UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 1 *Journal of Computer & Information Law - Fall 2003*

Article 3

Fall 2003

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 (2003)

Matthew B. Prince

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

MATTHEW B. PRINCE† AND PATRICK A. SHEA‡

I. INTRODUCTION

Thirty-six states have tried. Since 1997, thirty-six states have passed their own particular variation of an anti-spam law.[1] Beginning with Nevada, one by one across the country state after state drafted and passed laws designed to beat back the rising tide of unsolicited electronic mail. The scourge of unwanted messages, colloquially known as "spam," had become one of the top consumer complaints in legislators' offices nationwide.[2] It filled electronic mail inboxes with solicitations for pornog-

† Matthew B. Prince is the CEO and co-founder of Unspam, LLC, an Illinois-based business and government consulting company helping to draft and enforce effective anti-spam laws. He is a member of the Illinois Bar and an Adjunct Professor of Law at The John Marshall Law School. He received his J.D. from the University of Chicago Law School and his B.A. in English and Computer Science from Trinity College, Hartford, Connecticut.

‡ Patrick A. Shea is an attorney in private practice in Salt Lake City, Utah. He is a member of both the Utah and District of Columbia Bar and has taught law and political science at the University of Utah and Brigham Young University. Before joining Ballard Spahr, he worked for the Clinton Administration as the Deputy Assistant Secretary for Land and Minerals Management and the Director of the Bureau of Land Management. He has litigated extensively in the area of the First Amendment, freedom of speech, and the rights of the media. He received his J.D. from Harvard Law School, his M.A. in Genetics, Ethology, and Anthropology from Oxford University, and his B.A. from Stanford University, where he was a Rhodes Scholar.

1. *See* David E. Sorkin, *Spam Laws* <http://www.spamlaws.com/state/index.html> (accessed Jan. 30, 2004). The particular states and their individual statutes are cited explicitly below.

2. The Federal Trade Commission (FTC) reports that they receive more than 130,000 complaints about spam each day at a special electronic mail address the commission has

raphy, dubious herbal supplements, fraudulent credit offers, and scams sent from purported Nigerian diplomats.[3] For state legislators, there was no tastier dish to serve to constituents than a measure promising to broil spam.[4]

The problem was that as states set out to fry spam, every state followed the same basic recipe.[5] Unfortunately, that recipe simply did not work. In the seven years under anti-spam laws, only two states have brought successful prosecutions.[6] Only one of those was able to enforce

established (uce@ftc.gov). *See* FTC, *FTC Measures False Claims Inherent In Random Spam* <http://www.ftc.gov/opa/2003/04/spamrpt.htm> (Apr. 29, 2003). States, too, face consumers angry about spam. For example, in Washington state, spam has become the "number one consumer complaint," according to the Assistant Attorney General. *See* Paula Selis, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, May 2, 2003). The Washington Attorney General's office receives 1,000–1,600 complaints per month about spam. *See* Wa. Atty. Gen. Web site, *Junkmail* <http://www.atg.wa.gov/junkemail/> (accessed Jan. 30, 2004). ISPs too have stated that spam is the top complaint they receive from their customers. *See e.g.* Brian Morrissey, *Report: ISPs Block 17 Percent of Legit E-mail*, InternetNews.com (Aug. 12, 2003) (available at <http://www.internetnews.com/IAR/article.php/2247651>).

3. *See generally* Brian Bergstein, *AOL: Viagra, Oprah Among Top Spam Topics*, eWeek (Dec. 31, 2003) (available at <http://www.eweek.com/article2/0,4149,1425061,00.asp>) (a general list of the top subjects of spam for 2003).

4. Public support for anti-spam laws is extremely high. *See e.g.* InsightExpress and Unspam, *2003 Comprehensive Spam Survey,* <http://www.unspam.com/fight_spam/information/survey_personal.html> (updated Oct. 15, 2003) (more than eighty-five percent of respondents favor strong anti-spam laws, ninety-five percent of parents favor laws that protect children from pornographic spam); SurfControl, *SurfControl Survey Finds Majority of IT Professionals Favor Introduction of Federal Legislation to Regulate Spam* (Jan. 2003) (available at <http://www.surfcontrol.com / resources / surveys / SurfControl_Jan_Survey.pdf>) (ninety-five percent of information technology professionals support strong anti-spam laws).

