTRODUCTION

In the last fifty years, few technological inventions have surpassed the impact or potential of the Internet. The possibility for human interaction is unparalleled. With the click of a mouse, people can post anything online and within minutes it becomes available to millions around the world. Unfortunately, the Internet has a dark side. Lurking behind all of its positive qualities is a seemingly endless collection of pornography. For most adults, this is a relatively minor annoyance. However, it poses a grave threat for America’s youth.

Online pornography is a multi-billion dollar industry that consists of over 4.2 million websites and roughly 372 million pages.1 According to a recent study, the largest consumers of online pornography are children between the ages of twelve and seventeen.2 The same study found that “eighty percent of fifteen to seventeen-year-olds have had multiple exposures to hard-core pornography, and ninety percent of eight to sixteen-year-olds have viewed pornography online, most often while doing their homework.”3 Perhaps most disturbing is that certain providers specifically target children by creating websites with Internet addresses similar to the names of popular children’s figures, shows, and movies.4 For example, thousands of porno-

* Robert A. Gomez is an associate at Gibson, Dunn & Crutcher LLP, specializing in litigation. Mr. Gomez received an undergraduate degree from the University of California Los Angeles and a juris doctorate from Yale Law School. Mr. Gomez wishes to thank Yale Law Professor Ian Ayres for his insightful comments and invaluable guidance, and his supportive family.


2. Id.

3. Id.

4. Id.
graphic links are named after or attached to popular children's characters such as Pokemon and Action Man. In essence, trickery is used to cause inadvertent exposure. Exposure also occurs through more traditional routes. For example, one study found that twenty-eight percent of exposures occur when opening Email or clicking on links contained in Emails or Instant Messages.

Despite estimates that eleven million minors view pornographic websites each week, pinning down the exact psychological effects has proven to be a challenging task. Due to ethical and moral concerns associated with purposely exposing children to pornography, no study has directly monitored pornography's impact on minors. Nevertheless, there is general consensus that pornography has a detrimental effect on impressionable youths. Certain studies suggest that pornographic stimulation "has a negative impact similar to that of being exposed to extreme violence at such tender years." Other studies allege that youths prone to aggressive behavior may be triggered to act on their inhibitions as a result of exposure to online pornography. Lastly, youths exposed to online pornography may use the material as a social cue for what is appropriate and acceptable sexual behavior. Although adult entertainment is only supposed to be fantasy, there is a strong possibil-

10. Sosnay, supra note 9, at 454; see Richard B. Felson, Mass Media Effects on Violent Behavior, 22 ANNUAL REVIEW OF SOCIOLOGY 103, 103-28 (1996) (reviewing studies that demonstrate that viewing pornography increases the likelihood that one will become violent more easily if provoked).
11. Sosnay, supra note 9, at 454.
12. See Steven D. Burt, Strict Scrutiny in Cyberspace: The Invalidation of the Communications Decency Act and the Slow Demise of the Child Online Protec-
mandating an affirmative choice

ity that exposure could "negatively affect boys' relationships with girls and, later on, women," and that "many young women . . . accept their own sexual activities and responses (and those of their male partners) should mirror those seen in sexual-fantasy media."  

To its credit, Congress recognized these threats at an early stage in the Internet's development and responded by enacting bills such as the Communications Decency Act ("CDA"), the Child Online Protection Act ("COPA"), and the Children's Internet Protection Act ("CIPA"). Through these Acts, Congress has forcefully attempted to limit and prevent the opportunities for minors to be exposed to online pornography. However, because both the CDA and COPA restricted speech on the basis of its content, courts struck them down for violating the First Amendment. As a result, CIPA is the sole law currently being enforced.  

In the aftermath of the CDA and COPA, this article argues that Congress should pass a law requiring all new computers to come with blocking and filtering software. This software should require the buyer (i.e., parents) to make an affirmative choice, during the initial setup, regarding the computer's filter settings for each account on the computer. Part I discusses the First Amendment issues involved with attempting to restrict minors access to pornography on the Internet. Part II examines the statutory provisions and legal history of the CDA, COPA, and CIPA. Finally, Part III lays out a detailed argument for the implementation of a law that requires buyers to make a mandatory decision regarding the configuration of the computer's filter settings.

II. THE FIRST AMENDMENT

One of the core requirements of the Constitution is that "Congress shall make no law . . . abridging the freedom of speech." As a matter of principle, every branch of the Government has attempted to remain faithful to this guarantee. However, in practice, absolute freedom of speech is neither feasible nor desirable. In the famous words of Justice Holmes, "[t]he most stringent protection of free speech would not protect a man in falsely shouting


14. See infra Part II.A-B.

15. See infra Part II.C.


17. Roth v. United States, 354 U.S. 476, 483 (1957) (stating "the unconditional phrasing of the First Amendment was not intended to protect every utterance.").
fire in a theatre and causing a panic.”\(^{18}\) In essence, words that “create a clear and present danger” are not entitled to First Amendment protection.\(^{19}\) And just to provide another example, libel is another form of speech that is not within the zone of constitutionally protected speech.\(^{20}\)

The forms of regulation pertinent to this article are obscenity and indecency. In \textit{Roth v. United States}, the Supreme Court distinguished obscenity from sex.\(^{21}\) According to Justice Brennan, sex is “a great mysterious force in human life . . . [that] has indisputably been a subject of absorbing interest to mankind through the ages[.]”\(^{22}\) Accordingly, the portrayal of sex “in art, literature and scientific works is not itself sufficient reason to deny material the constitutional protection of freedom of speech and press.”\(^{23}\) Obscene material, on the other hand, “deals with sex in a manner appealing to prurient interest.”\(^{24}\)

Several years after \textit{Roth}, in \textit{Miller v. California}, the Court provided a test for courts to apply when determining whether material is obscene and, consequently, not protected by the First Amendment:

(a) whether “the average person, applying contemporary community standards” would find that the work, taken as a whole, appeals to the prurient interests; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.\(^{25}\)

Much like other communications, if material posted on the Internet does not violate this standard, it is entitled to “the same First Amendment protection as traditional speech.”\(^{26}\) However, courts have also recognized that different rules apply to material that can be accessed by minors.

