PICS, or it Won't Happen

by

Linus Banghart-Linn

Submitted in partial fulfillment of the requirements of the

King Scholar Program

Michigan State University College of Law

under the direction of

Professor Michael Lawrence

Spring, 2009

Introduction

The United States has long had a deep commitment to the principle of free speech. It is enshrined as one of the enumerated freedoms in the First Amendment to the Constitution, in terms that are, on their face, fairly unambiguous.[1] Although scholars and jurists differ on the appropriate breadth of First Amendment protection of speech, from the absolutist position under which "no law abridging" is read to mean "no law abridging,"[2] to the view that the prevention of prior restraints is the "chief purpose" of the First Amendment,[3] to any view in between. The consensus has been that the First Amendment protection of speech is fairly broad.

As broad as the protection afforded by the First Amendment is, however, it is not absolute. Certain categories of speech have been afforded limited or no protection. Among these are categories of speech which are recognized as harmful to the community and lacking in social value, including obscene speech.[4] The Supreme Court has also recognized that restrictions on speech are permissible when children are an audience.[5] Congress has acted to protect children in the realm of broadcast radio and television,[6] but as yet, no effective system for protecting children from content on the internet is in place. Twice Congress has passed statutes, and twice they have been struck down by the Supreme Court as unconstitutionally interfering with protected communications between adults.[7]

A system called PICS exists that allows publishers of content on the internet to tag content in terms of its appropriateness for children.[8] It also allows users to filter and block content they deem inappropriate. PICS never took off in the nineties when it was being

---

[1] U.S. Const. Amend. I ("Congress shall make no law . . . abridging the freedom of speech. . . .").
[2] Smith v. California, 361 U.S. 147, 221 (1959) (Black, J., concurring).
[3] *E.g.* Near v. Minnesota, 283 U.S. 697, 713 (1931).
[4] *E.g.* Roth v. United States, 354 U.S. 476 (1957).
[5] *See*, *e.g.*, Ginsberg v. New York, 390 U.S. 629 (1968).
[6] *See*, *e.g.*, FCC v. Pacifica Foundation, 438 U.S. 726 (1978);
[7] *See infra* discussion accompanying notes - and notes - .
[8] *See* Platform for Internet Content Selection, http://www.w3.org/PICS/

developed, possibly because it was completely voluntary, both on the publisher and consumer sides. But a system like PICS that gives parents and teachers a tool to effectively block potential harmful content through a system of voluntary tagging should be revived, since it is the most effective way to protect children consistent with the First Amendment's guarantees of free speech.

This paper proceeds in four Parts. Part I describes the background of constitutionally permissible restrictions on speech, particularly obscene speech and speech that reaches or may reach minors. It then describes attempts by Congress to restrict obscene and indecent speech on the internet, and why they have failed. Part II describes the PICS system that was developed in the late 1990s as a tool to allow publishers and users of the internet to apply and use labels to filter content. Part III discusses Professor Kevin Saunders' proposals regarding a PICS-like system, including his proposal to mandate filtering capability in browsers, and to use such a system as an aid in assigning criminal liability to those who distribute obscene materials. Part IV discusses another proposal, how it differs from Professor Saunders', and some of the limitations of PICS, and proposes changes and additions in order to make it fully effective.

I. Background – Restricting Obscene Speech, Access by Minors, Broadcast and Internet Speech

To see why PICS or a similar system is the best way for the government to protect children from harmful content, it is necessary to examine the contours of the government's ability to constrain this type of speech.

A. History of Censorship of Obscenity

Although the text of the First Amendment uses "unconditional language" in its grant of protection to free speech,[9] the Supreme Court has not held that the protection itself is unconditional. For example, defamation is not subject to First Amendment protection, and civil

[9] Roth v. U.S., 354 U.S. 476, 483 (1957).

and criminal liability may be imposed with no constitutional problem,[10] and incitement to lawlessness is also punishable.[11] Within these categories, the Court has tread carefully, balancing the harm to society against the social value of the speech sought to be punished. For example, while defamation is punishable, defamation of a public official may not be punished without a showing of "actual malice."[12] The Court raised the bar for this type of offense because of the recognition of the value to society of allowing criticism of public officials. Or for speech that is likely to incite a breach of the peace, the standard is high for showing that the speech is punishable, again recognizing the social value in protecting unpopular speech, and restricting punishment to cases where there is a "clear and present danger"[13] of violence.

Although obscene speech is always outside of the protection of the First Amendment, the Court has worked a similar balancing between social value and harm, but it has accomplished this by inserting the balancing test into the definition of obscenity itself. Obscenity is famously hard to define,[14] but it has a modern definition in the *Miller* test: "(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual content specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."[15] While the second prong lends itself to a relatively objective application, the other two prongs mean that a particular work cannot be deemed obscene in a vacuum – instead, the work must be judged against the applicable community standards, and no single part of the work may render the work obscene,

---

[10] *See* Beauharnais v. Illinois, 343 U.S. 250, 255-56 (1952).
[11] *See*, *e.g.*, Schenck v. United States, 249 U.S. 47 (1919).
[12] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964).
[13] *Schenck*, 249 U.S. at 52.
[14] *See* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., dissenting).
[15] Miller v. California, 413 U.S. 15, 24 (1973).

but the work must be examined as a whole. It is even possible for the same work in the same community to be obscene for one audience but not for another.[16]