5. Part of the reason for this appears to stem from the lobbyists advocating for the anti-spam laws. Technology companies such as Microsoft distributed position papers in multiple states calling for legislation following a basic formula. Microsoft Corporation, *Microsoft & Spam Legislation* 1–2 (unpublished legislative talking points memo, 2003) (copy on file with the authors). With few other organizations lobbying states, legislators appear to have generally followed the Microsoft model.

6. Washington and California are the only two states to successfully enforce their anti-spam laws. Washington has received two judgments in two different anti-spam cases and has a third pending. *See* Beth Taylor, *Anti-spam Law Fails to Deter Junk-mail Marketers*, Pudget Sound Bus. J. (available at <http://www.bizjournals.com/seattle/stories/2002/12/23/focus1.html>) (updated Dec. 20, 2002); *see also* Office of Wash. Atty. Gen, *State Sues Porn-Promoting Spammer* <http://www.atg.wa.gov/releases/rel_spam_121602.html> (accessed January 30, 2004). The judgments are notable because, having targeted spammers in Texas, Oregon, and California, Washington is the only state to have enforced its anti-spam law against any out-of-state spammers. *Id.* In addition to Washington, California recently received a 2 million dollar judgment against two spammers. *See* Elise Ackerman, *Judge Orders Spammers to Pay $2 Million Fine*, San Jose Mercury News Online <http://www.siliconvalley.com/mld/siliconvalley/7101397.htm> (Oct. 25, 2003). However, both spammers were based in the state, presenting fewer jurisdictional problems. *Id.* As this

its law against an out-of-state spammer.[7] And neither state has been able to collect more than trivial portions of the settlements or judgments that they have been awarded.[8] As the old adage goes, without enforcement there is no law. In spite of the fact that a majority of states had passed some anti-spam statute, these measures have offered almost no protection. When Federal legislators decided that this was a dinner party they wanted to crash, they too followed the same basic recipe that had repeatedly failed at the state level. Instead of strengthening and adjusting the law to address the problems states had faced, Congress passed a Federal statute, known as *CAN-SPAM*,[9] which merely watered down the recipe and served it to the entire nation.

Disturbingly, what is arguably the most powerful provision of the new Federal law is a section that appears to preempt state spam regulation.[10] While the first generation of state anti-spam laws has not enjoyed much success, Federal preemption is potentially troubling in this area because it threatens to enjoin future state experimentation. We all

---

article goes to press, two additional states have litigation pending under their anti-spam statutes. First, Jerry Kilgore, the Virginia Attorney General, has filed criminal charges against two out-of-state spammers and is seeking jail time. *See* Jonathan Krim, *Virginia Indicts Two Men on Spam Charges*, Wash. Post Online <http://www.washingtonpost.com/ac2/wp-dyn/A56209-2003Dec11> (Dec. 11, 2003). Second, Jay Nixon, the Missouri Attorney General, has filed a case against a Florida spammer who sent messages to an address maintained by the attorney general's office without including the required "ADV:" label. *See* Stefanie Olsen, *Missouri Files Spam Suit under New Law*, CNET News.com <http://news.com.com/2100-1028-5089720.html> (Oct. 10, 2003). Even if these cases prove successful, they represent a mere drop in the bucket given the enormous volume of illegal spam being sent. New York also has a case pending; however, it uses a traditional consumer protection statute, not an anti-spam statute, as New York is one of the fourteen states that does not have an anti-spam law. *See infra* n. 26.

7. Washington has had more success enforcing its anti-spam statute than any other state. The state has brought at least five actions under its anti-spam law, all of which were against out-of-state defendants. *See* Ellen Perlman, *The E-Mail Mess*, Governing.com (Jan. 2004) <http://governing.com/articles/1spam.htm>. Moreover, the state has defended a constitutional challenge to its anti-spam statute to the Supreme Court, which denied *certiorari* and affirmed the Washington State Supreme Court's decision upholding the statute. *See Washington v. Heckel*, 24 P.3d 404 (Wash. 2001).

8. Compare this with do-not-call legislation. States have been able to collect more than $4.5 million in fines from enforcing their do-not-call laws since 1997. *See Gryphon Networks: Latest Do-Not-Call News and Regulatory Information* (Summer 2004) <http://www.gryphonnetworks.com/press/newsletters/2003_06/2003_06.html> (accessed Jan. 30, 2004) (at least $4,618,150 in fines as of June 2004). Even when spam cases are successful, states have not been able to collect their judgments. *See e.g* Deborah Scoblionkov, *Washington Nabs a Spammer*, Wired News (Oct. 23, 1998) (available at <http:// www.wired.com/news/politics/0,1283,15786,00.html>) (little collected by state of Washington even after a successful prosecution).