In \textit{Ginsberg v. New York}, the Supreme Court upheld the constitutionality of a New York statute that prohibited “the sale to minors under 17 years

\begin{itemize}
  \item[18.] Schenck v. United States, 249 U.S. 47, 52 (1919).
  \item[19.] Id.
  \item[20.] Beauharnais v. Illinois, 343 U.S. 250, 266 (1952).
  \item[21.] See Roth, 354 U.S. at 487.
  \item[22.] Id.
  \item[23.] Id.
  \item[24.] Id.
  \item[25.] Miller v. California, 413 U.S. 15, 24 (1973) (citation omitted).
  \item[26.] Todd A. Nist, \textit{Finding the Right Approach: A Constitutional Alternative for Shielding Kids from Harmful Materials Online}, 65 Ohio St. L.J. 451, 454 (2004); The Supreme Court recently noted, “our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to the Internet.” Reno v. ACLU, 521 U.S. 844, 870 (1997).
\end{itemize}
of age of material defined to be obscene on the basis of its appeal to them whether or not it would be obscene to adults." 27 Although the Court's opinion did not anticipate the creation of the Internet, Justice Brennan noted, "the State has an interest 'to protect the welfare of children' and to see that they are 'safeguarded from abuses' which might prevent their 'growth into free and independent well-developed men and citizens.'" 28 Ginsberg ultimately stands for the proposition that legislatures may attempt to prevent minors from being exposed to obscene and indecent sexual depictions.

However, since Ginsberg, legislatures have struggled to avoid using content-based restrictions. 29 In TBS, Inc. v. FCC, the Court defined content-based restrictions as "laws that by their terms distinguish favored speech from disfavored speech on the basis of the ideas or views expressed are content-based." 30 According to the Court, "[t]he principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of disagreement with the message it conveys." 31 More importantly, "[c]ontent-based regulations are presumptively invalid" 32 and are therefore subjected to strict scrutiny. 33 Under strict scrutiny, "[i]f 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." 34 On the other hand, statutes which contain content-neutral restrictions are only subject to intermediate scrutiny. 35

As the following section demonstrates, Congress has generally been incapable of persuading courts to uphold content-based restrictions.

III. PREVIOUS CONGRESSIONAL EFFORTS

A. Communications Decency Act

In 1996, Congress passed the Communications Decency Act ("CDA") as a part of the Telecommunications Act of 1996. The CDA attempted to protect children from online pornography in two ways. 36 First, it prohibited

28. Id. at 641 (citing Prince v. Massachusetts, 321 U.S. 158, 165 (1944)).
30. Id. at 643.
35. Phillips, 107 F.3d at 172.
36. Novak, supra note 7, at 328.
individuals from knowingly transmitting obscene or indecent material to any person under eighteen years of age. The statute provided that:

Whoever in interstate or foreign communications, by means of a telecommunications device knowingly (i) makes, creates, or solicits, and (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication, shall be fined under Title 18, or imprisoned not more than two years, or both.

Second, section 223(d) stated that:

Whoever (1) in interstate or foreign communications knowingly (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, is obscene or child pornography, regardless of whether the user of such service placed the call or initiated the communication...shall be fined under Title 18, or imprisoned not more than two years, or both.

The statute provided persons prosecuted for violating its terms with two affirmative defenses. The first defense protected individuals who took "reasonable, effective, and appropriate" measures to limit access by minors. The second defense protected individuals that restricted access by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

The CDA's only real success was its passage. Immediately after President Clinton signed it into law, several groups filed lawsuits challenging the constitutionality of the "indecent transmission" provision and the "patently offensive display" provision. The Eastern District of Pennsylvania "preliminary enjoined" the Government "from enforcing, prosecuting, investigating
or reviewing” the challenged provisions. The Government appealed the
district court’s holding to the Supreme Court.

The Supreme Court affirmed the district court’s holding in *Reno v. ACLU*. In the course of doing so, the Court made several important find-
ings. First, the Court found that the CDA is a “content-based regulation of speech.” Second, and more importantly, the Court held that the challenged
provisions were facially overbroad in violation of the First Amendment. According to the Court, in attempting to deny minors access to potentially
harmful speech, the challenged provisions effectively suppressed speech that
adults have a constitutional right to receive and to address to one another. Moreover, proponents of the CDA failed to demonstrate that less restrictive
alternatives would not be equally as effective.

The Court also found the CDA constitutionality deficient for a host of other reasons. For example, the Court found that the statute’s scope was
ambiguous because “each of the two parts of the CDA use[ ] a different lin-
guistic form. The first uses the word ‘indecent,’ while the second speaks of
material that ‘in context, depicts or describes, in terms patently offensive as
measured by contemporary community standards, sexual or excretory activi-
ties of organs[,]’” The Court was particularly concerned with the statute’s
vagueness because of the potential “chilling effect on free speech.” Furthermore, because the CDA is a criminal statute, “[t]he severity of criminal
sanctions may . . . cause speakers to remain silent rather than communicate
even arguably unlawful words, ideas, and images.” Lastly, the Court found
the affirmative defenses insufficient to save the constitutionality of the Act.

