

# ‘Scrubbing’ The Inbox: A Constitutional Alternative To Child Protection Registries

D. Logan Pool  
University of Georgia School of Law

---

## Table of Contents

	Page No.
I. Introduction.....	34
A. Current Legal Challenge to Child Protection Registry.....	36
B. A New Direction.....	37
II. Background	
A. Failed Federal Legislation.....	38
1. <i>Communications Decency Act (CDA): A First Failed Federal Attempt</i> .....	38
2. <i>Child Online Protection Act (COPA): A Second Failed Federal Attempt</i> .....	38
B. Strict Scrutiny Under First Amendment Jurisprudence.....	39
1. <i>Nature of Regulation: Content-Based or Content-Neutral Government</i>	
<i>Regulation</i> .....	39
2. <i>Nature of Speech: Non-Protected Obscene or Semi-Protected Indecent</i>	
<i>Speech</i> .....	40
3. <i>Nature of Medium: Medium-Specific Analysis</i> .....	44
C. Overbreadth: Channeling v. Total Ban.....	45
D. Hurdle of Strict Scrutiny.....	47
E. CAN-SPAM Act of 2003.....	49
F. Child Protection Registries.....	50
1. <i>Utah and Michigan Laws</i> .....	50
2. <i>FTC Concerns</i> .....	54
III. Discussion.....	55
A. Child Protection Registries’ Constitutional Problems.....	55
1. <i>Child Protection Registries Subject to Strict Scrutiny</i> .....	56
2. <i>Overbreadth: Inability to Channel Indecent but “Harmful” Communication</i> ..	56
3. <i>Compelling Interest in Protecting Minors</i> .....	58
4. <i>Several Less Restrictive Alternatives</i> .....	58
B. Improved Model Legislation: Child and Non-Consenting Adult Do-Not-Email	
Domain.....	60
1. <i>Do-Not-Email Domain</i> .....	60
2. <i>Constitutional Analysis</i> .....	62
3. <i>Practical Concerns</i> .....	63
4. <i>Limitations on Domain Solution: Don’t Trash the Filter</i> .....	65
IV. Conclusion.....	66

## **Abstract**

After the judicial demise of the Communications Decency Act and Child Online Protection Act and the continued impotency of CAN-SPAM to curb unsolicited commercial email, children remain vulnerable to harmful, indecent content via their inbox. In a recent attempt to curtail such exposure, several States have created Child Protection Registries. In essence, the laws allow children to register their email addresses with the state. The state laws impose significant criminal and civil penalties on senders of indecent material who send such emails to registered minors. Because the States retain the list of protected emails, senders of potentially indecent emails must, prior to sending emails, submit email addresses to the State and pay the State to remove protected emails listed with the state registry. Such registries, however, pose a myriad of constitutional and practical concerns. By compiling a list of minors' emails, the States may be undermining minors' safety while exposing them to increased spam by potentially providing pedophiles and spammers with a verified list of emails. Additionally, given the inability to discern geography from a normal email address, such registries will hinder email as an open, cost-effective means of communication by requiring all indecent emails to first be submitted to States with registries. In addition to these practical concerns, the Supreme Court will likely strike down such statutes on First Amendment grounds as overbroad and not narrowly tailored to protecting minors.

As a constitutional alternative to child protection registries, this article will propose the creation of a new email domain for minors and adults who do not wish to receive indecent material. The domain, such as @kids.ut.gov, would provide notice as to both geography and the recipient's status as a minor or non-consenting adult on the face of the email. Such a proposal by not creating an identifiable list of emails or limiting registration to only minors will address many of the practical concerns with current child protection registries. Also, by providing easy notice of recipients' status on the face of each email address, protected expression among adults will not be overburdened. By asking that emailers simply not send indecent material to the protected domains, such a system could survive strict scrutiny under the Supreme Court's First Amendment analysis.

## **‘SCRUBBING’ THE INBOX: A CONSTITUTIONAL ALTERNATIVE TO CHILD PROTECTION REGISTRIES.**

### **I. INTRODUCTION**

Unknown to both Justice Holmes and John Stuart Mill, the internet as an open medium of communication<sup>1</sup> seemingly provides an unparalleled platform for the flourishing marketplace of ideas. Such unrestricted free trade, however, increasingly exposes minors to harmful content.<sup>2</sup> The internet poses particular concern, because unlike traditional communication media, a network of logical space shields the speaker from his audience by clouding both his identity and geography.<sup>3</sup> Such anonymity hinders a speaker’s ability to channel his speech to appropriate audiences, leaving minors increasingly exposed to content protected among adults but potentially harmful to minors.<sup>4</sup> Attempting to remedy minors’ unbridled access to adult speech, Congress twice passed laws specifically designed to limit such exposure to the internet’s indecent or harmful content,<sup>5</sup> but twice the Supreme Court struck down such laws on First Amendment grounds.<sup>6</sup> Because of the First Amendment hurdle, children remain unprotected in the crossfire of harmful voices.

In light of Congress’s successive failures in shielding minors from harm, States have joined the effort to craft protective legislation that will survive constitutional scrutiny. Several states including Georgia,<sup>7</sup> Hawaii,<sup>8</sup> Illinois,<sup>9</sup> Michigan<sup>10</sup> and Utah<sup>11</sup> have considered a child

---

<sup>1</sup> See FED. TRADE COMM’N, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS, 3 (June 2004), <http://www.ftc.gov/reports/dneregistry/report.pdf> (explaining how internet and email function noting email system is “open, allowing information to travel freely with relative anonymity and ease”).

<sup>2</sup> Press Release, Symantec, Symantec Survey Reveals More than 80 Percent of Children Using Email Receive Inappropriate Spam Daily (June 9, 2003), <http://www.symantec.com/press/2003/n030609a.html> (citing a survey conducted for Symantec by Applied Research who interviewed 1,000 children between the ages of seven and eighteen).

<sup>3</sup> See FED. TRADE COMM’N, *supra* note 1, at 3 (explaining internet’s geographic and age anonymity).

<sup>4</sup> See *Ashcroft v. ACLU*, 535 U.S. 564, 582 (discussing speaker’s inability to control release of material on internet to geographical areas).

<sup>5</sup> See Communications Decency Act of 1996, 47 U.S.C. § 223(a)(1994); Child Online Protection Act, 47 U.S.C. § 231 (2007).

<sup>6</sup> See *Reno v. ACLU*, 521 U.S. 844, 885 (1997) (finding CDA overbroad in violation of First Amendment); *Ashcroft v. ACLU*, 542 U.S. 656, 673 (finding COPA not least restrictive alternative and in violation of First Amendment).

<sup>7</sup> See Georgia Child, Family, and School Protection Act, S.B. 425, 2005-2006 Gen. Assem., Reg. Sess. (Ga. 2006), available at [http://www.legis.state.ga.us/legis/2005\\_06/pdf/sb425.pdf](http://www.legis.state.ga.us/legis/2005_06/pdf/sb425.pdf); See also Press Release, Senate Information Office, Senate Passes Legislation Creating Child Protection Registry (Feb. 8, 2006), available at [www.legis.state.ga.us/legis/2005\\_06/senate/pressreleases/Senatepasses425.pdf](http://www.legis.state.ga.us/legis/2005_06/senate/pressreleases/Senatepasses425.pdf) (stating Senate Bill 425 creating Child Protection Registry passed by unanimous vote).

<sup>8</sup> See Letter from Fed. Trade Comm’n to Carol Fukunaga, Hawaii State Senator (March 31, 2006), available at

protection registry as a solution to the problem of geographical and age anonymity. In both Utah and Michigan Child Registry laws are currently in force.<sup>12</sup> Under these laws, children or their guardians register emails with the state registry.<sup>13</sup> The State then requires senders of harmful material to submit their email distribution lists<sup>14</sup> to an organization that removes, or ‘scrubs,’ all emails registered under the Child Protection Registry from the list.<sup>15</sup> Although senders must pay for this service, failure to submit a list to be scrubbed can result in substantial criminal and civil penalties if a harmful email reaches a minor’s inbox.<sup>16</sup> States believe these registries confront the problem of the internet’s anonymity by allowing the State to identify which email addresses are accessed by minors, and hence, which email addresses should be protected by state law from likely harmful, adult content.

Such registries, however, pose a host of legal and practical concerns. First, the statutes—like their federal predecessors—are likely to suffer from overbreadth because they regulate adult speech that is entitled to protection under the First Amendment.<sup>17</sup> Second, less restrictive legislative or technological schemes exist to protect minors.<sup>18</sup> The Court, however, is likely to apply strict scrutiny and require the government to rebut these other less restrictive alternatives.<sup>19</sup> Such rebuttal will likely prove difficult. The state laws are very burdensome to

---

<http://www.ftc.gov/os/2006/04/V060012FTCStaffCommentReHawaiiSenateBill2200.pdf> (advising Senator Fukunaga against Senate Bill 2200 creating Child Protection Registry).

<sup>9</sup> See Press Release, Fed. Trade Comm’n, For the Consumer: Announcement Actions for November 1, 2005 (Nov. 1, 2005), available at <http://www.ftc.gov/opa/2005/11/fyi0577.htm> (commenting on Illinois House Bill 0572 to create Child Protection Registry); Letter from Fed. Trade Comm’n to Angelo Saviano, Illinois State Representative (Oct. 25, 2005), available at <http://www.ftc.gov/os/2005/11/051101cmtbill0572.pdf> (advising Representative Saviano of Illinois against creating Child Protection Registry under Illinois HB 0572).

<sup>10</sup> See Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1065(5)(1) (2006) (creating Child Protection Registry)

<sup>11</sup> See Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006) (creating Child Protection Registry)

<sup>12</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1065(5)(1) (2006)

<sup>13</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1065(5)(1) (2006)

<sup>14</sup> An email distribution list, or an email mailing list, is a collection email addresses used by an individual or an organization to send email to multiple recipients on the list at once.

<sup>15</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1065(5)(1) (2006).

<sup>16</sup> See Child Protection Registry, UTAH CODE ANN. § 13-39-301 through 302 (2006) (providing both criminal and civil penalties for noncompliance); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS §§ 752.1067, 752.1068 (2006) (Michigan provides both civil and criminal penalties for noncompliance).

<sup>17</sup> See discussion *infra* Part II.A

<sup>18</sup> See discussion *infra* Part II.A

<sup>19</sup> See discussion *infra* Part II.A

certain senders—especially since the laws require senders to pay for such scrubbing.<sup>20</sup> This requirement places a practical, financial burden on a previously open and cost effective means of communication through email. Additionally, as discussed *infra*,<sup>21</sup> such registries will not likely protect children from the internet’s harmful content but may actually exacerbate the problem.<sup>22</sup> Thus, the registries place a heavy burden on certain emailers but do not substantially advance the State’s compelling interest of protecting children.

### A. CURRENT LEGAL CHALLENGE TO CHILD PROTECTION REGISTRIES

Although many organizations have expressed concern over the registries,<sup>23</sup> groups are reluctant to legally challenge the statutes designed to protect children because of the potential political consequences.<sup>24</sup> As the chief executive of email service provider Bigfoot Interactive, Al DiGuido explained, “Who wants to step up and say ‘We’re against a method or a means to protect children?’”<sup>25</sup> On the flip side, politicians have found an easy cause. For example, Utah House Speaker Greg Curtis praised the registry as a bi-partisan effort to protect children.<sup>26</sup> He went on to explain that “[p]ornography is affecting families in the most base way. It’s destroying children as well as adults.”<sup>27</sup>

Despite these deterrents, the Free Speech Coalition (FSC), a pornography industry trade organization, brought the first suit against the Utah registry, seeking to enjoin enforcement of the Child Protection Registry.<sup>28</sup> After filing the initial lawsuit, many other organizations filed amicus

---

<sup>20</sup> See Child Protection Registry, UTAH CODE ANN. § 13-39-301 (2006) (providing civil penalties for noncompliance); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS §§ 752.1067 (2006) (Michigan provides civil penalties for noncompliance).