9. *See* 15 U.S.C. §§ 7701–16. *CAN-SPAM* stands for the *Controlling the Assault of Non-Solicited Pornography and Marketing Act.*

10. *See* 15 U.S.C. § 7707(b).

learned in eighth-grade civics class that one of the strengths of our system of government is that it comprises fifty "laboratories of democracy."[11] These laboratories are charged with innovating and implementing creative legislative solutions. The best ideas percolate up to the Federal level; others that are not successful fall away and are replaced.[12] If *CAN-SPAM* locked in a legal regime for fighting spam that we already know from experience will not be successful, and also completely preempted further state innovation in the area, then its passage signaled a grim day for America's inboxes.[13]

Fortunately, the Federal preemption language does leave some areas of experimentation open to the states. A careful reading of *CAN-SPAM* reveals that while the legislation generally tells states to stop cooking the same recipe, it leaves room to try some new ideas and creative approaches. States are, in effect, charged to examine why the first generation of anti-spam laws failed to cook spam, and to design the next generation of solutions to spice up the recipe. Most of the paths closed to the states are those that have been empirically demonstrated not to work, but the Federal law allows other promising routes that are more likely to be successful. So instead of states hanging up their spam frying pans and leaving the party early, the question now becomes what recipe should they try next?

This article sets out to answer that question. First, it outlines the initial generation of state anti-spam laws and the provisions they have contained. Second, as part of understanding why they failed, it examines

---

11. While he was not thinking about spam, Supreme Court Justice Brandeis echoed the sentiment of many eighth-grade civics teachers when he wrote: "Denial of the right to experiment may be fraught with serious consequences to the nation. It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country." *New State Ice Co. v. Libemann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

12. For example, do-not-call laws were developed around the same timeframe as anti-spam laws but were far more successful. In 1997 there was only one do-not-call law in the country (Florida). *See Gryphon Networks Regulatory Information* <http://www.gryphonnetworks.com/regulatory/regulatory.asp> (accessed Jan. 30, 2004). By 2004, forty-three states had passed their own do-not-call law. *Id.* After witnessing the success of the do-not-call legislation on the state level, as of October 1, 2003, the Federal government has begun enforcing its own do-not-call law. *Id.* It is worth noting that the Federal do-not-call law does not preempt states from continuing to enforce their own lists. *See* 15 USCS §§ 6101–04 (2003).

13. It appears that the predictions turned out to be true. A month after it went into effect, *CAN-SPAM* seems to have had little effect on the volume of spam. *See e.g.* Brian Morrissey, *CAN-SPAM Brings No Immediate Drop*, DMNews (Jan. 12, 2004) (available at <http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=26127>); Dan Lee, *Little hope seen for spam relief*, San Jose Mercury News (Jan. 24, 2004) (available at <http://www.siliconvalley.com/mld/siliconvalley/7787192.htm >).

the economics of prosecution and what has kept prosecutors from regularly enforcing the existing laws. As part of the analysis, it takes into account the structural, constitutional, and technological issues that increase the costs of trial and drive down a prosecutor's likelihood of success. Third, it proposes a new approach to anti-spam law, a Children's Protection Registry. Such a registry has the potential to be the next generation of anti-spam statutes. Instead of taking a general omnibus approach, the proposal focuses to curb the worst effects of the problem. In doing so, it overcomes many of the challenges of the first generation of anti-spam laws and therefore is more likely to be regularly and successfully enforced.

Finally, the article examines *CAN-SPAM*'s preemption language with a specific eye to the field of regulation left open to states. Even while preempting the first generation of anti-spam statutes, the Federal law specifically leaves room for states to experiment with innovative new regulations. This article concludes that creation of a Children's Protection Registry is not preempted by *CAN-SPAM* and, in fact, falls squarely within a state's traditional police powers. As a result, for states that are still out to cook spam and are looking for a way to afford their citizens, and especially their most vulnerable citizens, enhanced legal protection from unwanted messages, a Children's Protection Registry is the logical next step.[14]