B. Child Online Protection Act

In direct response to the CDA being struck down, Congress passed the
Child Online Protection Act (“COPA”) as a part of the Omnibus Consoli-

45. *Id.* at 871.
46. *Id.* at 864.
47. *Id.* at 874.
48. *Id.* at 879.
49. *Id.* at 870-71 (citations omitted).
50. *Id.* at 871-72.
51. *Id.* at 872.
52. *Id.* at 882 (stating “[w]e agree with the District Court’s conclusion that the
CDA places an unacceptably heavy burden on protected speech, and that the
defenses do not constitute the sort of ‘narrow tailoring’ that will save an other-
wise patently invalid unconstitutional provision”).
dated and Emergency Supplemental Appropriations Act of 1999. \(^{53}\) COPA was drafted with the specific intention of remedying the CDA’s defects. \(^{54}\) The Act made it illegal for a person to knowingly make, through the Internet, any communication for commercial purposes that is harmful to minors, unless the person makes a good faith effort to restrict access by minors to the communication. \(^{55}\) Moreover, under the terms of the statute, violators are susceptible to criminal and civil penalties. \(^{56}\)

One of the distinguishing features of COPA was its specificity. The statute defined “material prohibited to minors” as:

\[
\text{(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pande...}
\]

COPA also included safe harbors similar to those in the CDA. \(^{58}\)


\(^{54}\) Novak, supra note 7, at 332. According to Emily Novak, “[t]he Committee Report articulates that the bill strikes the appropriate balance between preserving the First Amendment rights of adults and protecting children from harmful material on the World Wide Web in response to the Supreme Court’s decision in Reno v. ACLU.” Id. at 332 n.36. See also H.R. Rep. No. 105-775, at 5 (1998).

\(^{55}\) Novak, supra note 7, at 332; see also H.R. Rep. No. 105-775, at 5. One of the most problematic aspects of COPA was that it only applied to pornography which is commercially distributed. Child Online Protection Act, 47 U.S.C. § 231 (2000). As a result, it made no effort to limit children from viewing pornography which is not commercially distributed. H.R. Rep. No. 105-775, at 5.

\(^{56}\) See H.R Rep. No. 105-775, at 5; see Novak, supra note 7, at 332-33.


\(^{58}\) Specifically the Act provides:
COPA, like the CDA, was challenged immediately after President Clinton signed it into law. The Eastern District of Pennsylvania granted a preliminary injunction largely on the grounds that COPA was not the least restrictive means available to prevent minors from accessing harmful material on the Internet.59

The Government appealed the preliminary injunction to the Third Circuit. The Third Circuit affirmed the district court’s holding, but on different grounds. It held that the “contemporary community standards” provision was unconstitutionally overbroad.60 The court also found that removing this provision would not salvage COPA because the standard was an essential component of the statute.61

The Supreme Court granted certiorari to consider one issue: whether the Act’s use of “contemporary community standards” to identify material harmful to minors runs afoul of the First Amendment.62 The Court held that “COPA’s reliance on community standards to identify ‘material that is harmful to minors’ does not by itself render the statute substantially overbroad for purposes of the First Amendment.”63 The Court rejected the Third Circuit’s finding that the “contemporary community standards” provision would require “all speakers on the Web to abide by the ‘most puritan’ community’s standards.”64 According to Justice Clarence Thomas, unlike the CDA, COPA “applies to significantly less material . . . and defines the harmful-to-minors material restricted by the statute in a manner parallel to the Miller definition of obscenity.”65

It is an affirmative defense to prosecution under this section that the defendant, in good faith has restricted access by minors to material that is harmful to minors –

(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;

(B) by accepting a digital certificate that verifies age; or

(C) by any other reasonable measures that are feasible under available technology.

Id. at § 231(c)(1).


60. ACLU v. Reno, 217 F.3d 162, 173-77 (3d Cir. 2000).

61. Id. at 177-80.


63. Id. at 585.

64. Id. at 577 (quoting ACLU v. Reno, 217 F.3d 162, 175 (3d Cir. 2000)).

65. Id. at 578.
On remand, the Third Circuit again reaffirmed the district court’s preliminary injunction. The court held that COPA does not satisfy strict scrutiny, which requires a statute to “(1) serve a compelling governmental interest; (2) be narrowly tailored to achieve that interest; and (3) be the least restrictive means of advancing that interest.” The court found that protecting children from harmful material on the Web is a compelling governmental interest. However, the court opined that COPA’s provisions regarding “material harmful to minors,” “commercial purposes,” and its affirmative defenses were not narrowly tailored to accomplish this task. The court also found that COPA was not the least restrictive alternative available to Congress. According to the court, “various blocking and filtering techniques...may be substantially less restrictive than COPA in achieving COPA’s objective of preventing a minor’s access to harmful material.” Finally, the court found that COPA suffers from “substantial overbreadth” as a result of numerous “unconstitutionally vague” terms.

In 2004, COPA went before the Supreme Court for a second time. In a 5-4 decision, the Court upheld the Third Circuit’s decision to allow the injunction to stand and remanded the case to the district court pending a full trial on the merits. Writing for the majority, Justice Anthony Kennedy began by rebutting the Third Circuit’s contention that the least restrictive alternative inquiry begins “with the status quo of existing regulations, then ask[ing] whether the challenged restriction has some additional ability to achieve Congress’ legitimate interest.” Applying this analysis, any speech restriction can be justified. Rather, “the court should ask whether the challenged regulation is the least restrictive means among available, effective alternatives.”

Using this analysis, the Court found that blocking and filtering software are less restrictive alternatives than COPA. According to the Court, blocking and filtering software are less restrictive because they permit the receiver

66. Ashcroft v. ACLU, 322 F.3d 240, 251 (3d Cir. 2003); see also Sable Commc’ns v. FCC, 492 U.S. 115, 126 (1989).
68. Id. at 251-55.
69. Id. at 256-57.
70. Id. at 257-61.
71. Id. at 265.
72. Id. at 266-71.
74. Id. at 666.
75. Id.
76. Id.
77. Id. at 666-67.
to determine what material he receives without criminally condemning a category of speech. The Court acknowledged that filtering software has a tendency to be over or under-inclusive. The Court brushed off this concern by noting, "[w]hatever the deficiencies of filters . . . the Government failed to introduce specific evidence proving that existing technologies are less effective than the restrictions in COPA."