<sup>21</sup> See discussion *infra* text accompanying notes 172-188.

<sup>22</sup> *Id.*

<sup>23</sup> Kortney Stringer, *E-Mail Law Upsets Parents*, DETROIT FREE PRESS, October 25, 2005 (quoting Dan Jaffe, vice president of government relations for Association of National Advertisers, criticizing child registry laws).

<sup>24</sup> Ken Magill, *Here Come the Registries*, DIRECT: PREMEDIA BUSINESS MAGAZINES & MEDIA INC., Sept. 1, 2005 (stating that most legal professionals believe registries could be successfully challenged, but “no one wants to make the first move.”); see also, Ken Magill, *Good News and Bad News (do-not-e-mail bill)*, DIRECT, Mar. 1, 2006 (stating Direct Marketing Association declined to challenge Utah’s registry laws to avoid bad press quoting association’s president as saying, “We knew if we did participate, it would get spun as ‘DMA attacks efforts to protect children...’ we believe such a perception would have been bad for our members.”).

<sup>25</sup> Magill, *supra* note 24, at 213.

<sup>26</sup> Ben Winslow, *Anti-Porn Registry is Defended*, DESERET MORNING NEWS, June 21, 2006, at B06 (quoting Greg Curtis)

<sup>27</sup> *Id.*

<sup>28</sup> <sup>28</sup> Complaint for Plaintiff, Free Speech Coalition, Inc. v. Shurtleff, No. 2:05-cv-00949, at 32 (C. D. Utah filed Nov. 17, 2005), available at <http://www.freespeechonline.org/webdocs/011706AmendedUtCPRComplaint.pdf>

briefs in support of the FSC.<sup>29</sup> Even though the FSC is incorporated in California, they argue because they cannot be certain a given email address is not associated with the Utah registry, they are forced to use Utah's scrubbing service even if they are not deliberately or knowingly having any contact with Utah or its minors.<sup>30</sup> Thus, the registry laws place a broad financial burden on the previously open marketplace of ideas.

As many predicted, the first lawsuit spawned parental ire and negative press.<sup>31</sup> Utah attorney General Mark Shurtleff cast FSC's lawsuit as a naked affront to children stating, "This lawsuit shows the pornographers true colors...by challenging our Child Protection Registry, they have proven their real intent to force smut on our children."<sup>32</sup> This public announcement, however, failed to address the legitimate concerns raised in the lawsuit.<sup>33</sup>

## B. A NEW DIRECTION

If children are truly to be protected, statutes first need to address the legitimate concerns raised by First Amendment jurisprudence. States will not succeed in protecting children by ignoring the constitutional errors of past legislation. Although Child Protection Registries implicate issues of preemption under CAN-SPAM and possible violations of the dormant commerce clause, this article will focus on what seems to be the first significant hurdle, the First Amendment. First, this article will discuss relevant First Amendment jurisprudence and detail the deficiencies of prior federal legislation. Second, against this background, this article will highlight current practical and constitutional deficiencies in child registries. Finally, a potentially constitutional solution will be proposed in which an opt-in email domain for minors and certain adults will be created. This domain will allow individuals to register a new email address under

---

<sup>29</sup> John Stith, *ESPC Goes After Utah's Child Protection Registry*, SECURITY PRO NEWS, Jan. 1, 2006, <http://www.securitypronews.com/news/securitynews/spn-45-20060125ESPCGoesAfterUtahsChildProtectionRegistry.html> (stating American Advertising Federation, American Association of Advertising Agencies, Email Sender and Provider Coalition, Association of National Advertisers, Electronic Frontier Foundation, and Center for Democracy and Technology all filing an application of amici curia against the Utah Child Protection Registry Act).

<sup>30</sup> Complaint for Plaintiff, Free Speech Coalition, Inc. v. Shurtleff, No. 2:05-cv-00949, at 13(C. D. Utah filed Nov. 17, 2005), available at <http://www.freespeechonline.org/webdocs/011706AmendedUtCPRComplaint.pdf>

<sup>31</sup> Wendy Leonard, *Marketers of Porn Fighting Web Law*, DESERETE MORNING NEWS, Nov. 18, 2005, at B02 (stating that marketers are attempting to market pornography to Utah residents regardless of age).

<sup>32</sup> News Release, *Attorney General Shurtleff Fights to Keep Kids Safe From Internet Porn*, US STATE NEWS, Dec. 7, 2005; see also, Ken Magill, Utah Fights Free Speech Coalition's Suit, DIRECT: PRIMEDIA BUSINESS MAGAZINES & MEDIA INC., Jan. 1, 2006 (quoting Mark Shurtleff)

<sup>33</sup> Magill, *supra* note 32. (stating "Shurtleff's statement didn't address the main arguments in the lawsuit" such as Utah's law being unduly burdensome on legitimate businesses, not likely to actually protect children, and preempted under federal law).

the domain such as username@kids.ut.gov. The domain will provide notice to legitimate marketers that the recipient is either a minor or an adult in Utah who wishes not to receive indecent material. Such a solution will hopefully shield children from harmful expression without overly restricting protected speech.

## II. BACKGROUND

### A. FAILED FEDERAL LEGISLATION

#### 1. *Communications Decency Act (CDA): A First Failed Federal Attempt*

Congress first attempted to protect children from online, indecent material through the Communications Decency Act of 1996 (CDA) by prohibiting the knowing transmission of obscene or *indecent* messages over the internet to a minor.<sup>34</sup> In *Reno v. ACLU* the Court applied strict scrutiny and struck down the CDA as overbroad and in violation of the First Amendment.<sup>35</sup> The Court reasoned that because of the CDA's content restrictions on protected, adult communication, its criminal nature, and the burdens imposed by the practical difficulties of age verification, the CDA was overbroad and in violation of the First Amendment.<sup>36</sup>

#### 2. *Child Online Protection Act (COPA): A Second Failed Federal Attempt*

In the wake of CDA's judicial demise, Congress enacted the Child Online Protection Act (COPA).<sup>37</sup> COPA imposes criminal penalties, fines, and six months in prison for knowingly posting onto a webpage, for a commercial purpose, material that is "harmful to minors."<sup>38</sup> Unlike the prior statute, COPA only applied to material displayed on webpages,<sup>39</sup> only covered commercial communications, and restricted the category of prohibited communications to

---

<sup>34</sup> 47 U.S.C. § 223(a)(1)(B)(ii) (1996) (criminalizing the "transmission of any...communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age").

<sup>35</sup> *Reno v. ACLU*, 521 U.S. 844 (1997).

<sup>36</sup> *See generally* *Reno v. ACLU*, 521 U.S. 844 (1997).

<sup>37</sup> *See* *Ashcroft v. ACLU*, 535 U.S. 564, 569 (2002) (stating Congress, in response to *Reno v. ACLU*, explored other avenues for restricting minors' access to pornographic material online, including the enactment of COPA).

<sup>38</sup> 47 U.S.C. § 231(a)(1) (2006). Harmful to minors is defined as: 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 pander to, the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.<sup>38</sup> 47 U.S.C. § 231(e)(6)

<sup>39</sup> The CDA applied to the internet generally, including emails, mail exploders, webpages, et cetera.

material “harmful to minors.”<sup>40</sup> Once again, the Court ultimately struck down CDA’s successor reasoning it likely violated the First Amendment.<sup>41</sup>

In 2001, organizations who posted, or had members who posted, sexually oriented material on the internet facially challenged COPA before the Court in *Ashcroft v. ACLU (Ashcroft I)*.<sup>42</sup> The group argued against COPA’s use of “community standards” to identify material that is “harmful to minors” as a violation of the First Amendment.<sup>43</sup> The Court, in a plurality opinion, upheld the use of community standards to define “harmful to minors” and remanded the case.<sup>44</sup> On remand, the Third Circuit once again affirmed the preliminary injunction, but found that COPA was overbroad and not narrowly tailored to serve a compelling governmental interest.<sup>45</sup> Hearing the case again after remand, the Court in *Ashcroft v. ACLU (Ashcroft II)* applied strict scrutiny and struck down COPA because there existed less restrictive technological alternatives such as filters.<sup>46</sup>

## **B. STRICT SCRUTINY UNDER FIRST AMENDMENT JURISPRUDENCE**

Attempts to protect children from explicit and harmful speech on the internet have faced significant First Amendment obstacles. In fact, some commentators have suggested that given the hurdles of current First Amendment law of overbreadth and strict scrutiny, a purely legislative solution to harmful internet speech may be impossible.<sup>47</sup> The level of scrutiny the Court applies depends on several factors such as a nature of the government regulation, the nature of speech involved, and the nature of the medium employed to distribute speech.

### *1. Nature of Regulation: Content-Based or Content-Neutral Government Regulation*

First, regarding the nature of the government regulation, the court applies two different standards depending on whether legislation engages in content-based or content-neutral

---

<sup>40</sup> *Ashcroft v. ACLU*, 535 U.S. 564, 569-70 (2002).

<sup>41</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 669 (2004) (finding the lower court did not abuse its discretion in granting preliminary injunction of the COPA).

<sup>42</sup> *See Ashcroft v. ACLU*, 535 U.S. 564, 571 (2002) (listing the numerous respondents who brought suit).

<sup>43</sup> *See id.* (recounting the elements of respondent’s complaint)

<sup>44</sup> *See id.* at 586 (remanding to Third Circuit).

<sup>45</sup> *See generally* *ACLU v. Ashcroft*, 322 F.3d 240, 266-67 (3d Cir. 2003).

<sup>46</sup> *See Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004) (finding government to failed its burden to show that COPA is less restrictive than filters).

<sup>47</sup> *See e.g.*, Tara Wheatland, *Ashcroft v. ACLU: In Search of Plausible, Less Restrictive Alternatives*, 20 BERKLEY TECH. L.J. 371 (2005) (concluding that current obscenity law as applied to internet may make it impossible for Congress to craft a constitutional statute).

discrimination.<sup>48</sup> Content-neutral restrictions “limit communication without regard to the message conveyed.”<sup>49</sup> Content-based restrictions, on the other hand, limit a certain viewpoint or subject matter.<sup>50</sup> Courts generally apply strict scrutiny to content-based restrictions on protected speech requiring the government to demonstrate that there exists a compelling state interest and that the legislation is the least restrictive means of achieving its stated goal.<sup>51</sup>

Attempts to protect children from the primary effects of harmful speech on the internet are content-based restrictions by attempting to restrict certain subject matter such as pornography, tobacco, or alcohol. In determining the level of scrutiny, the Court in *Reno v. ACLU* reasoned that the CDA is a content-based regulation of speech by seeking to protect children from the primary effect of indecent speech and hence subject to strict scrutiny.<sup>52</sup> Similarly in *Aschcroft II*, the Court found regulation of materials that were “harmful to minors” likewise to be a content-based regulation and subject to strict scrutiny. Thus, it seems that attempts to protect minors by regulating harmful content will likely be found to be a content-based restriction and subject to strict scrutiny.

## 2. Nature of Speech: Non-Protected Obscene or Semi-Protected Indecent Speech

Second, regarding the nature of speech involved, the Court recognizes a distinction between protected and unprotected (or less protected) speech.<sup>53</sup> In its First Amendment jurisprudence, the Court presumes the First Amendment protects all communication and then creates areas of non-protection only after affirmatively finding a given class of speech should not be entitled to protection.<sup>54</sup> For example, the Court has clearly established that obscene speech

---

<sup>48</sup> See Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 WM. & MARY L. REV. 189, 190 (1983).

<sup>49</sup> *Id.* at 189.

<sup>50</sup> See KATHLEEN M. SULLIVAN & GERALD GUNTHER, *Constitutional Law* 1193 (15 ed. 2004) (discussing content based restrictions); see e.g. *Police Dep’t v. Mosley*, 408 U.S. 92 (1972) (invalidating ordinance because it regulated permissible picketing in terms of its subject matter), *Burson v. Freeman*, 504 U.S. 191 (1992) (extending content-based regulation “not only to a restriction on a particular viewpoint, but also to a prohibition of public discussion on an entire topic”).