II. A BRIEF HISTORY OF ANTI-SPAM LAW

In July of 1997, the Nevada legislature, sensing a disturbing trend in the volume of unwanted electronic mail, moved to regulate unsolicited commercial messages sent via the medium.[15] The nation's first anti-

14. As this article goes to press, Utah became the first state to pass such a registry. *See* Utah H. 165, 2004 Gen. Sess. (Jan. 29, 2004) (available at <http://www.le.state.ut.us/~2004/bills/hbillint/ hb0165S01.htm>) (Utah legislation sponsored by Rep. Michael R. Styler, passed unanimously by both the House and Senate March 3, 2004, signed by the governor March 23, 2004); *see also* Kristen Stewart, *Plan would block spam to protect kids*, Salt Lake Trib. (Jan. 30, 2004) (available at <http://www.sltrib.com/2004/Jan/01302004/utah/133957.asp>). At least three additional states—Michigan, Illinois, and Georgia—are considering similar Children's Protection Registry statutes. *See* Mich. Sen. 1025, 2004 Gen. Sess (May 28, 2003) (available at <http://www.michiganlegislature.org/documents/20032004/billintroduced/senate/htm/2004-SIB-1025.htm>) (Sponsored by Sen. Mike Bishop); Ill. H. 4350, 2004 Gen. Sess. (Feb. 2, 2004) (available at <http://www.legis.state.il.us/legislation/fulltext.asp?DocName=&SessionId=3&GA=93&DocTypeId=HB&DocNum=4350&GAID=3&LegID=8643>) (Sponsored by Rep. Charles Jefferson); Ga. H. 1809, 2004 Gen. Sess. (Mar. 19, 2004) (available at <http://www.legis.state.ga.us/legis/2003_04/versions/hb1809_LC_34_0077_a_2.htm>) (Sponsored by Rep. Barbara Mobley); *see also* Tim Lemke, *Do-not-spam Lists Pushed to Protect Children*, Wash. Times (Feb. 17, 2004) (discussing legislative efforts in Utah and Michigan).

15. Nev. Rev. Stat. §§ 41.705–735 (1997). The original bill that gave rise to this statute, SB-13, was sponsored by Republican majority leader Senator William Raggio. *See*

spam law required senders of electronic mail messages containing advertisements to reveal their "legal name" and their "complete street address"[16] and to provide a valid return electronic mail address.[17] In addition, Nevada's statute mandated that senders provide "notice that the recipient may decline to receive additional electronic mail . . . and the procedures for declining such electronic mail."[18] Less than a year later, Washington's legislature followed suit and passed its own anti-spam statute.[19] Washington's statute took a slightly different tact, focusing on the deceptive nature of most spam messages. The state's law forbade the use of "a third party's internet domain name without permission of the third party."[20] It also required message senders to not disguise the "point of origin or the transmission path of a commercial electronic mail message"[21] and not provide "false or misleading information in the subject line."[22] A few months later, California took its own approach and added two more unique provisions. Specifically, the state became the first to require unsolicited messages to be labeled.[23] Basic unsolicited messages were required to carry "ADV:"[24] as the first four characters in the subject line; messages containing pornography were required to be labeled with "ADV:ADLT" as the first eight characters in the subject

---

CNET News.com, *Nevadans Against Spam* <http://news.com.com/2100-1023263458.html> (updated Jan. 20, 1997). The bill's original text was criticized as being sloppily written. *Id.* However, it required senders to receive permission before sending any commercial electronic mail messages: the so-called "opt-in" standard. *Id.* As it progressed through the legislature, it was amended to create a weaker "opt-out" standard before being passed and signed by the governor. This is significant because Nevada's choice of opt-out instead of opt-in set the initial precedent for all the anti-spam laws that were subsequently passed. Nev. Rev. Stat. Ann. § 41.705. Unlike the United States, Europe has opted for an opt-in standard. *See EuroCauce, Opt-In vs. Opt-Out* <http://www.euro.cauce.org/en/optinvsoptout.html> (accessed Jan. 30, 2004). Even with this tougher standard, however, they have had no more success than the United States in enforcing their laws. *Id.*

16. Nev. Rev. Stat. § 41.730(1)(c)(i). This is the first instance of a state requiring unsolicited electronic mail to contain the physical address and phone number of the sender.

17. *Id.* This is the first instance of a state requiring unsolicited electronic mail messages to contain a valid return address.