The Court cited three additional reasons for allowing the injunction to stand pending a full trial on the merits. First, reversing the injunction may cause "a serious chill upon protected speech" because speakers may censor themselves "rather than risk the perils of trial." Second, substantial factual disputes remain on the record. And finally, "the factual record does not reflect current technological realit[ies] . . . ."

Scant attention has been given to Justice Kennedy's rejection of the Government's "argument that filtering software is not an available alternative because Congress may not require it to be used." Justice Kennedy felt that this "argument carries little weight, because Congress undoubtedly may act to encourage the use of filters" pointing out that the Court has "held that Congress can give strong incentives to schools and libraries to use them."

Here, Justice Kennedy was presumably referring to the Children's Internet Protection Act (CIPA). CIPA, which will be discussed in greater detail in the following section, requires schools and libraries receiving federal funds for Internet access to use a "technology protection measure" that blocks or filters Internet access to "visual depictions that are obscene, [involve] child pornography, or [which are] 'harmful to minors.'" Justice Kennedy went on to state, "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."

On remand from the Supreme Court, the Eastern District of Pennsylvania recently reaffirmed its permanent injunction against the enforcement

78. Id. at 667.
79. Id. at 668-69.
80. Id. at 668.
81. Id. at 670-71.
82. Id. at 671.
83. Id.
84. Id. at 669.
85. Id.
of COPA.\textsuperscript{88} The district court cited three reasons for its holding. First, applying strict scrutiny, the court found that COPA is not narrowly tailored to Congress' compelling interest of "protecting minors from harmful material on the Web\textsuperscript{89} because it is over and under-inclusive.\textsuperscript{90} The statute is over-inclusive because its "broad definitions and provisions . . . prohibit[ ] much more speech than is necessary to further Congress' compelling interest.\textsuperscript{91} COPA is under-inclusive because it "is not applicable to a large amount of material that is unsuitable for children which originates overseas but is nevertheless available to children in the United States.\textsuperscript{92} The court also held that COPA's affirmative defenses do not sufficiently tailor the statute to Congress' compelling interest.\textsuperscript{93}

Second, the Government failed to show that COPA is the least restrictive and most effective alternative for achieving Congress' compelling interest.\textsuperscript{94} According to the court, the Government failed to rebut the plaintiffs' assertion that "filter software and the Government's promotion and support thereof is a less restrictive alternative to COPA.\textsuperscript{95} Moreover, although COPA has never been enforced, the Government "failed to show that filters are not at least as effective as COPA at protecting minors from harmful material on the Web.\textsuperscript{96} The court acknowledged that filtering technology is not perfect, but was ultimately persuaded by its ability to "block sexually explicit foreign material" and to provide parents with the opportunity to "customize filter settings depending on the ages of their children and what type of content they find objectionable.\textsuperscript{97} The court also notes that "filters are fairly easy to install and use.\textsuperscript{98} However, the court fails to take into account that many parents are not aware about the existence, much less the benefits, of filtering software.\textsuperscript{99}

Lastly, the court held that COPA suffers from vagueness and over-breadth. With respect to COPA's vague provisions, the court discusses cer-

\textsuperscript{89} Id. at 809.
\textsuperscript{90} Id. at 810.
\textsuperscript{91} Id.
\textsuperscript{92} Id.
\textsuperscript{93} Id. at 811.
\textsuperscript{94} Id. at 813-814.
\textsuperscript{95} Id. at 813.
\textsuperscript{96} Id. at 814.
\textsuperscript{97} Id. at 815.
\textsuperscript{98} Id.
\textsuperscript{99} See infra Part III.B.
Mandating an Affirmative Choice

tain language used in one section of the statute, but omitted or simply never defined in another. On the issue of overbreadth, the court states,

[B]ecause a story that might have "serious literary value" for a sixteen-year-old could be considered to appeal to the "prurient interest" of an eight-year-old and be "patently offensive" and without "serious value" to that child, Web publishers do not have fair notice regarding what they can place on the Web that will not be considered harmful to "any person under 17 years of age." The court was further troubled because the statute never explicitly stated that it was only intended for "commercial pornographers."

C. Children's Internet Protection Act

In 2000, Congress passed the Children's Internet Protection Act. The Act addresses libraries that receive federal subsidies via Internet access discounts and support under the Telecommunications Act of 1996 or from grants under the Library Services and Technology Act. The Act requires these libraries "to have in place certain Internet safety policies that protect both minors and adults from visual depictions which are obscene and involve child pornography, and for computers used by minors, visual depictions harmful to minors." Upon request, authorized persons may dis-

101. Id. at 819.
102. Id. at 820.
104. Id. § 254(h)(1)(B) (This section includes the Schools and Libraries programs (or E-rate), through which telecommunication carriers provide services to libraries and schools, at a lower rate than is charged to others).
105. 20 U.S.C. § 9121 (Supp. IV 2004) (This program distributes funds to libraries "to assist in accessing information through networks and pay costs associated with Internet accessible computers."); see Mota, supra note 59, at 107 n.120.
106. See Mota, supra note 59, at 107 (discussing the provisions of 47 U.S.C. § 254(h)); see 47 U.S.C. § 254(h)(7) (G) (stating that:

"Harmful to minors" refers to any picture, image, graphic image file, or other visual depiction that –
i) — taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.")
able the protection measure for bona fide research or other lawful purposes.107

Like Congress’ previous efforts to prevent children from accessing harmful material on the Internet, CIPA was challenged instantly. In a suit brought in the Eastern District of Pennsylvania, a group of public libraries, library associations, library patrons, and website publishers alleged that the Act was unconstitutional because it requires libraries to forego their First Amendment rights in order to receive federal funds and induces libraries to restrict their patrons’ First Amendment rights.108 The district court found that the Act should be subjected to strict scrutiny because “[s]oftware filters, by definition, block access to speech on the basis of its content.”109 Applying this standard of scrutiny, the district court found that the filtering software was not narrowly tailored110 and that less restrictive alternatives exist.111 Accordingly, the district court held that CIPA was “facially invalid under the First Amendment” and permanently enjoined its enforcement.112