B. History of Punishment of Distributing Materials to a Minor

There are two things to keep in mind regarding the constitutionality of laws that restrict the distribution of obscenity to minors. The first is that the Supreme Court has recognized that different standards of obscenity are applicable to different audiences. Because of this, laws which restrict material which is obscene for minors may also restrict the same material for adults, to whom it is protected. In 1968, the Supreme Court upheld the conviction of Sam Ginsberg for distributing obscene materials to a sixteen-year-old boy, in violation of a New York statute.[17] The Court characterized the materials as obscene for a minor, but "not obscene for adults"[18]; since they were obscene for a minor, they lacked the protection of the First Amendment with respect to minors. In 1957, the Court had considered a Michigan statute also designed to protect children from "obscene, immoral, lewd, or lascivious" materials.[19] In that case, the Court had reversed the conviction, because it attempted to bar the distribution of materials that might harm minors to anybody, including adults. The *Ginsberg* Court distinguished the New York statute from the one at issue in *Butler* by noting that the New York statute did not bar the distribution of the magazines in question to adults.[20] One requirement of any statute that seeks to protect minors from harmful communications is that the law have no greater effect than necessary on protected communications between adults. A law that restricts protected communication impinges on a fundamental right, and is subject to strict scrutiny. In order to be upheld, it must be narrowly

[16] Ginsberg v. New York, 390 U.S. 629, 634 (1968) (upholding conviction of sale of obscene magazines to minor, noting "The 'girlie' picture magazines involved in the sales here are not obscene for adults.")
[17] *Id.* at 645.
[18] *Id.* at 634.
[19] Butler v. Michigan, 352 U.S. 380, 381 (1957).
[20] *Ginsberg*, 390 U.S. at 635.

tailored to a compelling governmental interest, and it must be the least restrictive means available to carry out that interest.[21] The *Ginsberg* law restricted material that would have been obscene with respect to adults, but it did not restrict the distribution of such materials to adults, and was held constitutional. The *Butler* law did restrict such distribution, and was held unconstitutional.

C. Government Responses to Different Forms of Media

As new media came to prominence in the last century, the Supreme Court has recognized that different rules are appropriate to deal with different forms of media. For example, the Court has upheld restrictions on radio broadcasts that would not be upheld if applied to print media.

Radio and television are a fundamentally different medium from print when it comes to the difficulties of protecting minors from objectionable content. Even a mass-produced book or magazine can have its sale restricted to adults, so that no copy finds its way into the hands of a minor, at least in theory. But with a radio or television broadcast, there are no "copies" – anyone with a radio or television may access the content, if they tune into the right station at the right time. Unlike the statute at issue in *Butler*, which was struck down because it interfered with communications between adults, the Federal Communications Commission has been allowed to regulate radio and television broadcasts for the protection of children, even though those regulations necessarily interfere with adult-to-adult communications. There is not even a requirement that the materials regulated be obscene. The regulation upheld in *FCC v. Pacifica Foundation* was not limited to obscene speech; in fact, the speech at issue in the case, a radio broadcast of George Carlin's "Filthy Words" monologue, was indecent but not obscene.[22] In spite of this, the Supreme Court upheld the fine, noting that "the First Amendment has a special

[21] *E.g.* Kramer v. Union Free Sch. Dist. No. 15, 395 U.S. 621 (1969).
[22] 438 U.S. 726, 729 (1978).

meaning in the broadcasting context."[23] Given the special nature of radio broadcasting, and the fact that this broadcast was in the early afternoon, both of which created an increased risk that children might be exposed to the monologue, the Supreme Court held that the fine did not violate the First Amendment.[24]

D. Government Responses to the Internet

The development of the internet, followed by its increase in popularity and now near ubiquity, have presented new challenges to the balance between the interests in protecting children and protecting free expression. Previously, with radio and television, the main providers of programming have been a few good-sized corporations, licensed by the federal government. Posting content on the internet, on the other hand, is easy for nearly anyone, and practically free. Even those who are unable to afford a computer may go to their nearest public library.

Congress has already made three attempts to protect children from harmful content on the internet. The Communications Decency Act of 1996 (CDA), criminalizing the distribution of any obscene content knowing that the recipient is under 18, or displaying certain objectionable content to children under 18.[25] The CDA contained affirmative defenses to prosecution, protecting those who restricted access to minors by requiring a credit or debit card, or an adult access code or personal identification number,[26] and those who took "good faith, reasonable, effective, and appropriate actions" to restrict access by minors. The Supreme Court struck down the CDA in 1997, because of its effect on protected communications between adults.[27] Congress's second attempt was the Child Online Protection Act (COPA), passed in 1998. The

---

[23] *Id*. at 741 n.17 (1978).
[24] *Id*. at 750.
[25] 47 U.S.C. § 223.
[26] *Id*. § 223(e)(5).
[27] ACLU v. Reno, 521 U.S. 844 (1997).

Supreme Court upheld an injunction against the enforcement of this law as well, in 2004.[28] In 2007, the Eastern District of Pennsylvania District Court again enjoined the enforcement of the COPA,[29] the Third Circuit Court of Appeals affirmed,[30] and the Supreme Court did not hear the appeal.[31] The CIPA is a more narrowly focused effort; it denies federal assistance to schools and libraries who do not comply with its requirements of placing filtering software on their computers.[32] The CIPA was upheld by a divided Supreme Court, due to the fact that it acted through Congress's spending power rather than by a direct prohibition on speech, and also as a result of the fact that it allowed libraries to partially turn off the filter for adults.[33]

1. The CDA – What it Did and Why it Failed

The day after the CDA went into effect, the ACLU and other plaintiffs filed suit in the Eastern District of Pennsylvania, seeking to enjoin the government from enforcing the statute.[34] The plaintiffs attacked the CDA on grounds of vagueness and overbreadth. Vague laws violate the Fifth Amendment's guarantee of due process because they fail to give notice to individuals whether their conduct is breaking the law in question.[35] Overbroad laws that restrict speech violate the First Amendment by taking too much speech within its breadth, punishing protected speech along with the speech that may be punished.[36] A three-judge panel heard the case, pursuant to a provision of the CDA. The District Court granted the injunction, holding, in three separate opinions, that the challenged sections of the statute were unconstitutional.[37]