18. *Id.* at § 41.730(1)(c)(ii). This is the first instance of a state requiring unsolicited electronic mail messages to contain an opt-out mechanism. However, it is worth noting that the original Nevada statute contained no requirement that senders honor opt-out requests nor penalties if they did not.

19. Wash. Rev. Code §§ 19.190.005–050 (1998) (repealed 1999).

20. *Id.* at § 19.190.020(1)(a). This is the first instance of a state banning the use of a third party's domain in unsolicited electronic mail without the third party's consent.

21. *Id.* This is the first instance of a state requiring that the header and routing information of an electronic mail message be true and valid.

22. *Id.* at § 19.190.020(1)(b). This is the first instance of a state requiring that the subject line of an electronic mail message not be misleading.

23. Cal. Bus. & Prof. Code § 17538.4 (1998) (repealed 2003).

24. *Id.* at § 17538.4(g). This is the first instance of a state requiring a label ("ADV:") in the subject line for unsolicited electronic mail.

line.[25]

These three initial states are important because, in a span of one year, they drafted the eight key provisions that would form the basis of every subsequent state's anti-spam law.[26] Ordered in what turned out to be the most popular to the least, these eight provisions were: 1) requiring valid routing and no forged header information,[27] 2) mandating a valid opt-out mechanism,[28] 3) forbidding the use of a third party's domain without permission,[29] 4) proscribing a label (typically "ADV:") in the sub-

25. *Id.* This is the first instance of a state requiring an adult label ("ADV:ADLT") in the subject line of unsolicited, pornographic electronic mail.

26. The thirty-six states that enacted anti-spam laws between 1997 and 2004 are: Alaska, Alaska Stat. § 45.50.479 (2003); Arizona, Ariz. Rev. Stat. § 44-1372 (2003); Arkansas, Ark. Code Ann. §§ 4-88-601–607 (2003); California, Cal. Bus. & Prof. Code § 17529 (2003); Colorado, Col. Rev. Stat. §§ 6-2.5-101–105 (2000); Connecticut, §§ 53-451–453 (1999); Delaware, Del. Code Ann. tit. 11 §§ 931, 947–48 (1999); Idaho, Idaho Code § 48-603E (2000); Illinois, 815 Ill. Comp. Stat. § 511 (2000) (amended 2003); Indiana, Ind. Code §§ 24-5-22-1–10 (2003); Iowa, Iowa Code § 714E (1999); Kansas, Kan. Stat. Ann. § 50-6,107 (2002); Louisiana, La. Stat. Ann. §§ 14: 73.1, 14:73.6 (1999); Maine, 10 Me. Rev. Stat. Ann. § 1497 (2003); Maryland, Md. Commercial. Law Code §§ 14-3001–3003 (2002); Michigan, Mich. Comp, Laws §§ 445.2501–445.2508 (2003); Minnesota, Minn. Stat. § 325F.694 (2002); Missouri, Mo. Rev. Stat. §§ 407.1120–407.1132 (2003); Nevada, Nev. Rev. Stat. §§ 41.705–735 (1997) (amended 2003); New Mexico, N.M. Stat. Ann. § 57-12-23 (2003); North Carolina, N.C. Gen. Stat. §§ 14-453, 14-458 (1999); North Dakota, N.D. Cent. Code §§ 51-27-01–09 (2003); Ohio, Ohio Rev. Code Ann. § 2307.64 (2002); Oklahoma, Okla. Stat. tit. 15, §§ 776.1–7 (2003); Oregon, Or. Sen. 910, 72nd Leg. Assembly (effective March 1, 2004); Pennsylvania, 18 Pa. Consol. Stat. § 7661 (2002), 73 Pa. Consol. Stat. §§ 2250.1–8 (2002); Rhode Island, R.I. Gen. Laws §§ 11-52-1–8 (1999), R.I. Gen. Laws §§ 6-47-1–3; South Dakota, S.D. Codified Laws §§ 37-24-1–6 (2002); Tennessee, Tenn. Code Ann. §§ 47-18-2501, 47-18-2502 (1999) (amended 2003); Texas, Tex. Bus. & Com. Code Ann. §§ 46.001–011 (2003); Utah, Utah Code Ann. § 13-36-101–105 (2002); Virginia, Va. Code Ann. § 18.2-152.2–16 (2003); Washington, Wash. Rev. Code §§ 19.190.005–19.190.050 (1998) (amended 1999); West Virginia, W. Va. Code § 46A-6G-1–5 (1999); Wisconsin, Wis. Stat. § 944.25 (2001); and Wyoming, Wyo. Stat. Ann. § 40-12-401–404 (2003). The Federal *CAN-SPAM* Act preempts most existing state anti-spam statutes. It is likely that most of the statutes listed here are either void or severely limited.