On appeal, the Supreme Court reversed the district court.113 The issue before the Court was “whether the condition that Congress requires (use of filtering software) ‘would . . . be unconstitutional’ if performed by the library itself.”114 Chief Justice William Rehnquist, writing for a plurality, concluded that the use of filtering software by public libraries does not violate the First Amendment rights of library patrons.115 Thus, CIPA does not require libraries to violate the Constitution and, as such, is a legitimate exercise of power by Congress under the Spending Clause.116

The Court also determined that the district court erred in subjecting CIPA to strict scrutiny.117 According to the Court, a public library’s “need to exercise judgment in making collection decisions depends on its traditional role in identifying suitable and worthwhile material.”118 As institutions en-

47 U.S.C. § 254(h)(7)(D) (stating that “any person under seventeen years of age is a minor.”).
107. § 254(h)(5)(D).
109. Id. at 454 (citing United States v. Playboy Entm’t Group, Inc., 529 U.S. 803, 813 (2000)).
110. Id. at 475-79.
111. Id. at 480-84.
112. Id. at 496.
114. Id. at 203 n.2 (quoting Am. Library Ass’n, 201 F. Supp. 2d at 453).
115. Id. at 214.
116. Id.
117. Id. at 207 n.3 (quoting S. REP. NO. 106-141, at 7 (1999)).
118. Id. at 208.
Mandating an Affirmative Choice

trusted to promote and encourage the proliferation of knowledge, most libraries elect to "exclude pornography from their print collections because they deem it inappropriate for inclusion."119 Because these decisions are not subjected to heightened scrutiny, "it would make little sense to treat libraries' judgments to block online pornography any differently, when these judgments are made for just the same reason."120 Accordingly, "[i]n deciding not to collect pornographic material from the Internet, a public library need not satisfy a court that it has pursued the least restrictive means of implementing that decision."121

Ultimately, the Court determined that because public libraries retain their First Amendment rights, CIPA does not inhibit those libraries that choose to provide unfiltered access to patrons; rather, it merely "reflects Congress' decision not to subsidize their doing so."122

IV. Solution: Mandatory Choice

The CDA and COPA represent one school of thought on how to prevent children from accessing online pornography: content-based restrictions with criminal and civil sanctions for violators.123 As a result of their status as content-based restrictions, both statutes were subject to the highest standard of review, strict scrutiny. The fate of both statutes demonstrates that strict scrutiny is a very difficult standard to satisfy. Accordingly, Congress should refrain from attempting to pass substantively similar statutes.

The second, and preferable, alternative is the use of blocking and filtering software. On more than one occasion, the Court has specifically noted that blocking and filtering software are less restrictive and more effective means of preventing children from viewing pornography on the Internet.124 In fact, even a congressionally established commission found that blocking and filtering software are effective alternatives that pose relatively few First

119. Id.

120. Id.

121. Id. at 207 n.3.

122. Id. at 212.

123. See discussion supra Part II.A-B.

124. See generally Ashcroft v. ACLU, 542 U.S. 656, 672 (2004) (holding that the Government did not show that the less restrictive alternatives should be disregarded and may indeed be more effective than the provisions of COPA); see generally Am. Library Ass'n, 539 U.S. at 197 (expressing the view that filtering software can easily be disabled and that no better alternative had been presented).
Amendment concerns. In passing CIPA, Congress itself seemed to recognize and acknowledge this fact.

A. Blocking and Filtering Technology

An adequate discussion regarding the solution this article proposes requires explaining how blocking and filtering software work. At the most basic level, filtering software “allow[s] material or activities that are deemed inappropriate to be blocked, so that the individual using that filtered computer cannot gain access to that material or participate in those activities.”

Virtually all software companies use a combination of technology and human judgment to determine what constitutes inappropriate content. The process generally involves three steps. First, websites are classified into predetermined categories, such as “Adults Only,” “Drugs,” “Religion,” and “Violence.” Software companies create pre-determined categories by compiling “huge lists of Web addresses by following links from online directories . . ., by doing keyword searches on ordinary search engines, and by reviewing reports of newly-registered domain names.” In the second step, each flagged website is examined with automated systems that utilize keyword analysis. Based on this analysis, websites are recommended for inclusion in particular categories. Third, “a human receiver, at least in some companies . . ., makes the final decision” regarding how a website should be categorized. Unless requested to do so, most filtering companies


127. Id. at 21.


129. Bernfeld, supra note 128, at 237 n.15.

130. Id.

131. Id.

132. Id.
do not “re-review the contents” of websites after they have been categorized.133

Based on the analysis described above, four filter options have been developed: “client-side filters, content-limited Internet service providers, server-side filters, and search engine filters.”134 Client-side filters are installed in computers and a person with a password configures the profile of the system, which prevents others from accessing material that is deemed inappropriate.135 Content-limited Internet service providers provide and restrict access to certain subsets of the Internet for all subscribers.136 Server-side filters require “users at all access points” to conform to a pre-determined access policy.137 As a result, they are frequently used in institutional settings, such as school districts and libraries.138 Lastly, “search engine filters when activated by the user do not return links to inappropriate content found in a search, but they do not block access to specifically named Web sites.”139

Significant attention has been given to blocking and filtering software’s shortcomings. The primary complaints are that the software is under and over-inclusive.140 A filter is under-inclusive when it fails to block websites with indecent material.141 This occurs when the software “relies on pre-es-

133. Am. Library Ass’n v. United States, 201 F. Supp. 2d 401, 430 (E.D. Pa. 2002). With respect to requests to re-review particular categorizations, there is no guarantee that filtering companies do so in an accurate or timely fashion. While this is problematic, it does not directly affect the proposal made in this article. For the purposes of the proposal made in this argument, the only thing that matters is that websites that are filtered as a result of their categorization have some method of requesting that that categorization be re-reviewed.