---

[28] Ashcroft v. ACLU, 542 U.S. 656 (2004).
[29] ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007).
[30] ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008).
[31] Mukasey v. ACLU, __ U.S. __, 129 S. Ct. 1032 (Jan. 21, 2009).
[32] 20 U.S.C. §7001 *et seq*.
[33] United States v. American Library Association, Inc., 539 U.S. 194 (2003).
[34] ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).
[35] *See*, *e.g.*, City of Chicago v. Morales, 527 U.S. 41 (1999).
[36] *See*, *e.g.*, *id*.
[37] ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).

In the first of the opinions, Chief Circuit Judge Sloviter expressed concern that the CDA was likely vague and not narrowly tailored with respect to minors,[38] but ultimately granted the injunction because of the restrictions it would put upon speech that was protected with respect to adults. The material the CDA restricted, defined as "indecent" and "patently offensive," reached beyond obscenity, without limitation by the *Miller* requirements of appeal to a prurient interest and lacking serious value.[39] Judge Sloviter was not satisfied by the affirmative defenses offered by the CDA,[40] finding that the "[c]redit card and adult verification services . . . are not technologically or economically feasible for most providers,"[41] and that no technology existed at the time that would allow implementing other "reasonable, effective, and appropriate actions" to prevent minors from accessing the indecent material. , although the governmental interest that was supposed to justify the CDA was protecting minors from harmful content, the CDA was not limited to material that was harmful to minors. Content-based restrictions on speech are subject to strict scrutiny, which requires that they be narrowly tailored to meet the asserted governmental interest.

Judge Buckwalter concurred with Judge Sloviter but wrote a separate opinion, focusing on the vagueness of the CDA, which criminalized "indecency" without defining it, leaving providers of content on the internet potentially uncertain as to whether their websites might subject them to criminal penalties.[42] Apart from the due process problems caused by including vague terms in a criminal statute, there is also a First Amendment concern. If those who speak on the web are uncertain exactly where the line is between the lawful and the criminal, they will "undoubtedly" temper their speech to ensure that they are on the lawful side. This chilling effect

---

[38] *Id.* at 852-53.
[39] *Id.* at 855.
[40] 47 U.S.C. §223(e)(5).
[41] ACLU v. Reno, 929 F. Supp. at 856.
[42] *Id.* at 860-61.

of the statute on protected speech was Judge Buckwalter's chief concern in finding the CDA unconstitutional.

The third opinion, by Judge Dalzell, focused on the unique nature of the internet as a new and dynamic – even "chaotic" medium of communication, whose very strength lay in its chaos.[43]

The case was appealed directly to the Supreme Court, pursuant to the CDA's "fast-track" review provision, which provided that any finding by the District Court panel that the CDA was unconstitutional was "reviewable as of right by direct appeal to the Supreme Court."[44] The Supreme Court affirmed the grant of the injunction.[45] The Court's opinion, authored by Justice Stevens writing for a seven-Justice majority, held that the CDA was overbroad on its face because it purported to cover "indecent" material, not just material that was obscene, and because "indecent" was not satisfactorily defined within the statute.[46] The Court pointed out that, while vagueness is always a concern for criminal statutes, there is a special concern about vagueness when it comes to a content-based restriction on speech.[47] Vague restrictions on speech result in a "chilling effect," as speakers who are not certain whether their speech is punishable self-censor to avoid the possibility of prosecution; the Court found this chilling effect "obvious."[48]

2. COPA – What it Did and Why it Failed

Congress's second attempt to regulate indecency on the internet was the Child Online Protection Act (COPA), passed in 2003. COPA criminalized the posting on the World Wide Web of "material harmful to minors."[49] In defining "material harmful to minors," COPA

---

[43] *Id*. at 883.
[44] Telecommunications Act of 1996, Pub. L. No. 104-104, § 561(b), 110 Stat. 56, 143.
[45] Reno v. ACLU, 521 U.S. 844 (1997).
[46] *Id*. at 870-71.
[47] *Id*.
[48] *Id*. at 871.
[49] 47 U.S.C. §231(a)(1).

included obscene material, and then provided a definition that tracked the *Miller* definition of obscenity, but modified all three prongs by adding the language "with respect to minors"[50] – effectively banning material that is obscene with respect to minors. COPA also contained an affirmative defense, allowing a defendant to escape conviction if he or she restricted access to the site "by requiring use of a credit card, debit account, adult access code, or adult personal identification number; by accepting a digital certificate that verifies age; or by any other reasonable measures that are feasible under available technology."[51]

COPA, like CDA, was the subject of a challenge by the ACLU immediately after its passage in 1998, and the District Court for the Eastern District of Pennsylvania issued a preliminary injunction against its enforcement.[52] After dealing with issues of standing, the District Court found a substantial likelihood of success on the merits based on the burdens COPA placed both on publishers and adult consumers of non-obscene (with respect to adults) sexual content on the web.[53] As a content-based restriction on speech that was protected with respect to adults, the COPA was "presumptively invalid and subject to strict scrutiny,"[54] which requires the government to show that a challenged law is narrowly tailored to meet a compelling governmental interest, and that it serves this interest in the way that is least restrictive of protected speech. The district court had no problem finding a compelling governmental interest in the protection of children from obscenity online.[55] But the burden the COPA placed on publishers and consumers defeated the narrow tailoring requirement.[56]

---

[50] *Id.* §231(e)(6).
[51] *Id.* §231(c)(1).
[52] 31 F. Supp. 2d 473 (E.D. Pa. 1999).
[53] *Id.* at 493-95.
[54] *Id.* at 493.
[55] *Id.* at 495-96.
[56] *Id.* at 496-97.