<sup>51</sup> Wheatland, *supra* note 47.

<sup>52</sup> See *Reno v. ACLU*, 521 U.S. 844, 868 (1997) (stating the CDA “applies broadly to the entire universe of cyberspace” and because it regulates “primary effects of indecent and patently offensive speech...the CDA is a content-based restriction and cannot be properly analyzed as a form of time, place, and manner regulation.”).

<sup>53</sup> KATHLEEN M. SULLIVAN & GERALD GUNTHER, *Constitutional Law* 1192 (15 ed. 2004)

<sup>54</sup> See Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 WM. & MARY L. REV. 189 (1983). Examples of speech classes that the Court has found to have low First Amendment protection include express incitement, false statements of fact, obscenity, commercial speech, fighting words, and child pornography. See *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (incitement), *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974) (false statements), *Miller v. California* 413 U.S. 15 (1973) (obscenity), *Virginia State Bd. Of Pharmacy v. Virginia*

lacks First Amendment protection.<sup>55</sup> Some speech, however, may be considered unprotected when encountered by children, but not obscene and protected when encountered by consenting adults.<sup>56</sup> Many of the First Amendment concerns in both federal and state legislation that are designed to protect children fall into this murky middle ground where the speech is entitled to protection as to adults, but not entitled to protection as to children.

The Burger Court established modern obscenity law in *Miller v. California*.<sup>57</sup> Against the background of the Warren Court's "tortured history" in attempting to define obscenity, the Burger Court sought to clearly set forth standards to be used to identify obscene material so that a State may confidently regulate without infringing on the First Amendment.<sup>58</sup> The guidelines, now referred to as the *Miller* test, require three prongs to be found by the trier of fact.<sup>59</sup> First, the trier of fact must determine "whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest,"<sup>60</sup> later referred to as the "prurient interest prong." Second, the trier of fact must also determine "whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law."<sup>61</sup> Third, the trier of fact must determine "whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value,"<sup>62</sup> later referred to as the "serious value prong."

The Rehnquist Court continued to apply the *Miller* standard to laws regulating internet speech, finding that failure to sufficiently mirror the *Miller* standards may result in a statute's

---

Citizens Consumer Council, 425 U.S. 748 (1976) (commercial speech), *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942) (fighting words), *New York v. Ferber*, 458 U.S. 747 (1982) (child pornography)

<sup>55</sup> See *Roth v. United States*, 354 U.S. 476 (1957); *Miller v. California*, 413 U.S. 15, 24 (stating "[t]his much has been categorically settled by the Court, that obscene material is unprotected by the First Amendment).

<sup>56</sup> See generally *Ginsberg v. New York*, 390 U.S. 629 (1968) (finding state law prohibiting sale of adult material that was deemed not obscene as to adults but obscene as to minors to not violate the First Amendment).

<sup>57</sup> See *Miller v. California*, 413 U.S. 15 (1973) (discussing Warren Court's "tortured history" in defining obscenity and establishing new test for obscenity); See also KATHLEEN M. SULLIVAN & GERALD GUNTHER, *Constitutional Law* 1095 (15 ed. 2004) (explaining Burger Court agreed to *Miller* test that continues to define unprotected obscenity today).

<sup>58</sup> *Miller v. California*, 413 U.S. 15, 19-20 (1973) (characterizing previous jurisprudence as "tortured" and stated "in this context we are called on to define the standards which must be used to identify obscene material that a State may regulate without infringing on the First Amendment as applicable to the States through the Fourteenth Amendment). Prior to *Miller* the Warren Court issued a series of plurality rulings and failed to obtain a majority in defining obscenity. See e.g. *Roth v. United States* 354 U.S. 476 (1957) (plurality holding as to three elements of obscenity), SULLIVAN & GUNTHER, *supra* note 57, at 1095.

<sup>59</sup> *Miller*, 413 U.S. 15, 24 (1973).

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

overbreadth. In *Reno v. ACLU*, the primary reason the Court found the CDA to be both overbroad and vague was the statute’s failure to sufficiently conform to the *Miller* standards of obscenity. First, the CDA refers to indecent *or* obscene messages, either of which is sufficient for liability. The Court reasoned that the CDA failed to define the word “indecent” or restrict it to obscene speech, and hence, such language is problematic because “sexual expression which is indecent but not obscene is protected by the First Amendment.”<sup>63</sup> Second, although the CDA had a requirement similar to *Miller*’s second prong, in that it prohibited patently offensive communication, the CDA failed to specify that the offensive conduct be defined by state law.<sup>64</sup> The Court reasoned that being defined by state law reduces the vagueness inherent in open-ended community standard restrictions.<sup>65</sup> Third, the CDA failed to include *Miller*’s final requirement that the communication lack any serious value.<sup>66</sup> The court further reasoned that the vagueness and deviation from the *Miller* standards is particularly troubling given that the statute’s criminal nature that may further hinder speech by causing speakers to remain silent.<sup>67</sup>

The *Miller* test for obscenity likely only defines obscenity as to adults, but indecent material “harmful to minors” may nevertheless be regulated.<sup>68</sup> In *Ginsberg v. New York*, the Court applied rationality review to uphold a state law prohibiting the sale of materials that were “harmful to minors.”<sup>69</sup> The statute defined “harmful to minors” as material that (1) “predominantly appeals to the prurient, shameful or morbid interest *of minors*,” (2) “is patently offensive to prevailing standards in the adult community as a whole without respect to what is suitable material *for minors*,” and (3) “is utterly without redeeming social importance *for minors*.”<sup>70</sup> Thus, *Ginsberg* modified the binding test for obscenity<sup>71</sup> to reference minors. The

---

<sup>63</sup> See *id.* at 875 (quoting previous case to emphasize that it is well established that indecent sexual expression is protected).

<sup>64</sup> See *id.* at 873 (stating that purportedly analogous requirement in the CDA lacks a critical requirement that the proscribed material be defined by applicable state law).

<sup>65</sup> See *id.* at 873 (stating requirement of proscribed material being defined by applicable state law reduces vagueness in the open-ended term “patently offensive” used in the CDA).

<sup>66</sup> See *id.* at 865 (stating that “patently offensive material” omits any requirement that it lack serious literary, artistic, political, or scientific value.).

<sup>67</sup> See *id.* at 872 (stating the opprobrium and stigma of a criminal conviction as opposed to civil regulation may cause speakers to remain silent rather than communicate arguably unlawful words, ideas, and images).

<sup>68</sup> In *Ginsburg v. New York*, the Court was applying the precursor of the *Miller* standard that was similar to the *Miller* standard but less demanding. In addition, *Miller* reaffirmed *Ginsburg* when it cited *Ginsburg* for the proposition that “States have a legitimate interest in prohibiting dissemination or exhibition of obscene material when the mode of dissemination carries with it a significant danger of offending the sensibilities of unwilling recipients or of exposure to juveniles.” *Miller v. California*, 413 U.S. 15, 18-19 (1973).

<sup>69</sup> See *Ginsberg v. New York*, 390 U.S. 629, 634 (1968).

<sup>70</sup> See *Ginsberg v. New York*, 390 U.S. 629, 632-33 (1968) (emphasis added).

Court noted the law applied only to minors in that it did not restrict sale to persons seventeen years or older<sup>72</sup> and did not prevent parents from buying such material for their children.<sup>73</sup> The court stated that “material which is protected for distribution to adults is not necessarily protected from restriction upon its dissemination to children.”<sup>74</sup> The state has an interest to protect the welfare of children and see they are safeguarded from abuses.<sup>75</sup> Because the state may rationally believe such material is harmful to minors, the statute prohibiting distribution of such materials to minors is rationally related to the objective of safeguarding such minors from harm.<sup>76</sup> Later the Court recognized that the state has a “compelling interest” in protecting the well being of a minor.<sup>77</sup>

In *Ashcroft I*, Justice Thomas reasoned that the COPA’s use of “harmful to minors” was an improvement over the CDA because it was crafted to parallel the *Miller* definition of obscenity.<sup>78</sup> The plurality implied that strict compliance with the *Miller* standard would not always be required, because the plurality did not insist complete parallel with *Miller* but only required that the statute be narrowed by a “serious value” and a “community standards” prong.<sup>79</sup> The plurality did not rule on whether COPA was unconstitutionally vague or overbroad but remanded the case with the finding that COPA’s reliance on community standards to identify material that is “harmful to minors” does not render the statute substantially overbroad under the First Amendment.<sup>80</sup> By not requiring strict compliance with the *Miller* standards, the plurality implicitly approved of the “harmful to minors” standard similar to the standard upheld in *Ginsberg* to define material obscene as to minors and subject to limited government regulation .

---

<sup>71</sup> *Ginsberg v. New York* was decided prior to *Miller* and applied *Miller*’s predecessor *Memoirs v. Massachusetts*. See *Memoirs*, 383 U.S. 413 (1966) (Justice Warren, Fortas, and Brennan adopting interpretation of *Roth v. United States*, 354 U.S. 476, creating a three part test) (plurality opinion). The *Miller* obscenity test’s third prong differs from the *Memoirs*’ third prong by requiring material to have no ‘serious value’ instead of requiring the material be “utterly without redeeming social value.” Compare *Miller v. California*, 413 U.S. 15, 24 with *Memoirs v. Massachusetts*, 383 U.S. 413, 418 (1966).

<sup>72</sup> See *Ginsberg v. New York*, 390 U.S. 629, 634 (1968).

<sup>73</sup> *Id.* at 639.

<sup>74</sup> *Id.* at 635.

<sup>75</sup> *Id.* at 640.

<sup>76</sup> *Id.* at 643.

<sup>77</sup> See *New York v. Ferber*, 458 U.S. 747, 756-57 (1982) (stating “[i]t is evident beyond the need for elaboration that a State’s interest in ‘safeguarding the physical and psychological well-being of a minor’ is ‘compelling’”).

<sup>78</sup> See *Ashcroft v. ACLU*, 535 U.S. 564, 578 (2002) (comparing the CDA to COPA).

<sup>79</sup> See *id.* at 580 (plurality stating “[w]hen the scope of an obscenity statute’s coverage is sufficiently narrowed by a ‘serious value’ prong and a ‘prurient interest’ prong,’ we have held that requiring a speaker disseminating material to a national audience to observe varying community standards does not violate the First Amendment”).

<sup>80</sup> *Id.* at 586.

### 3. Nature of Medium: Medium-Specific Analysis

Third, regarding the nature of medium involved, the Court recognizes that each medium has varying characteristics that justify differences in the level of scrutiny to be applied.<sup>81</sup> In *Pacifica*, the Court justified a reduced level of scrutiny under the First Amendment due to the peculiar characteristics of radio and television broadcasting.<sup>82</sup> First, the scarcity of the broadcast spectrum in both television and radio requires that this resource be utilized in a way that furthers public interest.<sup>83</sup> Second, broadcasting has a pervasive nature in that it invades the home and subjects people to a constant risk of exposure to offensive material.<sup>84</sup> Third, and most importantly, both radio and television are easily accessible to children.<sup>85</sup> As compared with other medium such as print and motion pictures, broadcasting is immediately accessible to children and the government's interest in protection of minors and parents' interest in having a claim of authority in their household justify special treatment of indecent broadcasting. Recognizing that the speech used in the radio broadcast was not obscene<sup>86</sup> and would be protected in another medium, the Court nevertheless ruled that the regulation in question was permissible as to broadcast media due to the above listed characteristics.<sup>87</sup>

Other mediums, in contrast, have not received lower scrutiny by the Court, primarily because more controls may be exercised in those mediums to shield minors' access. In *United States v. Playboy Entertainment Group*, the Court justified striking down restrictions on cable television that might be unacceptable in broadcasting media, because of the characteristic of cable television that allowed providers to block, scramble, or limit specific programs or stations.<sup>88</sup> Similarly, in *Sable Communications v. California*, the court applied strict scrutiny and

---

<sup>81</sup> See *Fed. Comm'n Comm'n v. Pacifica*, 438 U.S. 726, 748 (1978) (stating each medium of speech "tends to present its own peculiar problems").