27. Twenty-seven states passed a provision requiring valid routing information and no forged headers: Arizona, Arkansas, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Virginia, Washington, and Wyoming. Several of these states went further and banned any software designed to forge headers: Connecticut, Delaware, Kansas, Louisiana, Michigan, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia.

28. Twenty-three states passed a provision requiring a mechanism for recipients to opt-out of future messages: Arizona, Arkansas, California, Colorado, Delaware, Illinois, Indiana, Iowa, Kansas, Maine, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, and Utah.

29. Twenty-one states passed a provision banning the use of a third party's domain in unsolicited electronic mail messages unless the sender has received permission from the domain's owner: Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Ma-

ject line of all unsolicited commercial messages,[30] 5) proscribing a slightly different label (typically "ADV:ADLT") in the subject line of all unsolicited pornographic messages,[31] 6) banning misleading subject lines,[32] 7) obligating senders to include a valid return address,[33] and 8) ordering the inclusion of the sender's physical contact information or telephone number.[34] Mixing and matching these eight common provisions, the remaining thirty-three states crafted their own particular

---

ryland, Michigan, Minnesota, North Dakota, Oregon, Pennsylvania, Rhode Island, South Dakota, Texas, Utah, Washington, West Virginia, and Wyoming.

30. Nineteen states require all unsolicited commercial electronic mail to have a label in the subject line: Arizona, California, Colorado, Illinois, Indiana, Kansas, Maine, Michigan, Minnesota, Missouri, Nevada, New Mexico, North Dakota, Oklahoma, Oregon, South Dakota, Tennessee, Texas, and Utah. "ADV:" as the first four characters in the subject line constitutes the typical label for nearly every state. Nevada allows either "ADV" or "ADVERTISEMENT."

31. Eighteen states required unsolicited pornographic electronic mail to have a special label in the subject line: Alaska, Arkansas, California, Illinois, Kansas, Louisiana, Maine, Minnesota, Missouri, New Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin. While the generic unsolicited electronic mail label ("ADV:") is basically standard from state to state, the "adult" label is not. A majority of states require the first eight characters of a pornographic spam's subject line to be "ADV:ADLT"—the standard California originally established in 1998. However, Louisiana, Minnesota, North Dakota, Oklahoma, and Pennsylvania require a slight variation ("ADV-ADULT"). Arkansas and Utah require "ADV:ADULT" (substituting a hyphen for a colon). Texas requires "ADV: ADULT ADVERTISEMENT" to appear at the beginning of the subject line. Finally, Wisconsin requires the words "ADULT ADVERTISEMENT" to appear somewhere in the message, although not necessarily in the subject line. While these differences may appear typically trivial, they mean that it is technically impossible to create a single message that meets the standards of, for example, Arkansas, Louisiana, Tennessee, and Texas. Since a sender cannot tell from an electronic mail address alone the jurisdiction that applies to the recipient, even theoretical spammers who are sending pornography and trying to follow the law find themselves in an impossible situation. Courts have acknowledged this conflict between adult spam labels. *See Ferguson v. Friendfinders*, 94 Cal. App. 4th 1255, 1265 (1st Dist. 2002). Moreover, this inability to determine what laws apply to which addresses makes the lack of compliance on the part of spammers more understandable and gives spammers a defense that courts have listened to. *See e.g. AOL v. Beyer*, Civ. Act. 30-474-A, Or. Granting Defs.' Mot. to Dismiss 1–4 (Dec. 24, 2003) (spam complaint by AOL against accused Florida spammers dismissed because the court found they had not purposefully availed themselves of the jurisdiction in order to establish personal jurisdiction).

32. Seventeen states ban unsolicited commercial electronic mail messages from containing a misleading subject line: Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, Nevada, North Dakota, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming.

33. Thirteen states require unsolicited commercial electronic mail messages to include a valid return address: Arkansas, California, Iowa, Kansas, Maine, Michigan, Nevada, North Dakota, Oklahoma, Pennsylvania, Texas, Utah, and West Virginia.