With respect to publishers, the court noted that the burden of implementing the safeguards necessary to avail themselves of any of the COPA's affirmative defenses would be significant, and relevant to the discussion.[57] Further, the court was concerned that users would be discouraged from accessing the content by the intervening screens demanding credit or debit card information, or the hassle of having to get an adult access code, and about the negative effects this would have on the revenues of these sites. The court was careful to point out that the profitability of these sites was not a First Amendment concern per se, but that if these sites were pushed out of business by the COPA, that that would have First Amendment implications, as it would drive protected speech from the "marketplace of ideas."[58]

The district court also suggested that filtering and blocking software, although not completely effective, might be at least as effective as the COPA, and far less restrictive. The court took this as some evidence that the COPA would fail the "least restrictive means" requirement.[59]

The Third Circuit U.S. Court of Appeals affirmed, but instead of basing its decision on anything argued or briefed by the parties, or discussed by the district court, the Third Circuit found fault with COPA's reliance on "community standards." Because the internet is a community that extends to the entire nation and beyond, and because content providers cannot, generally, restrict web content to within or outside of a particular geographic location, the court felt that the application of "contemporary community standards" to determine whether or not content was obscene would allow the most prudish locale – the "most restrictive and conservative state's community standards" – to dictate what is obscene for all web publishers.[60]

---

[57] *Id.* at 494-95.
[58] *Id.* at 495.
[59] *Id.* at 497.
[60] ACLU v. Reno, 217 F.3d 162, 166 (3d Cir. 2000).

Because content providers on the web are unable to restrict their speech geographically, the Third Circuit feared providers would have to tailor their speech so as not to run afoul of the community standards of a particularly conservative community, thus all other communities would receive the same watered-down speech, and the ultimate result would be that the most conservative communities would set the level of acceptable speech for adults in all communities.[61]

The Supreme Court found this reasoning unconvincing, but the Court was split on the reasoning. In all, eight Justices voted to vacate the Third Circuit's decision and remand for further consideration.[62] Justice Thomas, writing for a five-Justice majority, held that "COPA's reliance on community standards . . . does not *by itself* render the statute substantially overbroad for purposes of the First Amendment,"[63] but he did not command a majority for the analytical portion of his opinion. In that portion of the opinion, Justice Thomas pointed out that, although community standards necessarily vary from community to community, the presence of "serious value" does not. The "serious value" requirement would thus serve as a "national floor for socially redeeming value," acting as a check on the ability of an unusually puritan community to render a particular piece of speech obscene.[64] Having pointed out how the "community standards" factor is tempered by the "serious value" requirement, the plurality portion of Justice Thomas's opinion referred to the cases of *Hamling v. United States*[65] and *Sable Communications of California, Inc. v. FCC*.[66] Both cases dealt with the national distribution of potentially obscene material, *Hamling* dealing with the mailing of obscene material, and *Sable* dealing with

---

[61] *Id*. at 176.
[62] *Id*.
[63] Ashcroft v. ACLU, 535 U.S. 564 (2002) (*Ashcroft I*).
[64] *Id.* at 579.
[65] 418 U.S. 87 (1974).
[66] 492 U.S. 115 (1989).

a "dial-a-porn" line. The statutes at issue in both cases were attacked for the same reason the COPA was being attacked: that it required "speakers" addressing a national audience to "tailor all their messages to the least tolerant community."[67] In both cases, the Supreme Court found no constitutional problem with requiring conformity with different community standards.[68] Plaintiffs attempted to distinguish *Hamling* and *Sable* as cases in which the speaker was able to control the communities to which the message was delivered.[69] Justice Thomas rejected that, pointing out that the statute in *Hamling* allowed prosecution "in any district through which obscene mail passed while it was on route to its destination," a path that was not within the control of the sender.[70] Further, Justice Thomas noted that, if COPA were held unconstitutional solely because of its reliance on community standards, it would be unconstitutional to apply *any* federal obscenity statutes to an internet setting, since obscenity statutes necessarily rely on community standards.[71] This would be a strange result in light of the fact that the Supreme Court had already upheld the portion of the CDA that banned online obscenity,[72] and the fact that no one was challenging the portion of the COPA that banned online obscenity.[73] Finally, Justice Thomas pointed out that, even if the COPA was overbroad, that alone was not enough to render it unconstitutional. Rather, in order to be unconstitutional, the statute had to be substantially overbroad.[74]

Justice Kennedy, joined by Justices Souter and Ginsburg, wrote separately, concurring only in the judgment. Although Justice Kennedy agreed with Justice Thomas that the plaintiffs had not shown that the reliance on community standards rendered the statute unconstitutionally