<sup>82</sup> *Id.* at 748-50.

<sup>83</sup> *Id.* at 748.

<sup>84</sup> *Id.* at 749-50.

<sup>85</sup> *Id.*

<sup>86</sup> See *id.* at 756-57 (stating "the monologue at issue here is not obscene in the constitutional sense" and "some words used have been held protected by the First Amendment in other cases and contexts").

<sup>87</sup> *Id.* at 762 (finding that "[t]he result turns instead on the unique characteristics of the broadcast media, combined with society's right to protect its children from speech generally agreed to be inappropriate for their years, and with the interest of unwilling adults in not being assaulted by such offensive speech in their homes").

<sup>88</sup> *United States v. Playboy Entertainment Group*, 529 U.S. 803, 815 (2000) (distinguishing *Pacifica* as broadcasting that required special treatment because of peculiarities of its medium).

struck down a statute prohibiting indecent telephone messages.<sup>89</sup> The court held that the total prohibition of indecent telephone messages violates the First Amendment because it exceeds the government's "compelling interest" in limiting minors' access to such messages because the nature of telephone communication, as distinguished from broadcasting, requires affirmative steps to receive the communication<sup>90</sup> and there is likely a less restrictive, constitutional means to protect minors from receiving indecent telephone communications by requiring credit cards to receive indecent messages.<sup>91</sup>

In *Reno v. ACLU*, true to the medium-specific First Amendment analysis, the Court distinguished the internet from other media and found content regulations of the internet to be subject to strict scrutiny.<sup>92</sup> Unlike broadcasting, the internet has no history of extensive governmental regulation, no scarcity of available frequencies or resources, and was not considered as invasive as television or radio.<sup>93</sup> Thus, unlike broadcasting, the internet should not be subject to a lower level of scrutiny for a content-based restriction.

### C. OVERBREADTH: CHANNELING V. TOTAL BAN

The Court in *Reno v. ACLU*, implicitly noted that attempts to regulate the internet would likely be an overbroad, total ban on certain communications, because of the user's inability to channel internet communications to certain audiences. In particular, the Court voiced concerns about the practical, economic limitations for determining age and geographical location on the internet.<sup>94</sup> The Court reasoned that such practical limitations will inevitably inhibit adult, internet communication.<sup>95</sup> The Court accepted the lower court's findings of fact that there "is no effective

---

<sup>89</sup> See generally *Sable Communications v. FCC*, 492 U.S. 115 (1989).

<sup>90</sup> See *Sable Communications v. FCC*, 492 U.S. 115, 128 (1989) (distinguishing *Pacifica* as not involving a "captive audience problem" because of affirmative steps required to accept telephone communication).

<sup>91</sup> *Id.*

<sup>92</sup> Although the Court never explicitly used the word "strict scrutiny," it apparently applied a standard essentially indistinguishable from strict scrutiny. Other commentators also believe the court was applying strict scrutiny. See e.g. Debra M. Keiser, *Regulating the Internet: A Critique of Reno v. ACLU*, 62 ALB. L. REV. 769, 780-81 (1998) (stating "the Supreme Court assigned the Internet the highest level of First Amendment protection and subjected the CDA to strict scrutiny review"); Kelly M. Doherty, *www.obscurity.com: An Analysis of Obscenity and Indecency Regulation on the Internet*, 32 AKRON L. REV. 259, 276 (1999) (stating "the Internet was subject to strict scrutiny"). Cf. Tara Wheatland, *Ashcroft v. ACLU: In Search of Plausible, Less Restrictive Alternatives*, 20 BERKLEY TECH. L.J. 371, 375 (2005) (finding Court applied "a high level of scrutiny").

<sup>93</sup> See *Reno v. ACLU*, 521 U.S. 844, 869-70 (1997) (distinguishing *Pacifica* and *Sable*).

<sup>94</sup> See *id.* at 877 (evaluating practical matters of expense for speakers who have websites to verify their users are adults).

<sup>95</sup> See *id.* at 877 (stating prohibitive expense for speakers will curtail a significant amount of adult expression on the internet).

way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms.”<sup>96</sup> Although the Court noted surrogates for age verification were possible through credit cards or adult passwords, the Court accepted the lower court’s finding that the “cost of creating and maintaining such screening systems would be beyond their reach.”<sup>97</sup> Justice O’Connor agreed and explained that outside the internet in physical reality, “the twin characteristics of geography and identity enable the establishment’s proprietor to prevent children from entering the establishment, but let adults inside.”<sup>98</sup> In cyberspace, however, speakers and listeners may mask their identity, and hence it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.<sup>99</sup> Thus the Court concluded it would be “prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults.”<sup>100</sup>

Contrastingly, in *Aschcroft I*, Justice Thomas did not find the inability to target geography on the internet to be a burden relevant to First Amendment analysis.<sup>101</sup> Instead, he placed the burden on the publisher to use another medium that more narrowly targeted the intended audience.<sup>102</sup> After *Aschcroft I*, however, the issue remains unclear because Justices O’Connor and Kennedy in separate concurrences expressly disagreed with the plurality’s conclusion regarding geography and believed such geographical difficulties to be relevant in First Amendment analysis. Both found that given the speaker’s inability to control the geographic location of their audience, placing such a burden on the speaker would suppress a large amount of protected speech and likely undermine the internet as a means of communication.<sup>103</sup> Thus, it remains unclear whether given the speaker’s inability to target certain audiences on the internet, the speaker may nevertheless be given this burden.

---

<sup>96</sup> *Id.* at 855.

<sup>97</sup> *Id.* at 857.

<sup>98</sup> *Id.* at 889.

<sup>99</sup> *Reno v. ACLU*, 521 U.S. 844, 890 (1997).

<sup>100</sup> *Id.* at 877.

<sup>101</sup> *See Aschcroft v. ACLU*, 535 U.S. 564, 582 (2002). (Thomas reasoned that in no prior case was the “speaker’s ability to target the release of material into particular geographic areas integral to the legal analysis.”)

<sup>102</sup> *Id.* (stating that “[i]f a publisher wishes for its material to be judged only by the standards of particular communities, then it need only take the simple step of utilizing a medium that enables it to target the release of its material into those communities”).

<sup>103</sup> *Reno v. ACLU*, 521 U.S. 844, 587 (1997) (O’Connor reasoned that “given internet speakers’ inability to control the geographic location of their audience, expecting them to bear the burden of controlling the recipients of their speech...may be entirely too much to ask, and would potentially suppress an inordinate amount of expression”)(O’Connor, J., concurring).

#### D. HURDLE OF STRICT SCRUTINY

Under strict scrutiny, governmental regulations are only permissible if: (1) the government demonstrates that the regulation is in furtherance of a compelling state interest, and (2) the government demonstrates that the chosen method is narrowly tailored and is the least restrictive means of achieving its stated goal.<sup>104</sup> The first hurdle of strict scrutiny is easily met. In both *Reno v. ACLU* and *Ashcroft II*, the Court recognized that the government has a compelling interest in protecting children.<sup>105</sup> The second requirement of being narrowly tailored and the least restrictive alternative, however, poses a greater hurdle.

In *Reno v. ACLU*, although the Court recognized the government's compelling interest in protecting children, the Court reasoned that such an interest does not justify a broad suppression of speech by stating that “[r]egardless of the strength of the government's interest in protecting children, the level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox.”<sup>106</sup> Given the size of the audience reached on the internet, mere knowledge that some minors may actually view the material should not interfere with adult communication.<sup>107</sup> Similarly, in *Ashcroft II*, although the government had a compelling interest in protecting children, Justice Kennedy, writing for the majority, struck down the statute because less restrictive means of protecting children from accessing harmful material are available through the use of filtering software.<sup>108</sup>

The *Ashcroft II* Court found COPA was not the least restrictive alternative, because on the receiving end, users could employ blocking and filtering software to impose selective restrictions on the content they can view.<sup>109</sup> COPA on the contrary imposed “universal restrictions at the source.”<sup>110</sup> Promoting filters would not criminalize protected speech, would allow adults to gain access to protected speech, and would hinder minors' access to such content.<sup>111</sup> Thus, filters would prohibit less constitutionally protected speech.<sup>112</sup>

---

<sup>104</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 666 (2004).

<sup>105</sup> *Id.* at 875.

<sup>106</sup> *Id.*

<sup>107</sup> *See id.* at 876 (speaking hypothetically Court opined, “Knowledge that, for instance, one or more members of a 100-person chat group will be a minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults.”).

<sup>108</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004).

<sup>109</sup> *Id.* at 667.

<sup>110</sup> *Id.*

<sup>111</sup> *See id.* at 667 (reasoning filtering software is less restrictive but more effective than COPA).

<sup>112</sup> *Id.*

Filters would also be more effective in achieving the government's goal of protecting children than COPA.<sup>113</sup> First, whereas COPA's restrictions only apply to domestic pornography, filters can be applied to all pornography.<sup>114</sup> Second, whereas COPA only applies to webpages, filters may be "more effective because they can be applied to all forms of Internet communication, including e-mail, not just communications available via the World Wide Web."<sup>115</sup> Although the Court recognized such filtering software currently has flaws, the Court found that the government failed in its burden to show the filters were less effective than COPA.<sup>116</sup>

In sum, where speech is not obscene, but merely indecent it receives protection. Additionally, restrictions on indecent, non-obscene speech are subject to strict scrutiny where the statute provides for a content-based restriction unless the speech is delivered in a medium that requires a lower level of scrutiny such as broadcasting. The state has a compelling interest in protecting its minors, but such a compelling interest will not be justified unless the statute is the least restrictive alternative and narrowly tailored.

Because the internet does not receive lower level of scrutiny, to the extent a statute restricts the source and content of internet communication, it should limit its scope to obscene conduct or conduct that is "harmful to minors."<sup>117</sup> A "harmful to minors" standard is not overbroad on its face because it is limited by both a community standards prong and a serious value prong. Where the "harmful to minors" standard is used to regulate the internet, however, the Court will still apply strict scrutiny and require that the statute be the least restrictive alternative in light of both legislative tailoring to Miller standards and technological developments such as filtering. However, there has been no clear holding as to the weight the internet's geographical difficulties play in the First Amendment analysis.<sup>118</sup> Thus, uncertainty remains as to whether geographical determinations may be taken into account in determining burdens on free speech.

---

<sup>113</sup> *See id.* at 668 (stating "filters also may be more effective" than COPA).

<sup>114</sup> *Id.*

<sup>115</sup> *Id.*

<sup>116</sup> *See id.* at 669 (finding the government failed in its burden to prove that COPA was less restrictive than filters and hence, affirming the district court's preliminary injunction against COPA).

<sup>117</sup> *Id.* at 580.

<sup>118</sup> *Compare* Ashcroft v. ACLU, 535 U.S. 564, 583, 587, 597 (2002). (2002) (O'Connor, J., Concurring) (plurality rejecting geography limitations as an important factor) *with* Ashcroft v. ACLU, 535 U.S. 564, 587, 597 (2002) (both concurrences reasoning geography limitations carry great weight).