34. Seven states require unsolicited commercial electronic mail messages to include the sender's identity in the form of a postal address or telephone number: Arkansas, Kansas, Maine, Michigan, Nevada, Ohio, and Utah.

anti-spam statutes over the next six years.[35] There was little innovation and little creativity, so it is not surprising that universally there has been little success.

It is worth noting that the volume of spam has increased at an astounding rate since these legislative measures were initially crafted. In 1997, mail statistics show that most electronic mail users received less than one spam message *per week*.[36] By 2003, average users reported receiving approximately twenty-five spam messages *daily*, with many receiving several times more.[37] This is in spite of the rapid growth and wide deployment of advanced filtering technology, which was virtually non-existent in 1997.[38] In fact, if you were to remove the filters that protect most users' inboxes today, it is likely that the flood of spam would be crushing. Internet Service Providers ("ISPs") and anti-spam companies agree that spam today constitutes more than half of all electronic

35. There are a couple of notable exceptions. Delaware's anti-spam law establishes a so-called "opt-in" standard. *See* Del. Code Ann. tit. 11 §§ 931, 947–48 (1999). This means that under the state's statute, commercial mailers must receive the permission of a resident of the state before sending a message. The law's enforcement is limited to the state's attorney general who, to this point, has never elected to enforce it. In addition, because it is typically impossible to determine what electronic mail addresses belong to Delaware residents, there is substantial question as to whether the law would survive constitutional challenges under the Commerce Clause, the Due Process Clause, and the First Amendment. *See generally* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L. J. 785, 793–94 (2001). In 2003, California amended its anti-spam law to create an opt-in standard similar to Delaware's. However, under the California law individual consumers were given the right to sue. Before the California law could go into effect, the *CAN-SPAM* law was passed by Congress. The Federal law was given an effective date of January 1, 2004, for the specific purpose of preempting the California law. *See* Roy Mark, *Lawmakers: Spam Bill Is a Turkey*, Internet News <http://dc.internet.com/news/article.php/3113941> (Nov. 26, 2003). Even if it had not been preempted by the Federal law, the California anti-spam statute would likely have been struck down under the Commerce Clause, Due Process Clause, or the First Amendment under the same rationale that would challenge Delaware's law. Both Delaware's law and California's are likely at least substantially preempted by *CAN-SPAM*.

36. *See* Lorrie Faith Cranor and Brian A. LaMacchia, *Spam!*, 41 Communs. of the ACM 8, 76 (Aug. 1998) (available at <http://www.acm.org/pubs/citations/journals/cacm/1998-41-8/p74-cranor/>).

37. *See* InsightExpress and Unspam, *2003 Comprehensive Spam Survey* <http://www.unspam.com/fight_spam/information/survey_personal.html> (updated Oct. 15, 2003).

38. Brightmail, a leading anti-spam filtering company, was founded in 1998. *See Brightmail—Company* <http://www.brightmail.com/about_us.html> (accessed Jan. 20, 2003). SpamAssassin, a widely used anti-spam filter, was first released to the public in 2001 and was only conceived in 1998. *See SpamAssassin PreHistory* <http://spamassassin.org/prehistory/> (updated July 14, 2003). *SpamAssassin History* <http://wiki.spamassassin.org/w/SpamAssassinHistory> (updated Dec. 9, 2003). In fact, the dramatic rise in spam coincides with the spread of filters. It appears that spammers cranked up their volume to overwhelm the new technological protections put in place.

mail traffic;[39] some put the estimate as high as ninety percent.[40] Filters have become our only defense, with America Online ("AOL"), for example, blocking more than one billion messages daily that would otherwise end up in their users' inboxes.[41] Unfortunately, there is no sign that the growth in the volume of spam is slowing.[42]

Legislatively, it is important to keep in mind the astounding rise in the volume of spam. The huge increase shows that in 1997, when our anti-spam laws were first crafted, they were designed around a problem different from the one confronting us today. Back when the provisions were originally envisioned, a few prosecutions may have made a significant dent in the spam problem. From humble beginnings, spam has become a serious business with many players.[43] It is therefore likely to take a much broader legal effort to make any significant impact. This means that in order for spam laws to make an impact on the huge volume of spam and spammers we now face, the laws must be drafted in such a way as to be as cheap and easy to prosecute as possible. If spammers do not face a clear and present risk of liability, then the other fixed costs of entering the business are likely too low to sufficiently deter new entrants from replacing the few that are removed by prosecution.[44] Nevertheless, an important puzzle remains. Even acknowledging that yesterday's laws are incapable of completely solving today's problem, why is

39. *See* Patrick Gray, *Spam Hits Two-thirds of all Email Traffic* (Jan. 12, 2004) (available at <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39117729,00.htm>); Mitch Wagner, *Spam May Overtake E-mail in 2003*, CNN.com (Dec. 12, 2002) (available at <http://www.cnn.com/2002/TECH/biztech/12/12/techweb.email.swamp/>).