---

[67] *Id.* at 124 (*quoted in Ashcroft I*, 535 U.S. at 581).
[68] *Ashcroft I*, 535 U.S. at 581.
[69] *Id.*
[70] *Id.* at 582 n.12.
[71] *Id.* at 584.
[72] *Id*.
[73] ACLU v. Reno, 31 F. Supp. 2d 473, 479 n.1 (E.D. Pa. 1999).
[74] *Id.*

overbroad, they parted ways on the meaning of *Hamling* and *Sable*. While Justice Thomas quoted *Hamling* for the proposition that "the fact that distributors of allegedly obscene materials may be subjected to varying community standards in the various federal judicial districts into which they transmit the materials does not render a federal statute unconstitutional," Justice Kennedy read the cases as meaning that "requiring a speaker addressing a national audience to meet varying community standards does not *always* violate the First Amendment."[75] Justice Kennedy compared the idea of requiring Web publishers to conform to the most conservative community to the idea of "mak[ing] the eavesdropper the arbiter of propriety on the Web."[76] Although Justice Kennedy felt that reliance on community standards could potentially render the COPA unconstitutional, he agreed with Justice Thomas that such reliance alone did not. Since the plaintiffs made no showing of what speech was covered by the COPA, and what variations existed in community standards, Justice Kennedy described the situation as one in which "speculation meets speculation."[77]

Justices Breyer and O'Connor joined most of Justice Thomas's plurality opinion, but wrote separately to discuss the constitutionality and advisability of applying one national community standard, as opposed to different standards for different local communities.[78] Justice Stevens alone dissented, finding the criminalization of speech based on community standards to be unconstitutional in light of the inability of web content providers to segregate their content by geography.[79]

---

[75] *Id*. at 594 (emph. added).
[76] *Id.* at 596.
[77] *Id.* at 598.
[78] *Id.* at 586-91.
[79] *Id.* at 602.

On remand, the Third Circuit found other reasons to uphold the injunction.[80] Three provisions of the COPA were found not to be narrowly tailored: The definition of "material that is harmful to minors," which included the phrase "taken as whole"; the definition of "commercial purposes," which included the phrase "engaged in the business"; and the affirmative defenses.[81] With respect to the first provision, which the Third Circuit held that the COPA was overbroad in that it would hinder protected communication between adults.

The Supreme Court affirmed the injunction by a six-Justice majority.[82] Justice Kennedy's relatively short opinion noted that it was not in dispute that the COPA "was likely to burden some speech that is protected for adults."[83] Because of this, the Court held that the statute could only be upheld if it was "the least restrictive means among available, effective alternatives."[84] Noting the existence of filtering software, and the likelihood that such software would constitute a less restrictive means of achieving the same objective, the Court affirmed the injunction, strongly suggesting that the COPA was unconstitutional on its face.[85] After a trial, the District Court granted a permanent injunction against COPA's enforcement.[86] This was affirmed by the Third Circuit,[87] and earlier this year the Supreme Court denied certiorari, spelling the end of COPA.[88]

C. CIPA

A third federal statute that attempts to protect children from inappropriate content is the Child Internet Protection Act (CIPA), passed in 2000, which takes a much narrower approach. It

[80] ACLU v. Ashcroft, 322 F.3d 240 (3d Cir. 2003).
[81] *Id.* at 251.
[82] Ashcroft v. ACLU, 542 U.S. 656 (2004).
[83] *Id*. at 665.
[84] *Id*. at 666.
[85] *Id*. at 666-73.
[86] ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007).
[87] ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008).
[88] Mukasey v. ACLU, __ U.S. __, 129 S. Ct. 1032 (Jan. 21, 2009).

applies only to schools and libraries who receive federal assistance to help provide internet access to patrons, under either the E-Rate program pursuant to the Telecommunications Act of 1996[89] or pursuant to the Library Services and Technology Act (LSTA).[90] The CIPA does not directly require schools or libraries to do anything, but it makes E-Rate and LSTA assistance contingent on the installation of filtering software on their computers that block obscenity, child pornography, and material that is "harmful to minors."[91] The CIPA defines material harmful to minors in the same terms as the COPA.[92] The CIPA also required schools and libraries who received such federal assistance to have a policy in place that ensured the filters always blocked obscenity and child pornography, and blocked material harmful to minors whenever a minor was using the computer.[93] Adults could request to have the filter for the third category turned off while they used the computers.

The CIPA was challenged shortly after its passage by, among others, the American Library Association.[94] The U.S. District Court for the Eastern District of Pennsylvania held that the statute was unconstitutional, as the technology was not advanced enough to serve the purposes of CIPA without either overblocking or underblocking web content. If a library or school uses filtering software that underblocks (lets through material that should be blocked), it violates CIPA by not using software that is effective in preventing the proscribed types of content from being viewed. If a library or school uses filtering software that overblocks (blocks material that should be let through), reasoned the District Court, it defeats the requirement of narrow tailoring.[95]

---

[89] 110 Stat. 71, 47 U. S. C. §254(h)(1)(B).
[90] 110 Stat. 3009-295, as amended, 20 U. S. C. §9101 *et seq.*
[91] CIPA Sec. 3601(a)(1)(A)(i).
[92] CIPA Sec. 1703(b)(2).
[93] CIPA Sec. 3601(a)(1).
[94] American Library Association, Inc. v. United States, 201 F. Supp. 2d 401 (E.D. Pa. 2002).
[95] *Id*. at 489.