## E. CAN-SPAM ACT OF 2003

After the CDA and COPA have been enjoined, the federal legislation that remains protects children's privacy rights (COPPA)<sup>119</sup> and provides children a website safe haven (kids.us).<sup>120</sup> However, children are still at risk to encounter harmful content via their own email accounts. Although Congress passed the CAN-SPAM Act,<sup>121</sup> such legislation only bans false or misleading header information, prohibits deceptive subject lines, requires an opt-out for end users,<sup>122</sup> and necessitates warning labels in the subject header for email with sexually oriented content.<sup>123</sup> The act does not expressly protect children from viewing harmful material, but is aimed primarily at preventing misleading practices in general. Thus, advertisements for herbal supplements, male enhancements, and pornography may still lawfully and indiscriminately fill inboxes daily.<sup>124</sup> Unfortunately, many of these recipients are children. Almost fifty percent of children receive emails with links to adult websites on a daily basis.<sup>125</sup> Anticipating this problem, the CAN-SPAM Act called upon the Federal Trade Commission (FTC) to establish a plan and timeline for establishing a "National Do Not Email Registry" (similar to the National Do-Not-Call List).<sup>126</sup>

After considering several models for a National Do Not Email Registry,<sup>127</sup> however, the commission concluded that because of the inability to authenticate the origin of email messages, such a registry would fail to reduce the amount of spam and may actually increase the volume of

---

<sup>119</sup> The regulations require institutions that collect a child's information to disclose information collection practices on website or by written notice, obtain parental consent, provide parents with means to have child's personal information deleted, and establish procedures to protect the confidentiality, security, and integrity of the personal information collected from children. Children's Online Protection Rule, 16 C.F.R. § 312.4-8 (2006).

<sup>120</sup> See *infra* text accompanying note 225.

<sup>121</sup> CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (stating Act's purpose is to regulate transmission of unsolicited commercial email).

<sup>122</sup> *Id.*

<sup>123</sup> S. Jenell Trigg, *The CAN-SPAM Act and Other Restrictions on Commercial E-mail*, 23 COMM. LAW. 14, 14 (2006).

<sup>124</sup> FED. TRADE COMM'N, FALSE CLAIMS IN SPAM: A REPORT BY THE FTC'S DIVISION OF MARKETING PRACTICES, 2 (Apr. 30, 2003), <http://www.ftc.gov/reports/spam/030429spamreport.pdf> (reporting almost twenty percent of spam to offer adult content). Peter B. Maggs, *Abusive Advertising on the Internet (SPAM) Under United States Law*, 54 AM J. COMP. L. 385, 385 (2006) (concluding CAN-SPAM "has been a total failure" citing studies that found an increase in spam and a lack of conformity with CAN-SPAM's requirements).

<sup>125</sup> Press Release, Symantec, Symantec Survey Reveals More than 80 Percent of Children Using Email Receive Inappropriate Spam Daily (June 9, 2003), <http://www.symantec.com/press/2003/n030609a.html> (citing a survey conducted for Symantec by Applied Research who interviewed 1,000 children between the ages of seven and eighteen).

<sup>126</sup> SPAM Act of 2003, 15 U.S.C. § 7708 (2006).

<sup>127</sup> FED. TRADE COMM'N, *supra* note 1, at 13-15 (considering several models for a Do Not Email Registry including the registry of individual emails addresses, registry of domains, and registry of individual email addresses with a third-party forwarding service).

spam received by consumers.<sup>128</sup> Spam may increase with a Do Not Email Registry, because spammers may use a registry as a mechanism for verifying active email addresses.<sup>129</sup> This problem would not be solved by contemporary security techniques such as centralized scrubbing and encryption.<sup>130</sup> To have email lists scrubbed, marketers would submit their distribution lists to a contractor who would return a list purged of all registered email addresses.<sup>131</sup> While a centralized scrubbing system might prevent spammers from accessing the entire registry, they could still utilize the registry to verify current email addresses by comparing their original list to the scrubbed list.<sup>132</sup> Through numerous list submissions, spammers could reconstruct a large subset of the registry.<sup>133</sup> This threat would not be hampered by encrypting the registry, because the spammer would still have access to both the original list and the scrubbed list so active email addresses could be inferred. Thus, past legislation has proved powerless in protecting children from a barrage of harmful emails.

## F. CHILD PROTECTION REGISTRY

### 1. *Utah and Michigan Laws*

Michael Prince and Patrick Shea argue for a model—similar to the model rejected on a national level by the FTC—that they contend will keep states relevant in the fight against SPAM.<sup>134</sup> They propose that parents can list their child’s contact points—including email, cell phones, and instant message identities—on a centralized Child Protection Registry, providing notice to spammers of the recipient’s protected minor status.<sup>135</sup> By continuing to send inappropriate email to registered contact points, the spammer will face substantial liability.<sup>136</sup> The model legislation focuses on material and services not appropriate for minors and would require spammers of such material to check (or “scrub”) their lists against the Child Protection

---

<sup>128</sup> *Id.* at i.

<sup>129</sup> FED. TRADE COMM’N, *supra* note 1, at 17-18.

<sup>130</sup> FED. TRADE COMM’N, *supra* note 1, at 18-19

<sup>131</sup> FED. TRADE COMM’N, *supra* note 1, at 19.

<sup>132</sup> *Id.*

<sup>133</sup> *Id.*

<sup>134</sup> Matthew B. Prince & Patrick A. Shea, *After CAN-SPAM, How States can stay Relevant in the Fight Against Unwanted Messages: How a Children’s Protection Registry Can be Effective, and is not Preempted, Under the New Federal Anti-Spam Law*, 22 J. MARSHALL J. COMPUTER & INFO. L., 29, 53 (2003) (stating “if states wish to remain relevant in the fight against unwanted electronic messages” they should create a Child Protection Registry).

<sup>135</sup> Prince, *supra* note 134, at 53 (stating parents should list their child’s email on contact list that provides spammers with notice of child’s minority status).

<sup>136</sup> *Id.* (stating if spammers continue to send spam to a registered address, they will face substantial liability).

Registry before sending their messages.<sup>137</sup> Unlike prior email legislation, however, the model statute would apply to all contact points of minors including email, instant messages, mobile phones, et cetera.<sup>138</sup>

Prince believes such a scheme would not only protect children but would effectively eliminate the practice of indiscriminately sending spam, because “[i]f children’s electronic email addresses are effectively designated legal landmines for spammers, then the net protection afforded by the registry could be broader than it originally appears.”<sup>139</sup> Thus, by creating a Child Protection Registry, States could satisfy their dual aims of protecting children and reducing indiscriminate email in general.

Prodded by the lobbying of UnSpam Technologies, Inc. (UnSpam) both Utah and Michigan granted UnSpam contracts to run two Child Protection Registries<sup>140</sup> very similar to the one proposed by Michael Prince, Unspam’s president.<sup>141</sup> Both registries are now currently active,<sup>142</sup> and in both Utah and Michigan, minors may now register their “contact points” such as email addresses, instant message identities, and telephone numbers with the registry.<sup>143</sup> Additionally, schools that primarily serve minors may register entire domains.<sup>144</sup> Michigan Governor Jennifer M. Granholm lauded the registry saying “Michigan’s child protection registry is a great way parents can shield their children from inappropriate email.”<sup>145</sup>

Both laws provide that a marketer may not send prohibited communications to contact

---

<sup>137</sup> *Id.* at 56

<sup>138</sup> *Id.*

<sup>139</sup> *Id.*

<sup>140</sup> Trigg, *supra* note 123, 20. *See also*, Peter Nagy, *Measure to Expand Child-Data Registry*, DESERET MORNING NEWS, Feb. 11, 2006 (reporting on lobbyist Craig Peterson easing representatives’ fears that the registry may not adequately secure minor’s contact points); Ken Magill, *Michigan Casts Wide Do-Not-E-mail Net*, DIRECT, Oct. 1, 2006, at Vol. 18, Issue 11 (stating Unspam has been lobbying to have registry laws enacted in several states).

<sup>141</sup> Michigan’s Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1061 (stating the “intent of this act is to provide safeguards to prevent certain messages regarding tobacco, alcohol, pornography, gambling, illegal drugs, and other illegal products from reaching the minor children of this state.”)

<sup>142</sup> *See* <https://www.protectmichild.com/> (Michigan’s Registry), <https://www.utahkidsregistry.com/> (Utah’s Registry).

<sup>143</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-102 (2006). Although both laws provide that only contact points accessible by minors may be registered, the registries only require visitors to affirm they are residents by checking a box and entering a postal code and to affirm a minor has access to the address registered. Additionally, schools that primarily serve minors may register entire domains. *See* Utah Kids Registry, <https://www.utahkidsregistry.com/> (allowing registration to all visitors who affirm they are Utah residents, affirm minors have access to the registry, and provide a Utah postal code).

<sup>144</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-201(3)(c) (2006).

<sup>145</sup> News Release, Michigan Launches Registry to Protection Children from Inappropriate Email (July 1, 2005), <http://www.govtech.net/news/news.php?id=94504> (Last accessed August 30, 2006).

points that have been registered for thirty days.<sup>146</sup> In effect, marketers must scrub their email distribution list once a month against both the Utah and Michigan registry to be compliant,<sup>147</sup> and are charged a half cent per email address scrubbed in Utah<sup>148</sup> and \$.007 per email scrubbed in Michigan.<sup>149</sup> Such charges are significant, costing marketers with a list of 1 million, \$60,000 per year in Utah alone.<sup>150</sup>

In Utah, the law prohibits communications with the primary purpose of advertising a product or service that a “minor is prohibited by [Utah] law from purchasing” or is “harmful to minors.”<sup>151</sup> “Harmful to minors” is statutorily defined under a three-prong test that mirrors the *Miller* test.<sup>152</sup> Although not technically a legal opinion, the Division of Consumer Protection further clarified “harmful to minors” to include “an alcoholic beverage or product, any form of tobacco, pornographic materials, and any product or service that is illegal in Utah.”<sup>153</sup> Michigan’s statute provides a more extensive and specific list stating harmful items include but

---

<sup>146</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1065(5)(1) (2006) (a marketer may not send a message to a contact point that has been registered for more than thirty calendar days if the primary purpose of the message is to advertise a product or service that a minor is prohibited by law from purchasing, viewing, possessing, participating in, or otherwise receiving)

<sup>147</sup> Gregory M. Saylin & Leanne N. Webster, *Utah’s Newest Anti-Spam Law: The Child Protection Registry*, 18 UTAH B.J. 33, 33 (2005); Utah Kids Registry, <https://www.utahkidsregistry.com/senders/> (stating “Senders of adult-oriented messages should scrub their lists at least every 30 days in order to comply with the law.”); *See also*, Institute for Spam and Internet Public Policy (ISIPP), New July 1<sup>st</sup> Child Email Address Registry Laws a Big Surprise Affecting All Emailers, warns Institute for Spam and Internet Public Policy (June 27, 2005) <http://www.isipp.com/news-mich-and-utah-laws.php> (stating “In order to ensure that they don’t send unpermitted material to any email address on the registry, email senders are required to match their mailing lists against the registries on a monthly basis...”); Direct Marketing Association, Summary of Michigan and Utah Protection Registry Statutes (July 1, 2005), <http://www.the-dma.org/cgi/dispnewsstand?article=3888> (stating “to avoid liability, monthly verification of contact points is necessary...”).

<sup>148</sup> Utah Kids Registry, <https://www.utahkidsregistry.com/senders/answer.html?src=q&id=359> (explaining the cost of scrubbing by stating “To calculate your scrub cost, multiply the number of addresses that you check by the fee, regardless of scrub type. For example, if you scrubbed a 1,000 address list against the Utah registry, you would calculate your cost as follows: 1,000 X \$0.005 = \$5.00 total cost.”).

<sup>149</sup> Protect MI Child (Michigan’s Child Protection Registry Website), <https://www.protectmichild.com/senders/answer.html?src=q&id=159> (stating “The fee for Michigan is currently set at seven tenths of a cent, \$0.007.”)

<sup>150</sup> Ken Magill, *Here Come the Registries*, DIRECT: PRIMEDIA BUSINESS MAGAZINES & MEDIA INC., Sept. 1, 2005, at 212.

<sup>151</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-202(1) (2006)

<sup>152</sup> “‘Harmful to minors’” means that quality of any description or representation, in whatsoever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when it: (a) taken as a whole, appeals to the prurient interest in sex of minors; (b) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and (c) taken as a whole, does not have serious value for minors. Serious value includes only serious literary, artistic, political or scientific value for minors.”, UTAH CODE ANN. § 76-10-1201 (4) (2006).