134. See Novak, supra note 7, at 355 (providing a more complete discussion regarding filters).

135. Youth, Pornography, and the Internet, supra note 126, at 12.1.1; see Novak, supra note 7, at 355.

136. Youth, Pornography, and the Internet, supra note 126, at 12.1.1; see Novak, supra note 7, at 355-56.

137. Youth, Pornography, and the Internet, supra note 126, at 12.1.1; see Novak, supra note 7, at 356.


139. See id. (explaining Youth, Pornography, and the Internet, supra note 126, at 12.1.1). Generally speaking, when “a user attempts to access a Web site or page that is blocked by the filter, the user is immediately presented with a screen that indicates that a block has occurred as a result of the operation of the filtering software. These ‘denial screens’ appear only at the point that a user attempts to access a site or page in an enabled category.” Am. Library Ass’n v. United States, 201 F. Supp. 2d 401, 429 (E.D. Pa. 2002).

140. Merlis, supra note 6, at *35.

141. Id.
established lists to filter out indecent websites."142 Unless the software is updated on a regular basis, these lists date quickly.143 Filters are also under-inclusive because they rely on text analysis.144 Text analysis is incapable of appropriately identifying and restricting access to indecent images.145 As a result, it is not uncommon for websites with images but no text to bypass a filter's grip.146 Software providers have attempted to address this shortcoming by developing filters that identify "large expanses of what is likely to be flesh in an image."147 Unfortunately, this technology is "highly error-prone."148

Filters, on the other hand, are over-inclusive when they block websites that contain material that is not indecent.149 This typically occurs because filters cannot properly analyze the meaning of text. As a result, "filters sometimes block educational websites containing words typically associated with indecent publications."150 In order to preempt complaints that their software is ineffective, which may occur with under-inclusive blocking, many manufacturing companies pre-configure over-inclusive settings.151

The most serious threat posed by over-inclusive filters is their potential to degrade the First Amendment through censorship. Unless a user is knowledgeable about the filter's settings, it is possible that he could unknowingly be denied access to speech that he is constitutionally entitled to receive.152 This argument is most effective in public settings, such as public libraries, where users are unable to adjust the filter's settings.153 However, it fails to apply "to filters voluntarily used in private homes."154 If a user is unsatisfied

142. Id.
143. Id.
144. Id.
145. Id.
146. Id. (citing Kevin W. Saunders, Do Children Have the Same First Amendment Rights as Adults?: The Need for a Two (or More) Tiered First Amendment to Provide for the Protection of Children, 79 CHI.-KENT L. REV. 257, 259 (2004)).
147. YOUTH, PORNOGRAPHY, AND THE INTERNET, supra note 1248, at 56; see Weekes, supra note 866, at 68 n.143.
148. Id.
149. Merlis, supra note 6, at *36.
150. Id.
151. Id.
152. Id. at *37.
153. Id.
154. Id.
with the settings, assuming he is adequately informed regarding those settings, he can simply “adjust the filters or remove the filters altogether.”

B. Mandating an Affirmative Choice

In Ashcroft, the Government argued that the primary reason for Congress’ apprehension to the use of filters was that “Congress may not require” their use. The Court rejected this argument on the basis that “Congress may act to encourage such use . . . by promoting the development of filters by industry and their use by parents.” Although the Court is correct, its argument does nothing to address the fact that a significant number of parents are not aware or knowledgeable about the existence and benefits of filters. This, in turn, suggests that parents “will fail to act.”

Instead of merely providing parents with incentives to acquire blocking or filtering software, Congress should pass a law requiring all new computers to come with pre-installed blocking and filtering software. The software should require the purchaser (or first user) to make a mandatory affirmative choice during the initial setup, regarding the software’s settings on each user’s account for that computer. Such a law may take the following form:

155. Id.
157. Id.
158. Merlis, supra note 6, at *39.
160. Given that virtually all activity on the Internet is interstate by nature, Congress could pass such a law under the auspices of the Commerce Clause. U.S. CONST. art. I, § 8, cl. 3. Because virtually all computers have the ability to connect to the Internet and filtering software impacts online activities, the Commerce Clause provides Congress with ample authority to pass such a law.
162. This amounts, in essence, to a client-side filter.
163. See Ian Ayres, Valuing Modern Contract Scholarship, 112 YALE L.J. 881, 899 n.79 (2003). According to Professor Ayres, an “affirmative choice rule is a type of penalty default that forces contractors to make an affirmative choice in order to create a contract.” Id. Here, if the user does not make a decision regarding the software’s settings, during the initial setup, he will simply not be able to use the computer.
In recognition of the threat that pornography and other indecent and harmful materials on the World Wide Web poses to America's youth, and to limit the opportunities for minors to be exposed to such materials,

(a) Computer manufacturers.
1. Computer manufacturers shall include blocking and filtering software on all personal desktops and laptops sold in the United States;
2. that includes a menu requiring the activating user to affirmatively select whether to block and filter particular Internet categories for each account on the computer; and
3. include a label on the packaging of the computer that informs the user that an affirmative choice regarding blocking and filtering settings must be made in order to activate the computer.

(b) Software requirements.
1. The software must require action by the activating user during the computer's initial set-up;
2. contain a menu listing all possible categories that a user may select to block or filter;
3. contain no pre-checked categories;
4. adequately inform and explain to the activating user the purpose of the software, how the software works, the types of websites that may be blocked by selecting to block and filter a particular category, and all other relevant information;
5. create a menu on the activating user's account that allows the activating user to change the settings at any time; and
6. require the activating user to create a password to access the menu for changing the blocking and filtering settings.

A law incorporating these provisions would address virtually every concern enunciated by Congress and the courts.