The Supreme Court, divided 6 to 3, and without a majority opinion, reversed, holding the CIPA to be constitutional.[96] Justice Rehnquist, writing for a four-Justice plurality, noted that the CIPA allowed libraries to turn off the blocking software upon the request of a user, and that that provision essentially eliminated any First Amendment concerns regarding overblocking.[97] Justice Kennedy, concurring, wrote separately to note that, if the unblocking took an inordinately long time, or if it were unavailable in some libraries, the CIPA would be vulnerable to an as-applied challenge.[98] Justice Breyer also concurred, calling for a lower level of scrutiny, heightened, but not strict.[99] There were two dissents as well: Justice Stevens argued that the state of the technology was such that overblocking was likely, and that the fact that adult patrons could request unblocking meant little, considering the patrons would have no way of knowing what the content was on the blocked site in the first place.[100] He also refused to distinguish between a federal law that would penalize libraries for failing to install filtering software, and a statute like the CIPA, which only refused to fund non-compliant libraries.[101] Justice Souter's dissent focused on comparing the CIPA to requiring a library to deny access to parts of its stacks to adult patrons.[102]

II. PICS

The *status quo*, then, is a lack of any constitutionally enforceable means of responding to the unique challenge the internet provides, enabling the protection of children from harmful content while still respecting to the greatest extent possible the right of adults to communicate with each other. To this end, Professor Kevin Saunders suggests a method of regulating speech

---

[96] United States v. American Library Association, Inc., 539 U.S. 194 (2003).
[97] *Id*. at 208-09.
[98] *Id*. at (Kennedy, J., concurring).
[99] *Id*. at 216 (Breyer, J., concurring).
[100] *Id*. at (Stevens, J., dissenting).
[101] *Id*. at
[102] *Id*. at (Souter, J., dissenting).

online.[103] Under his proposal, web browsers, email clients, and newsreaders would be required to have a feature similar to the "V-chip" on a television set: the ability to filter out content that is inappropriate for children. The filter could be set to respond to a signal attached to every web page, email, or news post. By default, every such file would be tagged as unsafe for children, and the publisher of the content would have the ability to toggle the tag to indicate that the content is safe for children. A browser with the filter activated would only display content that was tagged as safe for children. The law would criminalize the purposeful, knowing, or reckless distribution to minors of content that is obscene with respect to minors. Content would be tagged as either being safe for children or not, and web browsers would be required to have the ability to be configured to either block unsafe content, or let it through. Content providers would only be liable for providing inappropriate content to children if that content was tagged child-safe when it was posted. Those who provide content aimed at children, or consider their content to be appropriate for all ages, can tag the content child-safe, and know that all users will be able to access the content. Those who provide sexual, violent, or other "adult-oriented" content can tag the content not child-safe, and know that they will not be held liable if the content is delivered to a minor. On the user side, adults may leave the blocking feature turned off, and they will be able to access all web content. But adults who have children and wish to block objectionable content may turn on the blocking feature of their web browser.

In addition to providing parents and teachers with a tool to use to protect children, there is another facet to Professor Saunders' proposal. It would be an affirmative defense to a prosecution of distributing indecent material to a minor that that material was tagged as not

[103] Kevin W. Saunders, Electronic Indecency: Protecting Children in the Wake of the Cable and Internet Cases, 46 DRAKE L. REV. 1, 42-47 (1997).

child-safe. Criminal liability would only be imposed on those who publish obscene content tagged as safe for children, if that content is then accessed by a child.

This plan bears a number of similarities to the V-chip technology present in television sets currently. Although it is fairly clear that the United States may more directly regulate the content of television programming, the internet does not use the public airwaves, and is not considered as "intrusive" as television.

The Supreme Court discussed a "tagging" process similar to Professor Saunders' proposal in their arguments in *Reno v. ACLU*.[104] The system was discussed in two contexts: it was raised by the United States as a means of saving the CDA from being unconstitutional. The CDA contained an affirmative defense: if the defendant could demonstrate that he or she had taken "good faith, reasonable, effective, and appropriate actions" to prevent access by minors, this would constitute a defense to the conviction.[105] The argument of the United States was that the CDA was not overly restrictive because publishers could avail themselves of the tagging system with relatively little burden, and this would be the type of action that would be a defense.[106] The Supreme Court rejected this argument entirely, because no system was in place, and because it ultimately relied too heavily on the efforts of third persons: "Without the impossible knowledge that every guardian in America is screening for the 'tag,' the transmitter could not reasonably rely on its action to be 'effective.'"

The other context in which the tagging system was raised in *Reno v. ACLU* was as a less restrictive means of protecting children. As a content-based restriction on speech, the CDA had to be narrowly tailored to pass constitutional muster. Even though a tagging system was not in operation at the time of *Reno v. ACLU*, the fact that it was being developed and could have been

---

[104] 521 U.S. 844, 847 (1997).
[105] *Id*. at 881 (citing CDA, 47 U.S.C. §223(e)(5)).
[106] *Id.*

mandated by the government showed that the CDA as written was not the least restrictive means of achieving the goal, which is a requirement of narrow tailoring.[107]

I propose a plan based on the PICS technology, and similar to that advanced by Professor Saunders, but with a few changes and additions. Some of the changes I propose are minor improvements. Others relate to the most significant limitations to the proposal brought about by recent developments in internet communications: "Web 2.0" and Virtual Worlds.

A method for tagging internet content has been developed already, although not solely for the purpose of filtering out content that might be harmful to children. PICS[108] (Platform for Internet Content Selection) was a project in the latter half of the 1990s that sought to create a system similar to the V-chip, but "still better."[109] Specifically, PICS aimed to do three things: to "enable content providers to voluntarily label the content they create and distribute," to allow interested third parties to label content provided by others, and to "enable parents and teachers to use ratings and labels from a diversity of sources to control the information that children under their supervision receive."[110] It was not the intention of PICS to create a tool to allow governments to censor internet content, although they were aware that that was a possibility. PICS allows for much greater control, both by authors and consumers of internet content, than is needed to satisfy the concerns raised in this paper. Beyond simply labeling a web page as child-safe or not child-safe, PICS allowed authors to label their sites by level of "bad language" content, level of violent content, and level of sexual content. As a tool for parents and teachers, this makes PICS more valuable – consider, for example, the desired blocking levels of a

---

[107] *Id.* at 879.
[108] "PICS" was the name the group that developed the system of controls. In this paper, "PICS" also refers to the system of controls they developed.
[109] Paul Resnick and James Miller, PICS: Internet Access Controls Without Censorship, 39 Communications of the ACM 87-93 (1996), *available at* http://www.w3.org/PICS/iacwcv2.htm
[110] PICS Statement of Principles, *available at* http://www.w3.org/PICS/principles.html (last visited April 1, 2009).

kindergarten class computer, a home computer for a 12-year-old, a home computer for a 17-year-old, and a computer used in a 12th-grade advanced English classroom. The fact that each variable can be labeled on a continuum, rather than as a binary choice, allows those who supervise older children to have some relaxation on content without opening the flood gates. And the fact that the different types of content can be labeled separately means that the advanced English teacher can relax the blocking on language to allow students access to a broader variety of literary content, while still keeping a tight lid on, say, pornographic images.