<sup>153</sup> Francine A. Giani, Utah Division of Consumer Protection, Policy Statement Concerning UTAH CODE. ANN. § 13-29-202(1) (July 8, 2005), <http://dcp.utah.gov/PolicyStatement.pdf>

are not limited to alcohol,<sup>154</sup> tobacco,<sup>155</sup> pornography and obscene material,<sup>156</sup> gambling,<sup>157</sup> lotteries,<sup>158</sup> illegal drugs,<sup>159</sup> and firearms.<sup>160</sup>

Both the Utah and Michigan statutes impose strict liability with criminal and civil penalties,<sup>161</sup> and unlike the CAN-SPAM Act, provide minors and guardians standing to sue.<sup>162</sup> The civil penalties in Utah for sending an email to registered contact points are substantial: one thousand dollars for each communication sent.<sup>163</sup> The civil penalties in Michigan are similarly severe holding marketers liable for the lesser of five thousand dollars per message to registered contact point or two-hundred fifty thousand dollars per day that the violation occurs.<sup>164</sup> In Utah, a person who sends a prohibited email to a contact point is subject to a class B misdemeanor for the first offense<sup>165</sup> and a class A misdemeanor for each subsequent violation.<sup>166</sup> A marketer is subject to a second degree felony, if he uses the information from the registry to send a solicitation via a third party or himself.<sup>167</sup> In Michigan sending prohibited communications to a registered contact point is considered a “computer crime”<sup>168</sup> and subject to felony charges and two years in jail.<sup>169</sup>

In a suit against a marketer, consent of the minor is no defense,<sup>170</sup> and the only defense statutorily available is that the marketer reasonably relied on the Registry’s scrubbing

---

<sup>154</sup> MICH. COMP. LAWS § 436.1701 (2006)

<sup>155</sup> MICH. COMP. LAWS § 722.641 (2006)

<sup>156</sup> MICH. COMP. LAWS §§ 722.673-722.677, §§ 750.142-750.143 (2006); 47 U.S.C. § 231(e)(6)(2006).

<sup>157</sup> MICH. COMP. LAWS § 432.218 (2006)

<sup>158</sup> MICH. COMP. LAWS § 432.29 (2006)

<sup>159</sup> MICH. COMP. LAWS § 333.7401 (2006)

<sup>160</sup> MICH. COMP. LAWS §§ 750.223, 28.422 (2006)

<sup>161</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-301 (2006); UTAH CODE ANN. § 13-39-302 (2006) (providing both criminal and civil penalties for noncompliance); Michigan Children’s Protection Registry Act, MICH. COMP. LAWS §§ 752.1067, 752.1068 (2006) (Michigan provides both civil and criminal penalties for noncompliance).

<sup>162</sup> Compare, Child Protection Registry, UTAH CODE ANN. § 13-39-302(1) (2006) (providing minors and guardians standing in civil actions to sue) and Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1068(8)(1) (2006) (giving minors or their guardians standing in civil court) with CAN-SPAM Act, PL 108-187, 117 Stat. 2699, 2712-2713 (2003) (providing so citizen suit provision).

<sup>163</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-302(2)(a)(ii) (2006).

<sup>164</sup> Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1068(8)(5)(i-ii) (2006).

<sup>165</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-301(1)(a) (2006).

<sup>166</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-301(1)(b) (2006).

<sup>167</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-301(2) (2006).

<sup>168</sup> Michigan Children’s Protection Registry Act, MICH. COMP. LAWS § 752.1067(7) (2006).

<sup>169</sup> Protect MI Child, <https://www.protectmichild.com/senders/answer.html?src=q&id=158> (stating “Marketers who continue to target addresses that are registered on the Michigan Children’s Protection Registry face felony charges and up to two years in jail.”)

<sup>170</sup> MICH. COMP. LAWS § 752.1065(3) (2006); UTAH CODE ANN. § 13-39-202(2) (2006).

mechanism or took reasonable measures to comply with the code.<sup>171</sup>

## 2. *FTC Concerns*

In a letter from the FTC's Office of Policy Planning to Illinois State Representative Angelo Saviano, the FTC outlined the potential problems with a child email registry.<sup>172</sup> First, such a registry may provide pedophiles and other dangerous persons with a list of contact points of children, because such a list cannot be effectively monitored for abuse.<sup>173</sup> Also, a state's attorney general's office will not likely be able to screen every marketer's background who seeks to scrub its list against the registry.<sup>174</sup>

Second, minors' email addresses on the registry are unlikely to receive less spam and may receive more adult oriented spam.<sup>175</sup> The FTC explained that currently spammers face a hurdle in determining which emails are active and valid.<sup>176</sup> A registry of email addresses would "eliminate that technological hurdle, one of the few remaining barriers that can slow spammers down."<sup>177</sup>

Third, existing security techniques would not prevent the abuse of the list.<sup>178</sup> One technique, currently used in both Utah and Michigan, would allow centralized scrubbing in which marketers would submit a list to the agency administering the registry and then the agency would then return a list purged of minor's email addresses.<sup>179</sup> For the same reason the FTC rejected such a method on the national level, the FTC reiterated that the same threat exists for state run child registries: "spammers would simply have to compare their pre-scrubbed and post-scrubbed lists for differences between them, and identify email addresses removed by the scrubbing."<sup>180</sup> Thus spammers could construct a substantial portion of the registry, and even if the state tracked the identities of marketers the state would have no way to know if the marketers were misusing the registry addresses since most spammers are virtually untraceable.<sup>181</sup>

---

<sup>171</sup> Child Protection Registry, UTAH CODE ANN. § 13-39-304 (2006).

<sup>172</sup> See generally, Letter from Fed. Trade Comm'n to Angelo Saviano, *supra* note 9.

<sup>173</sup> *Id.* at 6-7

<sup>174</sup> *Id.* at 7

<sup>175</sup> *Id.*

<sup>176</sup> *Id.* at 8

<sup>177</sup> Letter from Fed. Trade Comm'n to Angelo Saviano, *supra* note 9, at 8.

<sup>178</sup> *Id.* at 9

<sup>179</sup> *Id.* at 10

<sup>180</sup> *Id.*

<sup>181</sup> *Id.*

Additionally, one-way hashing—using cryptographic algorithms to transform a string of text into character strings called “hashes” in order to render the email address unreadable—also will not prevent registry misuse.<sup>182</sup> Although such hashing would prevent a hacker from appropriating useful information, an illegitimate marketer may still determine minor’s active email addresses from comparison of distribution lists before and after the scrubbing.<sup>183</sup>

Finally, such child registry laws would have negative consequences for consumers and competition.<sup>184</sup> Because an email address does not indicate the geographic location of the user, a marketer cannot easily separate the emails from a given state.<sup>185</sup> Thus, a sender marketing goods would have to scrub its list continually to ensure compliance.<sup>186</sup> Such costs can be substantial for marketers and may “cause some legitimate marketers to consider ending mass email campaigns altogether.”<sup>187</sup> Given such concerns, the FTC strongly advises against the creation of such child protection registries.<sup>188</sup>

### III. DISCUSSION

#### A. CHILD PROTECTION REGISTRIES’ CONSTITUTIONAL PROBLEMS

After *Reno v. ACLU* and *Ashcroft v. ACLU*, the spectrum of solutions to protect children from emails’ potentially harmful material content seems slim. While COPA addressed the Court’s initial concern with the CDA by narrowly applying to commercial speech, to content that is “harmful to minors,” and to a narrower medium of only webpages (as opposed to the entire internet), COPA still failed constitutional muster under the First Amendment.<sup>189</sup> The law failed because the Court found the statute was content-based legislation, regulating the internet, and was not wholly limited to unprotected, obscene speech.<sup>190</sup> Hence the Court applied strict scrutiny and found that filtering software provided a plausible less restrictive alternative.<sup>191</sup>

---

<sup>182</sup> *Id.* at 10

<sup>183</sup> *Id.* at 11

<sup>184</sup> *Id.* at 13

<sup>185</sup> *Id.*

<sup>186</sup> *Id.*

<sup>187</sup> *Id.* at 14

<sup>188</sup> *Id.* at 15

<sup>189</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004) (finding COPA not least restrictive alternative)

<sup>190</sup> *See supra* text accompanying notes 34-133.

<sup>191</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004) (finding COPA not least restrictive alternative)

### *1. Child Protection Registries Subject to Strict Scrutiny*

Analogously to COPA, the Child Protection Registry is also likely to be found unconstitutional under the First Amendment. First, as both *Reno v. ACLU* and *Ashcroft I and II* made clear, the Court will view content regulations of the internet with strict scrutiny. Like both the CDA and COPA, the child registry laws are content-based legislation because they attempt to prevent certain content, i.e. materials regarding pornography, tobacco and alcohol, from reaching a minors' inbox. Also, the Child Protection Registry is a regulation the internet, including email and instant messages and unlike broadcasting will not likely subject to a lower level of scrutiny because of the medium.

### *2. Overbreadth: Inability to Channel Indecent but "Harmful" Communications*

Although the "harmful to minors" standard is likely constitutional in certain contexts, given the speaker's inability to effectively channel communications to his intended internet audience, the Court will likely find the child registries overbroad. In *Ashcroft v. ACLU I*, the plurality found that when the scope of the obscenity statute's coverage is limited by a serious value prong and a prurient interest prong or a community standards prong, the Court will find no First Amendment violation.<sup>192</sup> Here, the "harmless to minors" standard defined prohibited content as material that "(a) taken as a whole, appeals to the prurient interest in sex of minors; (b) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and (c) taken as a whole, does not have serious value for minors."<sup>193</sup> The statute further defines serious value to include "only serious literary, artistic, political or scientific value for minors."<sup>194</sup> Thus, the statute is similar to *Miller* in that it is limited by a community standards prong of (b) and a serious value prong of (c), and is similar to *Ginsberg* in that its alters the obscenity standard to reference minors. Arguably, since COPA was remanded without reaching the overbreadth issue,<sup>195</sup> and *Ginsberg* upheld a substantially similar provision,<sup>196</sup> the "harmless to minors" standard may not be substantially overbroad so as to render it unconstitutional because it is limited by both a community standards prong and serious

---

<sup>192</sup> *Ashcroft v. ACLU*, 535 U.S. 564, 582 (2002).

<sup>193</sup> UTAH CODE ANN. § 76-10-1201 (4) (2006) (emphasis added).

<sup>194</sup> UTAH CODE ANN. § 76-10-1201 (4) (2006).

<sup>195</sup> See *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004) (remanding because COPA not least restrictive alternative and not reaching issue of overbreadth)

<sup>196</sup> See *supra* text accompanying notes 68-77.

value prong.

In *Ginsberg*, however, the speakers could channel adult speech to adults but inhibit such speech from reaching the eyes and ears of minors.<sup>197</sup> In contrast, with the CDA, COPA, and Child Protection Registries, there is no ability to channel content to only adults.<sup>198</sup> Although the “harmful to minors” standard is limited by both a “community standards” prong and a “serious value” prong as required by the plurality in *Ashcroft v. ACLU I*,<sup>199</sup> like COPA, it differs from *Miller* because each prong is measured as to minors, making the covered content broader than obscene content as defined in *Miller* and hence applicable to merely indecent material. The plurality only found that use of “community standards” to define a prong of “harmful to minors” was not overbroad.<sup>200</sup> Upholding use of community standards to define harmful content as to minors was not surprising given the use of community standards in the *Miller* test. Because the “harmful to minors” standard does not strictly parallel the *Miller* test for obscenity, the Child Protection Registry necessarily applies to protected, indecent speech by referencing minors.<sup>201</sup> However, unlike in *Ginsberg* where the seller of ‘girlie’ magazines needed only to check a buyer’s identification in order to channel indecent speech to adults and away from children,<sup>202</sup> by lacking cost effective age verification techniques, the Child Protection Registry, like the CDA, is likely overbroad since the speaker has no ability to channel his communications. Given the inability to channel communications, the Child Protection Registry, through its substantial civil and criminal penalties reduces the inbox to what is suitable for the sandbox.