As the previous subsection demonstrated, filters that depend upon user involvement in private homes do not upset the First Amendment. Filters, unlike content-based restrictions, "impose selective restrictions on speech at the receiving end, not universal restrictions at the source."164 Including a menu that lists all the possible categories that may be blocked165 and requ-

165. For example, N2H2 Bess/i2100 offers the following categories: "Adults Only; Alcohol; Auction; Chat; Drugs; Electronic Commerce; Employment Search; Free Mail; Free Pages; Gambling; Games; Hate/Discrimination; Illegal; Jokes; Lingerie; Message/Bulletin Boards; Murder/Suicide; News; Nudity; Personal Information; Personals; Pornography; Profanity; Recreation/Entertainment; School Cheating Information; Search Engines; Search Terms; Sex; Sports; Stocks; Swimsuits; Tasteless/Gross; Tobacco; Violence; and Weapons." Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 428 (E.D. Pa. 2002). Moreover, "N2H2 offers seven 'exception categories,'" which include "Education, Filtered Search Engine, For Kids, History, Medical, Moderated, and Text/
Mandating an Affirmative Choice

Mandating an Affirmative Choice

...ing users to make a conscious and affirmative choice regarding whether to filter websites that are identified as “Adults Only,” “Drugs,” “Religion” or “Violence,” would not upset the First Amendment because users would retain the ability to program the settings according to their own preferences. Adults, with or without children, would be able to gain access to protected speech by simply turning off the technology on their personal accounts. Moreover, Congress could minimize any potential allegations that the statute violates the First Amendment by including a provision that requires the software to adequately inform users of the likely effects associated with selecting to block and filter a particular category. This would ensure that any censorship is self-imposed. In the end, only children would have their In-

Spoken Only. When an exception category is enabled, access to any Web site or page via a URL associated with both a category and an exception . . . will be allowed, even if the customer has enabled the product to otherwise . . . block the category . . . .” Id. at 428-29.

SmartFilter provides the following categories: “Anonymizers/Translators; Art & Culture; Chat; Criminal Skills; Cults/Occult; Dating; Drugs; Entertainment; Extreme/Obscene/Violence; Gambling; Games; General News; Hate Speech; Humor; Investing; Job Search; Lifestyle; Mature; MP3 Sites; Nudity; Online Sales; Personal Pages; Politics, Opinion & Religion; Portal Sites; Self-Help/Health; Sex; Sports; Travel; Usenet News; and Webmail.” Id. at 429.

Bernfeld, supra note 128, at 237.

Borrowing further from Professor Ayres' concepts, a statute that requires computer companies to include filtering software which forces the activating user to make an affirmative choice regarding the software's settings for each account on the computer would serve as the functional equivalent of a legislative imposed mandatory, open-ended contractual menu. According to Professor Ayres, “[a] menu is a contractual offer that empowers the offeree to accept more than one type of contract.” Ian Ayres, Menus Matter, 73 U. Chi. L. Rev. 3, 3 (2006). The mandatory menu would run between two private parties: the computer company that includes the software and the computer purchaser. Moreover, the menu would be open-ended because the activating user would have the freedom to select from a variety of different filtering settings.

In practice, a mandatory, open-ended contractual menu would “protect those who need protecting (parents that are not aware or knowledgeable about the threat posed by online pornography and the benefits of filtering technology) without restricting the freedom of those who can do just fine on their own” and provide the offeree (the parent) with an opportunity to “opt-in” to the settings of his liking. Id. at 4, 8 (alteration in original); see generally id. (explaining the use of contractual menus).

In a recent online article, an ACLU spokesperson made the following argument against the use of filtering software: “most blocking software prevents access to sites based on criteria provided by the vendor,” which implies that “somebody out there is making judgments about what is offensive and controversial, judgments that may not coincide with [the user’s judgment]. The First Amendment exists precisely to protect the most offensive and controversial speech from government suppression.” Harry Hochheiser, Censorship in a Box: Why
ternet access restricted. Even then, parents would retain the ability to permit their children to view material they are prepared to handle.

In order to avoid any semblance of a content-based restriction, it is absolutely essential that the law contain a provision requiring that the software include no pre-checked categories. Although it is conceivable for a statute mandating certain categories to come pre-checked to pass constitutional muster, Congress should avoid taking any chances. A law requiring the activating user to affirmatively select each category he wants filtered would limit computer and software manufacturers to merely presenting the user with a list of categories available for restriction. Because the final decision to restrict access to certain categories would rest with the activating user, any content-based restriction would occur as a result of the activating user's own actions and, as a result, would not be constitutionally problematic.

A mandatory decision regarding the settings on each account would also directly address Congress' concern that parents "will fail to act." Prior to the release of Microsoft's Windows Vista, computers did not come equipped with blocking and filtering software. Windows Vista includes a centralized blocking software is wrong for public libraries, ACLU, Sept. 16, 2002, http://www.aclu.org/Privacy/Privacy.cfm?ID=13624&cc=252; see Bemfeld, supra note 128 (for a complete conversation regarding Hochheiser's article). The ACLU spokesperson is correct that filtering software has the potential to be over-inclusive. However, under the solution proposed in this article, the activating user would make a conscious decision regarding what material he wants filtered on each account. If the filtering manufacturer adequately explains to the activating user the effects of selecting each category, a user that selects the most restrictive form of filtering would undoubtedly be aware that he may be restricted from viewing material that is neither obscene nor indecent. As a result, any First Amendment restriction would be self-imposed.

169. This is not problematic because "constitutional interpretation has consistently recognized that the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society. 'It is cardinal with us that the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder.'" Ginsberg v. New York, 390 U.S. 629, 639 (1968) (citing Prince v. Massachusetts, 321 U.S. 158, 166 (1944)).