But this flexibility, while a benefit in terms of the effectiveness of PICS as a tool for parents and teachers, it appears to be a detriment when it comes to using PICS as a tool for determining criminal liability. One commentator refers to this as a tension between rules and standards,[111] with the usual advantages and disadvantages of each category. Standards allow for greater flexibility, but reduced consistency and predictability. Rules allow for a more uniform treatment, but may, in a situation like this, force people to choose between two options they don't feel comfortable with.

Congress's next attempt at protecting minors from online obscenity should require PICS-type filtering technology in web browsers. It should be an affirmative defense to prosecution that the material in question was not tagged as safe for children. Professor Saunders proposes that the defense be that the material be tagged as unsafe for children. But since this statute would act as a content-based restriction on speech, it is important that the least restrictive means of regulating speech be employed. Instead of using the PICS-enabled browser to *exclude* tagged *unsafe* content, it should be configured to *include* only tagged *safe* content. This puts less of a burden on the providers of content, because it subjects them to prosecution only if they took an affirmative step which could only be aimed at making their content available to minors (or

[111] Jonathan Weinberg, Rating the Net, 19 Hastings Comm. & Ent. L.J. 453, 463 (1997).

uninterested adults). Because a PICS requirement places no burden on content providers, except for a minimal burden on those who wish to make their speech available to children, it should be free of the constitutional defects of the CDA and the COPA.

IV. Limitations on PICS and Proposals for Improvement.

One minor difference between my proposal and Professor Saunders' relates to the nature of the filtering signal. Although I agree with Saunders that the default setting should be the one which the browser will block if filtering is activated, I think it will be technically easier and less burdensome on providers if the default setting is no signal at all, as opposed to a signal that indicates the content may not be child-safe. By attempting to require posters to tag all content as safe or unsafe, a problem is created for providers who are unwilling, unable, or neglectful, for whatever reason, to see that the default signal is attached to their mails, posts, and files. Untagged content should be treated as child-unsafe by default. Browsers set to filter content would only display pages and files with the child-safe tag, and untagged content would be blocked. This would guarantee that posters of inappropriate content would not be punished unless they undertook the affirmative action of tagging the content as childsafe, and would also ensure that no burden would be placed on publishers of content unwillingly.

Another addition I which my proposal differs from Professor Saunders is that, while his proposal follows the pattern of the CDA and the COPA in providing affirmative defenses to prosecution, I propose to shift the burden, and, instead of making tagging an affirmative defense, make the adding of a child-safe tag an element of the offense. This might have little practical effect, but it addresses the concerns of Judge Sloviter, writing in the first opinion on the CDA, who noted that an affirmative defense is not a bar to prosecution, but only to conviction, and that

even an unsuccessful prosecution can impose a considerable burden on a defendant.[112] In order to come up with a law that is truly the least restrictive of protected speech, the less restrictive option of placing the burden on the government to prove inappropriate tagging is preferable to the more restrictive option of placing the burden on the defendant to prove appropriate tagging (or non-tagging).

One major limitation of using PICS for protection lies in the new architecture of the Web. Sometimes called "Web 2.0," many websites allow their users to upload material for other users to view, download, and otherwise interact with. Perhaps the best known example of this type of site is YouTube, which allows any user to upload a video file, which any other user may access. Many of the popular websites now are almost entirely user-provided content, including YouTube, photo hosting sites such as Flickr, "social networking" sites such as Facebook and MySpace, auction and advertising sites such as eBay and Craigslist, and blog hosts such as Blogger and Livejournal. Where should the criminal liability lie if a user uploads obscene content to one of these sites, and a minor user views the content? Under Saunders' plan as presented, it appears that the host of the content would be liable, instead of (or possibly in addition to) the user who actually added the content. This does not seem inherently unfair: after all, it is the host who sent the content to the minor user, and assuming distributing obscene content to a minor ought to be punishable, the host is a fair target. What is concerning about the rule is the effect it would have on many of these websites. Just as it is a First Amendment concern when protected speech is driven from the marketplace by government action, it should be considered a First Amendment concern when a new forum – indeed, a new *type* of forum – is driven from the marketplace. Although YouTube makes efforts to ensure that obscene videos are not posted on its site, the efforts center around finding and removing objectionable content after it is posted. Using its

[112] ACLU v. Reno, 929 F. Supp 824, 855-56 (E.D. Pa. 1996).

current method, YouTube cannot guarantee that no minors will view harmful content before it is removed. Presumably, those who run YouTube would be unwilling to face criminal liability for the chance viewing of an obscene video before their censors could intercept it, if they could help it. Is the best solution to allow YouTube to simply operate "untagged"? This would mean no criminal liability, but it would also mean that the entire site is completely inaccessible to children whose parents took advantage of the blocking capabilities. Although sites like YouTube should certainly be allowed to operate this way if they like, they should also be allowed to tag their videos separately, so that the innocent videos get through and the objectionable ones are blocked. Since PICS operates at the website level – that is, an entire page is tagged, there appears to be no room for the labeling of individual files that display on a web page. The files that are displayed on a web site, whether pictures, audio, or video, are called from the website through the use of tags that are part of the website. In order for PICS to be an effective tool for protecting children from harmful content without stifling free communication between adults, it should be modified, if possible, to allow the labeling of individual tags as child-safe or not child-safe. The filter on the browser should be able to filter on that level as well. In this way, PICS will remain an effective tool to protect children, without threatening the existence of these distinctive fora.