Although the Child Protection Registry facially appears to only channel communications away from minors like in *Ginsberg*, it could effectively curtail adult communications by creating substantial criminal and civil penalties which might chill protected email communication. A marketer’s cost of scrubbing a registry places practical burdens similar to those the Court recognized in ruling the CDA and COPA unconstitutional.<sup>203</sup> In *Reno v. ACLU*, the Court concluded that it would be “prohibitively expensive...to verify that their users are adults.”<sup>204</sup>

---

<sup>197</sup> See *supra* text accompanying notes 68-77.

<sup>198</sup> See *supra* text accompanying notes 94-103.

<sup>199</sup> See *supra* text accompanying notes 94-103.

<sup>200</sup> *Ashcroft v. ACLU*, 535 U.S. 564 (2002).

<sup>201</sup> See *Reno v. ACLU*, 521 U.S. 844, 875 (1997) (stating that “sexual expression which is indecent but not obscene is protected by the First Amendment”).

<sup>202</sup> *supra* text accompanying notes 68-77.

<sup>203</sup> See *supra* note 94-103 and accompanying text.

<sup>204</sup> *Reno v. ACLU*, 521 U.S. 844, 877 (1997).

Similarly, because email lacks geographical identification or age verification, the only practical way to avoid the Child Protection Registries' substantial criminal and civil penalties would be to pay both Utah and Michigan for monthly scrubbing.<sup>205</sup> Because both statutes are strict liability statutes, potentially 'harmful' emails<sup>206</sup> must be scrubbed to avoid potential liability even if that expression is not intended to reach Utah or Michigan minors. Interestingly analogous, Justice Stevens, writing for the majority in *Reno v. ACLU* surmised that "[k]nowledge that, for instance, one or more members of a 100-person chat group will be a minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults."<sup>207</sup> Given the Court's acknowledgement of practical costs as burdens on free speech, the cost and effort of monthly scrubbing against both registries will likely be found to be a substantial burden on free speech that can only be justified by a compelling state interest and as the least restrictive alternative.

### 3. *Compelling Interest in Protecting Minors*

Although the government has a compelling interest in protecting its resident minors from harmful content,<sup>208</sup> the Court has found that such interest, however compelling, does not justify such a broad suppression of speech so as to limit adults to that which is appropriate for children.<sup>209</sup> Thus, to the extent the Utah and Michigan statutes unnecessarily regulate protected speech by not providing an ability to channel communications only to adults, the statutes would likely be overbroad and a violation of the First Amendment.<sup>210</sup>

### 4. *Several Less Restrictive Alternatives*

Because the Child Protection Registry is a content-based restriction of the internet that is not restricted to obscene speech as defined under *Miller*, the Court will likely apply strict scrutiny and demand a governmental showing that notwithstanding the recognized compelling interest of protecting children, the legislation must be the least restrictive legislative or technological alternative.

---

<sup>205</sup> Complaint at 23, *Free Speech Coalition v. Shurtleff*, (C.D. Utah) (No. 2:05-cv-00949) available at <http://www.freespeechonline.org/webdocs/011706AmendedUtCPRComplaint.pdf>

<sup>206</sup> By harmful emails I mean emails that would be protected among adults but obscene with respect to children.

<sup>207</sup> *Reno v. ACLU*, 521 U.S. 844, 876 (1997).

<sup>208</sup> *Reno v. ACLU*, 521 U.S. 844, 875 (1997).

<sup>209</sup> *Id.* (stating the government may not "reduce the adult population to only what is fit for children").

<sup>210</sup> The First Amendment made applicable to the states through the Fourteenth Amendment.

Several possible, less restrictive, legislative regulations are available. The Free Speech Coalition provided three simple alternatives in their amended complaint in *Free Speech Coalition v. Shurtleff* that would provide less restriction on protected speech. First, both Michigan and Utah could require Unspam to post hash values of the registered contact points on a website so that emailers could examine those values without cost, reducing the practical burden on costly monthly scrubbing.<sup>211</sup> Second, instead of charging per email scrubbed, Utah or Michigan could impose a minimal charge upon only those email addresses that actually are listed in the protection registry, thereby avoiding the burdensome cost on the majority of emails that do not belong to registered minors.<sup>212</sup> Third the burden on protected speech could be lessened by abolishing the statutes' strict liability provisions or accepting a defense that an emailer reasonably believed an adult requested the email.<sup>213</sup>

Even less restrictive than legislative reforms, however, is the promotion of technological solutions such as email filters. In *Ashcroft II*, Justice Kennedy found the COPA likely to violate the First Amendment because webpage filters could provide a less restrictive means of achieving the government's compelling interest of protecting children.<sup>214</sup> Like webpage filters, email filters are currently available and may provide a less restrictive means of protecting children from unwanted and harmful emails.<sup>215</sup> Under Kennedy's reasoning, the promotion of such filters would not criminalize protected speech, would allow adults to gain access to protected speech, and would hinder minors' access to such content.<sup>216</sup>

One commentator argues that technological solutions will almost always provide a less restrictive alternative to congressional legislation affecting the internet.<sup>217</sup> The *Miller* obscenity standard and also the *Ginsberg* "harmful to minors" standard both require a community standard

---

<sup>211</sup> Complaint at 29, *Free Speech Coalition v. Shurtleff*, (C.D. Utah) (No. 2:05-cv-00949) available at <http://www.freespeechonline.org/webdocs/011706AmendedUtCPRComplaint.pdf>

<sup>212</sup> *Id.*

<sup>213</sup> *Id.* at 30.

<sup>214</sup> *Ashcroft v. ACLU*, 543 U.S. 656, 667 (2004).

<sup>215</sup> FED. TRADE COMM'N, A Report by the Federal Trade Commission's Division of Marketing Practices: Email Address Harvesting and the Effectiveness of Anti-Spam Filters, at 6 (Nov. 2005) available at <http://www.ftc.gov/opa/2005/11/spamharvest.pdf> (concluding although marketers continue to send spam, anti-spam technologies, such as ISP filtering software, dramatically reduces spam that actually reaches consumers).

<sup>216</sup> This reasoning parallels Kennedy's reasoning. See *Ashcroft v. ACLU*, 542 U.S. 656, 667 (finding governmental promotion of webpage filters would not criminalize protected speech, would allow adults to gain access to protected speech, and would hinder minors' access to such content).

<sup>217</sup> See Wheatland, *supra* note 47, at 385 (arguing "a technical solution imposed by the user will almost always be less restrictive").

prong that is measured by local, not national, standards.<sup>218</sup> Since the internet is not confined to a given community, statutorily applying that standard to the broad, nebulous structure of the internet will inevitably restrict speech that is protected in certain communities.<sup>219</sup> Since the internet is not limited to one community, speakers are forced to bow to the most sensitive ears.<sup>220</sup> Such an outcome, however, burdens a broad spectrum of speech which the Court has denounced as unacceptable in *Reno v. ACLU* and *ACLU v. Ashcroft*.<sup>221</sup> On the other hand, technology likely changes more rapidly than Congress can pass laws, making a new, less restrictive technological alternative always possible.<sup>222</sup> Technological solutions in general allow for greater parental control over material affecting their children by providing controls at the user end, while at the same time not affecting other users of the internet.<sup>223</sup> As a solution, Congress should not pass broad proscriptive statutory controls but should encourage the implementation of technological solutions.<sup>224</sup>

## **B. IMPROVED MODEL LEGISLATION: CHILD AND NON-CONSENTING ADULT DO-NOT-EMAIL DOMAIN**

### *1. Do-Not-Email Domain*

In addition to mere filters and other technologies created by private industry, however, the least restrictive and most efficacious alternative may be a proactive legislative solution that uses technology to create a child-friendly email domain. If Congress were to create an email domain for children and adults who wish not to receive either obscene or indecent material the channeling problems of the internet would be reduced. Such a domain would address many of the concerns raised by the FTC, would allow legislatures to pass constituent-pleasing legislation, and would be narrowly tailored to the compelling interest of protecting children while being the least restrictive burden on protected adult speech.

Under this model, legislation a new domain would be created where children and adults who wished to receive only those emails appropriate for minors could register a new email

---

<sup>218</sup> *Id.* at 384

<sup>219</sup> *Id.*

<sup>220</sup> *Id.*

<sup>221</sup> *Id.* at 386.

<sup>222</sup> *Id.*

<sup>223</sup> *Id.* at 385.

<sup>224</sup> *Id.* at 390 (arguing Congress should either take “hands off” approach or enact legislation promoting technological solutions such as filters, mandatory labeling of websites, and creation of certificate authority)

address under the statutorily restricted domain. The legislation creating the new domain would prohibit the sending of emails that were harmful to minors as defined under the “harmful to minors” three prong test used in COPA to any email under the domain.

In fact, a restricted domain similar to the one proposed is already in force, known as the Dot Kids Implementation and Efficiency Act of 2002.<sup>225</sup> This act granted the National Telecommunications and Information Administration (NTIA) the power to establish a second-level domain within the United States country code domain [.kids.us].<sup>226</sup> Kids.us is essentially a new webspace dedicated to child-appropriate content.<sup>227</sup> The Dots Kids Act requires that registrars enter written agreements that they will only provide access “to material that is suitable for minors and not harmful to minors.”<sup>228</sup> It also requires that the NTIA provide procedures for removing non-complying registrars and a process for efficient and impartial dispute resolution. In addition, it prohibits “two-way” and “multi-user interactive services” unless the registrant certifies such services are in compliance with the content standards and operated to protect minors from harm.<sup>229</sup> Since all content providers on the kids.us domain will have certified that they will comply with kid-friendly content and will be monitored by NeuStar, kids.us provides a safe haven for children and provides a constitutional and kid-friendly alternative to broad regulation of the internet.

Alice McAfee argues the Kids.us domain provides a constitutional solution to providing a “kid-friendly webspace.”<sup>230</sup> The “harmful to minors” three factor definition<sup>231</sup> mirrors the language from *Miller*’s three-prong obscenity test and likely falls outside the purview of the First Amendment.<sup>232</sup> McAfee noted that the Court previously addressed such a definition in *Ashcroft II* and found that COPA was an improvement over the CDA because it defined “harmful to minors” in a manner parallel to the *Miller* definition of obscenity.<sup>233</sup> McAfee’s analysis is correct given that the Act channeled minors to another domain separate from the regular internet,

---

<sup>225</sup> Dot Kids Implementation and Efficiency Act of 2002, Publ. L. No. 107-317, 116 Stat. 2766, (2002) (codified at 47 U.S.C.A. § 941 (2006)).

<sup>226</sup> 47 U.S.C.A. § 941(a) (2006)

<sup>227</sup> See generally Alice G. McAfee, *Creating Kid-Friendly Webspace: A playground Model for Internet Regulation*, 82 TEX. L. REV. 201, 224 (2003).

<sup>227</sup> 47 U.S.C.A. § 941(j)(1) (2006).

<sup>228</sup> 47 U.S.C.A. § 941(a) (2006).

<sup>229</sup> 47 U.S.C.A. § 941(c)(10) (2006).

<sup>230</sup> See generally, McAfee, *supra* note 227.

<sup>231</sup> 47 U.S.C.A. § 941(j)(1) (2006).

<sup>232</sup> McAfee, *supra* note 227, at 219.

<sup>233</sup> *Id.*

thereby not burdening protected, adult speech, which may still be posted outside of the new web-domain. Thus, the kids.us will be protective of children beyond that which can be constitutionally secured outside the kids.us domain.<sup>234</sup>

Although the kids.us domain does not currently allow email,<sup>235</sup> it provides just the type of restricted domain needed. Congress should either pass legislation allowing email access to the kids.us domain and create third-level domains for each state (e.g. ga.kids.us) or pass legislation allowing states to create their own third-level domain.<sup>236</sup> Thus, minors or non-consenting adults could register an email address under the [state].kids.us domain, creating, for example, lawdawg@ga.kids.us. Under the alternative scheme, States such as Utah or Michigan could create a third-level domain under their current domains [for example kids.ut.gov] allowing Utah residents who wish to opt out of such communications to register an email address in the same fashion [for example GAfan@kids.ut.gov].