170. This could be accomplished several ways. First, the filtering software could periodically ask the user that activates the computer to make an updated decision regarding each account's settings. Second, the filtering software should include a menu on the activating user's account that allows him to update each user's settings at his own leisure. A provision incorporating either of these options could be included in the statute.

171. At a very minimum, the software would have to make it known to the user that certain categories are pre-checked and provide the user with a clear opportunity to accept or reject these selections.

Mandating an Affirmative Choice

Parental Controls panel, as a part of the User Accounts and Family Safety Control Panel applet, which “provides a centralized location where [the parent] can turn parental controls on and off; block or allow specific programs, games, and websites; and set controls for every aspect of [a] child’s computer use.”\textsuperscript{173} Although commendable, the mere inclusion of such software is insufficient because parents that are not technologically savvy may never use or even know that the software is on their computer. In this respect, Windows Vista fails to provide adequate relief. However, by passing legislation that requires a mandatory decision, parents would have no choice but to become familiar with filtering technology and to make an affirmative choice regarding each account’s settings.\textsuperscript{174}

Congress should require that blocking and filtering software provide a weekly summary to the activating user of all users’ activities in order to prevent technologically savvy children from avoiding the settings put in place by their parents.\textsuperscript{175} Functionally, this would operate similarly to monitoring devices, which act “as a deterrent rather than a preventative measure because the parent monitors the child’s online activity rather than blocking material [and] the threat of punishment or embarrassment will deter children from viewing web sites that they know are unsuitable for their eyes.”\textsuperscript{176}

\textsuperscript{173.} Microsoft Windows Vista, Parental Controls, http://www.microsoft.com/windows/products/windowsvista/features/details/parentalcontrols.mspx (last visited Sept. 25, 2007). According to Microsoft, “Internet Explorer 7 in Windows Vista gives parents the ability to create filters and settings to block children’s access to objectionable content and approve access to trusted or acceptable sites.”\textit{Id.}

\textsuperscript{174.} A mandatory decision default is also superior to a filtered default because a filtered default runs the risk of functioning as a form of content-regulation. If the computer company and software manufacturer make the decision regarding the computer’s settings without the activating user’s involvement, protected speech may be filtered without the user’s consent. This exact concern is the reason that Congress should require computer companies and filtering manufacturers to include an open-ended menu which requires the activating user to actively select the categories he wants filtered on each account. This will require computer companies and filtering manufacturers to adequately inform the activating user of the types of websites that will [and may] be blocked if a particular category is selected. If structured exactly along these lines, any content-regulation would result solely from the activating user’s own choices.

\textsuperscript{175.} Microsoft Windows Vista,\textit{ supra} note 173 (To Microsoft’s credit, Windows Vista contains, as a part of the Parental Controls panel, an activity report that allows parents to monitor how their children have been using the computer. Unfortunately, Vista’s activity reports only appear when prompted by the user. As a result, parents that are not knowledgeable about this feature may never use it. However, requiring the activity report to appear at set times will ensure that all parents review their children’s activities on the Internet).

\textsuperscript{176.} Novak,\textit{ supra} note 7, at 357.
Moreover, a law incorporating the provisions proposed in this article would place the onus back where it belongs: on parents. As Ginsberg recognized, “parents’ claim to authority in their own household to direct the rearing of their children is basic in the structure of our society.” 177 The current problem is that parents are not completely aware of the threat that online pornography poses to their children. Most parents are also not equipped with the tools necessary to restrict their children’s access to indecent material on the Internet. Instead of taking it upon itself to say what minors can and cannot view on the Internet, Congress should be mindful that parents have the “primary responsibility for children’s well-being [and] are entitled to the support of laws designed to aid discharge of that responsibility.” 178 Ultimately, parents are in the best position to determine what material their children are prepared to view.

The release of Vista addresses two issues that would have arisen from this proposal. The first concerns the financial burden associated with requiring all computers to come with blocking and filtering software. The second concerns how computer companies should implement the blocking and filtering requirements. With respect to the financial implications, because such a large percentage of computers that are sold in the United States include a Microsoft operating system, 179 the cost of affixing such software to computers has already been largely internalized into the market. 180 The only mainstream alternative to a Microsoft operating system is Apple’s Mac OS X, which constitutes a mere five percent of the market for computers in the United States. 181 As a result, a law requiring inclusion of the software argued for in this article should not have a large financial impact on the ability of most Americans to purchase computers. Lastly, assuming that Apple and other computer manufacturers that do not use a Microsoft operating system follow the example set by Microsoft, computer companies may find it more cost efficient and less burdensome to develop their own blocking and filtering software.

V. CONCLUSION

Although researchers may never be capable of demonstrating the exact detrimental effects of pornography on minors, there is little doubt that online pornography has the potential to severely harm the psychological develop-

178. Id.
180. Assuming that Windows Vista becomes the standard operating system for all personal computers that feature a Microsoft operating system.
181. Market Share, supra note 179.
ment of children. In recognition of this fact, Congress cannot allow the constitutional fate of the CDA and COPA to dissuade it from continuing to protect America's youth. The Supreme Court's decision to uphold the use of blocking and filtering software in CIPA should persuade Congress to refrain from passing laws containing content-based restrictions.

Instead, Congress should pass a law that requires all computer companies to include blocking and filtering software that requires the activating user to make a mandatory, affirmative, and informed choice regarding the software's settings for each account on the computer. Although blocking and filtering software restricts material on the Internet on the basis of its content, an informed user's active participation guarantees that any speech restriction is self-imposed. Accordingly, blocking and filtering software does not violate the First Amendment right to, among other things, receive constitutionally protected speech. Moreover, requiring an activating user to make a mandatory choice regarding other computer users' access level will shift the burden of protecting children back to parents, while making sure that they are adequately informed and equipped to act. In the final analysis, rearing children is an activity that is best left to parents. The solution proposed in this article accomplishes this task, without violating the First Amendment, by requiring parents to make a mandatory choice regarding what type of material their children may view on the Internet.