Limitations on a Browser-Centered Solution and the Operating System-Centered Response

Unfortunately, as elegant and effective a solution as mandating PICS appears to be, there is a rather large hole through which a child might gain access to harmful content. An interested child could simply download a new web browser whose PICS filters have not yet been activated, and use those browsers to get whatever content they like unimpeded. Or worse – as the first user of a newly installed browser, a child could set the PICS password, not only allowing the child access to any content, but preventing the parents from changing the settings. If PICS is the

internet analog to the V-chip, then this would be the analog of circumventing the V-chip by simply bringing home a new television set, except that, unlike bringing home a new television set, downloading a new browser is fast, easy, and free. The solution has to allow the parent to not just control how the internet-accessing software is to be used; it has to allow the parent to control what software is installed. In order to do this, the regulations have to go beyond the browser level to the operating system level. Operating systems (the most commonly used are the various versions of Windows and Macintosh OS X) should be required to have easy-to-use tools that block installation of new software without a password. Only the parent has the password, and so the parent can decide what new software is installed, and if the parent decides to install a new web browser, he or she can at that point set the PICS settings to the desired level.

Virtual Worlds

Another area of the internet that may not have been on the radar of the PICS group is what has come to be known as "virtual worlds." Virtual worlds are online environments in which many people can log on and interact with each other. Nowadays, many virtual worlds are grap PICS was focused on web content, but virtual worlds do not, for the most part, exist as part of the web. The earliest virtual worlds, text-only affairs known as "MUDs" and "MOOs," were accessed through Telnet clients. Their modern counterparts are fully animated graphical displays, which operate through clients specific to the virtual worlds. That is, World of Warcraft is accessed via the World of Warcraft software, Sims Online is accessed through the Sims Online software, Second Life is accessed through the Second Life software, etc. It is conceivable, perhaps, that Congress could require a PICS-like tagging system on all virtual world clients, such that players or participants with the blocking options activated would only see the "parts" of the virtual worlds that were age-appropriate, and not be able to see the "parts" of the virtual worlds

that had sexual or violent content, etc. It is also conceivable to require sellers of "girly" magazines to keep from minors those pages that contain nudity, or to require theaters showing pornographic movies to eject minors right before the graphic parts. As impractical as that sounds, it is an apt analogy to taking a virtual world and censoring certain parts of it. A virtual world is meant to be just that: a world, one continuous unbroken world in which users can "work," play, and otherwise interact.

A PICS-like solution to the problem of obscene content on virtual worlds is probably not practical. Instead, the solution must be, as described above, at the operating system level. If a parent is concerned with what her child is exposed to on the internet, the best tool she can have is the ability to block the installation of new software pending an investigation. If the virtual world in question is one in which the content is inoffensive, the parent can install the client (using her password to do so). If the virtual world is similar to Second Life, in which any member with the ability can produce any content he or she can imagine, including the obscene and the indecent, the parent may wish to block. If it is one in which the options for avatars[113] and items within the world are limited to a finite selection, and that selection excludes material the parents find objectionable, the parents may allow the installation of the client.

Conclusion

It is not disputed that Congress has a compelling interest in protecting children from sexual content, including that which is published on the internet. The first serious attempt to do so, the CDA, failed because it was vague and burdened speech that was protected between adults. The second attempt, the COPA, attempted to correct the failings of the CDA by defining the prohibited conduct more specifically, by trying to tailor that definition to the definition of obscenity, which lacks First Amendment protection, and by opening up less burdensome

[113] Graphic representations of users within virtual worlds.

affirmative defenses to providers of content. The COPA failed to pass constitutional muster as well, because it was still too burdensome on protected speech.

Filtering and blocking software was discussed in several of the opinions regarding the CDA and the COPA, as a less restrictive alternative to those statutes. Filtering and blocking programs provide a solution that does not impose a burden on providers of content, but their effectiveness is questionable, as they do not always block all objectionable content, and they can block content that is appropriate.

PICS, or a similar system, has the best potential as a tool parents can use to help control what kind of content their children are able to view, but that potential is going unrealized at present because web browsers are not equipped with the filtering capability and because content providers do not have an incentive to accurately tag their content. In order to protect children and give parents an effective tool without violating the First Amendment, I propose that Congress, in its next attempt to regulate the internet, mandate a PICS-type blocking technology on all web browsers and criminalize the publishing of non-child-safe content with a child-safe tag attached to it. In order to increase the effectiveness of such a law, and reduce the burden on protected speech, I further propose mandating a whitelist and blacklist function on web browsers, as well as a blacklist feature on operating systems.

It may be impossible to completely keep children from seeing the pornographic, the indecent, or even the obscene. As new media emerge, new opportunities arise with them. The unfortunate truth is probably that there is no way to completely prevent children from ever seeing an inappropriate image. A solution like PICS is at the same time probably the most effective tool parents have to protect their children, and the most constitutionally sound means to

achieve this compelling interest. The market has not brought PICS capability to web browsers, but the need for it exists, and Congress should act to require it.