## 2. *Constitutional Analysis*

The domain-based email registry potentially solves many of the legal problems previously faced by the CDA and COPA and the Child Protection Registries. First, restricted domains solve the dual problems of identity and geography and hence alleviate many of the earlier constitutional concerns addressed by O'Connor.<sup>237</sup> The inclusion of the sub-domain in the email address would announce that the recipient opted into the restricted domain and hence was either a minor or an adult who only wished to receive emails appropriate for minors. Although such legislation would be regulating based on the content of emails, such a statute would be narrowly tailored to the protected interest of shielding minors and incidentally non-consenting adults from 'harmful' material while allowing free exchange of protected expression among consenting adults. For example, since sexual expression is only protected among consenting adults, and only non-consenting adults and minors have "opted-in" for email addresses under the restricted domain, the legislation is not regulating any protected speech on its face. Additionally,

---

<sup>234</sup> McAfee, *supra* note 227, at 222.

<sup>235</sup> See *supra* text and accompanying footnote 112.

<sup>236</sup> I propose that Congress pass legislation allowing states to create their own third level domains to avoid any state concerns with violations of the dormant commerce clause and hence to facilitate state involvement in protecting minors from harm. See e.g. *Am. Library Ass'n v. Pataki* 969 F. Supp. 160, 183-84 (S.D.N.Y. 1997) (finding state regulation of internet preventing knowing communication to minors of material harmful to minors to violate Commerce Clause).

<sup>237</sup> See *supra* text accompanying notes 94-103.

because the domain is apparent in the email itself (e.g. kids.us would be at the end of every email address), senders of emails would only be inconvenienced by having to look at the address prior to sending messages that would be harmful to minors.

The problems previously experienced by the *Miller* test and the “harmful to minors” test as applied to the internet would no longer exist. One can infer that the “harmful to minors” standard alone did not result in COPA being the least restrictive alternative. The United States Court of Appeals held that COPA’s use of contemporary community standards was overbroad because there was no way to distinguish between geographic communities.<sup>238</sup> Even though the Supreme Court vacated this ruling on other grounds, the Court still lauded the COPA “harmful to minors standard” as an improvement over the CDA and further mentioned that “COPA’s reliance on community standards to identify ‘material that is harmful to minors’ does not by itself render the statute substantially overbroad.”<sup>239</sup> In light of the reasoning of the Court of Appeals, the Supreme Court and our discussion *infra*,<sup>240</sup> the main problem with using community standards on the internet was that no local internet community existed, so speakers—not knowing who would receive their message—had to pander to the most sensitive community. Under a domain based email system, in contrast, a community has been created under a domain that is related to a particular geographical community(i.e. utah.gov) and composed of minors and non-consenting adults. Hence the geographical blinders of the internet’s logical space are removed, providing a sender with notice that a message sent to a particular domain will be judged by the standards of that local community and by state law as to their most sensitive members—minors and non-consenting adults. Thus the impediments to providing a local community on the internet are resolved. Hence, since ‘harmful’ to minors may now be defined with a prurient interest prong, a community standards prong as defined by state law, and a serious value prong, and only applies to minors and non-consenting adults who have opted into the domain, no overbreadth problems remain and regulation may survive the hurdle of strict scrutiny.

### 3. Practical Concerns

The domain-based email also addresses many of the other practical concerns raised by the Federal Trade Commission regarding the National Do-Not-Email and Child Protection

---

<sup>238</sup> See *ACLU v. Reno*, 217 F.3d 162, 176-80 (3d. Cir. 2000).

<sup>239</sup> *ACLU v. Ashcroft*, 535 U.S. 564, 578 (2002).

<sup>240</sup> See *supra* text accompanying notes 217-224.

Registries. First, the FTC was concerned that protection registries would make a complete list of contact points potentially available to the public, including pedophiles. Second, the FTC noted that spammers may use registries to verify active email addresses by comparing pre-scrubbed and post-scrubbed lists.<sup>241</sup> Regarding both these concerns, a domain-based protection makes no list available to the public for scrubbing like in the Child Protection Registries. Also, the mere existence of an email does not signal the email is active any more than the existence of any other email, because the number of potential email addresses under a domain are limitless (i.e. lawdawg1@kids.ga.us, lawdawg2@kids.ga.us, lawdawg3@kids.ga.us, etc.). Also, since either minors or adults may create a new email address under the domain, pedophiles will not know which emails specifically belong to minors. Thirdly, the concerns raised by the FTC regarding the National-Do-Not-Email registry primarily focused on the availability of an identifiable list that may fall into the wrong hands or allow for spammers to verify email addresses.<sup>242</sup> Again, in contrast to both the National-Do-Not-Email registry and the Child Protection Registry, in this proposal no list of protected emails exists. Thus, just as one would sign up for a gmail.com account, one would opt-into this proposed domain. Fourthly, the FTC also voiced concerns over the Child Protection Registry's potential harm to consumers and competition given the difficulty of marketers to identify both geography and identity of email users.<sup>243</sup> An email domain solves this problem by providing notice in the domain name itself. Lastly, the FTC also rejected a National-Do-Not-Email Registry because of the inability to authenticate an email's sender.<sup>244</sup> Although this concern addresses problems with the underlying structure of the email system,<sup>245</sup> the CAN-SPAM Act addressed false and misleading email headers making it illegal to change the header so as to conceal the sender of an email.<sup>246</sup> Thus, such legislation creating domains would at least serve to curb adult-oriented expression originating from legitimate businesses and citizens. As seen in Michigan's recent indictments,<sup>247</sup> legitimate businesses send advertisements

---

<sup>241</sup> See *supra* text accompanying footnotes 129, 175-177

<sup>242</sup> See generally AVIEL D. RUBIN, A REPORT TO THE FEDERAL TRADE COMMISSION ON RESPONSES TO THEIR REQUEST FOR INFORMATION ON ESTABLISHING A NATIONAL DO NOT E-MAIL REGISTRY, (May 10, 2004), <http://www.ftc.gov/reports/dneregistry/expterrpts/rubin.pdf> (rejecting various proposals for Do Not Email Registry considering third-party forwarding, scrubbing, and hashing)

<sup>243</sup> See *supra* text accompanying footnotes 184-188

<sup>244</sup> See *supra* text accompanying footnote 128

<sup>245</sup> See RUBIN, *supra* note 242, at 13 (discussing current problems with tracing non-complaint spammers because of open proxies, open SMTP relays that require no authentication, use of zombie computers to relay messages).

<sup>246</sup> See *supra* text and accompanying footnote 121.

<sup>247</sup> Michigan Attorney General Mike Cox filed criminal and civil charges after an email wine advertisement was sent

for material that is deemed harmful to minors and the origin of the email may be traced to the appropriate sender so long as the email header information is not illegally altered.

#### 4. *Limitations on Domain Solution: Don't Trash the Filter*

The Do-Not-Email Domain is not a cure-all. Illegitimate businesses that route messages through proxies, zombie computers and open SMTP protocols are very difficult to trace. Open SMTP relays do not require authentication and simply forward email to any destination allowing illegitimate business to disguise their email as originating from the open relay by changing the information in the email's header.<sup>248</sup> These practices are already illegal and prosecuted pursuant CAN-SPAM<sup>249</sup> and will not likely be cured by a do-not-email domain. Additionally, a large amount spam comes from overseas, where prosecutions are even more difficult.<sup>250</sup> The Do-Not-Email Domain would not effectively protect children from such illegitimate marketers. To address such illegitimate marketers, users should continue the use of private filters to sift unsolicited commercial email from their inboxes.

Filters, however, are not perfect. The effectiveness of filters as a less restrictive alternative to COPA is currently being challenged in *ACLU v. Gonzalez*.<sup>251</sup> Filters lack common sense in that they do not understand a word's meaning but simply block prohibited words.<sup>252</sup> Filters will be both over and under-inclusive, banning appropriate material and also allowing inappropriate material to pass through.<sup>253</sup> Combining a domain-based email registry with filters would provide the benefits of both methods. Illegitimate marketers could be filtered by users who wished not to receive such advertisements, and legitimate marketers of harmful content would be deterred from sending material that is harmful to minors under the protected domain.

---

to Kelly Cool of Oakland County, Michigan. The advertisement promoted Four Seasons Wine a business that delivers wine from small boutique wineries. See Ken Magill, Michigan Casts Wide Do-Not-E-mail Net, DIRECT, Oct. 1, 2006; Ken Magill, *Michigan Casts Wide Do-Not-E-Mail Net*, PRIMEDIA INSIGHT, Sept. 12, 2006; Robert Jaques, *US Firms Under Fire for Spamming Children*, VNU BUSINESS PUBLICATIONS, Aug. 16, 2006.

<sup>248</sup> See RUBIN, *supra* note 242, at 14 (discussing open SMTP relays).

<sup>249</sup> See FED. TRADE COMM'N, *supra* note 1, at 23 (discussing prosecutions under CAN-SPAM).

<sup>250</sup> See RUBIN, *supra* note 242, at 15 (stating much spam originates from overseas).

<sup>251</sup> See Andrew Noyes, *Experts Call Into Question Value of Internet Filters*, TECHNOLOGY DAILY PM, Nov. 13, 2006 (reporting on Justice Department arguments in federal court that internet filtering software does not work nor will it ever be completely effective in keeping children safe from inappropriate material online); Warren Publ'g, Inc., *Complexity of Language Dooms filters, Government. Witness Says in COPA Trial*, WARREN'S WASHINGTON INTERNET DAILY, Nov. 13, 2006, at Vol.II, Issue 218 (reporting on witness testimony in *ACLU v. Gonzales*).

<sup>252</sup> See Warren Publ'g, *supra* note 251 (reporting on Rutgers University linguist Stephen Neale testifying that filters lack common sense in discerning meaning of statements).

<sup>253</sup> See *id.* (reporting on Neale providing analogy to sleek hawks and chubby robins entering birdhouses to demonstrate that filters are both over and under-inclusive).

As witnessed from both the federal and state legislation, however, legislatures wish to provide more protection than just private filters. The Do-Not-Email Domain will provide just such extra protection from legitimate marketers sending harmful content to minors by providing notice of a recipient's status as a minor or non-consenting adult and providing an incentive to remove those email addresses from their distribution lists through sanctions.

In sum, the secondary domain for non-consenting adults and minors would solve the dual problems of geography and identity, allow emailers to cull their distribution lists themselves without resorting to costly scrubbing, and provide a narrowly tailored alternative by regulating only emails to minors and non-consenting adults, thereby alleviating the constitutional problem of restraint of non-obscene communication between consenting adults. Such a solution is limited to addressing harmful content from legitimate marketers, and filters should still be used to combat illegitimate spam.

#### **IV. CONCLUSION**

Legislators and their constituents are striving to protect their minors from harmful content on the internet. Although email filters may protect children, the push of parents and legislatures for greater protection is evidenced by Congress's enactment of the CDA, its continued struggle to uphold COPA, and Utah and Michigan's enforcement of Child Protection Registries despite the protection already afforded by filters. As the Court has made clear, however, this extra protection must not come at the expense of adult communication. Each legislative act likely failed constitutional scrutiny because each targeted or restrained too broad an audience in an attempt to protect minors. The CDA targeted the entire internet, COPA effectively targeted all website users, and the Child Registries effectively targeted all emailers of adult oriented material. Each legislative attempt failed because it only sought purely broad legislative solutions. By creating an email domain for minors and non-consenting adults, the legislature would effectively partition a portion of the vast internet, allowing targeted legislation without unnecessarily burdening protected expression. Although private industry may eventually prove efficacious in protecting minors through extremely effective filters, Congress and State legislatures will still have to face their angry constituents in the interim. By creating an email domain for minors and non-consenting adults, Congress and state legislatures would proactively protect minors from harm while respecting the First Amendment rights of consenting adults.