40. While fifty percent is probably a more reasonable estimate, some anti-spam companies are estimating spam to be as high as ninety percent of all electronic mail traffic. *See* Frank Catalano, *Spam Wars: Collateral Damage* (Jan. 28, 2004) (available at <http://www.seattleweekly.com/features/0404/040128_news_spam_fight.php>).

41. *See* Wired News, *So Much Spam in So Little Time* (Mar. 6, 2003) (available at <http://www.wired.com/news/business/0,1367,57936,00.html>) (AOL blocks at least a billion messages a day).

42. *See* Anita Ramasastry, *Why the New Federal 'CAN Spam' Law ProbablyWwon't Work*, CNN.com (Dec. 5, 2003) <http://www.cnn.com/2003/LAW/12/05/findlaw.analysis.ramasastry.spam/> (little reason to believe Federal law will stem the tide of spam). In fact, the amount of spam has continued to rise since the *CAN-SPAM* law began being enforced Jan. 1, 2004. *See Postini Anti-Spam Statistics* <http://www.postini.com/> (accessed Jan. 30, 2004); *Impact of CAN-SPAM? Brightmail Finds Spam is Still Flowing*, Brightmail Web site (Feb. 2, 2004) (available at <http://www.brightmail.com/pressreleases/020204_*CAN-SPAM*-impact.html>) (in spite of new law, spam continued to rise in 2004).

43. *See* James Gleick, *Tangled Up in Spam*, N.Y. Times Mag. 42 (Feb. 9, 2003) (article tracks the rise of spam and how spammers today make substantial money plying their trade).

44. *See* Rebecca Lieb, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, May 1, 2003) (a discussion of the economics of spam, and the low barrier to entry into the spam business).

it that with so many targets on the radar screen there have still been virtually no prosecutions?

In order to answer that question, it is instructive to look at the decision process prosecutors go through before they bring a case. At the simplest level, such a decision must be a cost–benefit analysis. Resources are limited so prosecutors weigh the costs of bringing a case against the potential benefit. On the cost side, a prosecutor faces the expenses of tracking down an individual spammer and then taking the case to trial. After these expenses are tallied, a prosecutor must divide them by the likelihood of success at trial and weigh that resulting total against the social benefit that would be derived from a victory.[45] Effectively, the lower the chance a case will be successful, the larger the multiplier on the costs faced by the prosecutor, and the bigger the social benefit must be in order to justify bringing a case. This means that in crafting effective anti-spam legislation, there are four key numbers to keep in mind: 1) the cost of tracking down a spammer, 2) the cost of bringing a trial, 3) the likelihood of success at trial, and 4) the social benefit derived from winning a case.

These are going to be difficult numbers to determine definitively, but we do have some data to work with. Whatever the tally of the costs divided by the perceived chance of success at trial is today, it is generally high enough to outweigh the social benefit prosecutors see in bringing a case. The fact that there have been so few prosecutions under traditional law empirically proves this. However, it must be at least a somewhat close call because a handful of prosecutors have chosen to try to bring cases.[46] In the end, although there are many laws now on the books,

45. Imagine that the expenses of tracking down a spammer amount to $100 and the expenses of bringing a trial amount to $200. The total initial costs a prosecutor faces are $300. If there is a 100-percent chance of victory, then the social benefit of bringing the case needs to be at least $300 in order to justify the prosecutor bringing the case. Put another way: ($100 + $200)/1.0 = Social Benefit. If the chance of a successful prosecution drops to fifty percent, then the social benefit of bringing the case must double in order for the prosecutor to justify bringing the case. This is because, taking into account the chance of victory, the effective costs to the prosecutor have gone from $300 to $600. Again, put another way:($100 + $200)/0.5 = Social Benefit.

46. Several states have tried to file cases against spammers. Only Washington and California have successfully prosecuted cases under an anti-spam law. *See supra* n. 6. However, New York and Arizona have also prosecuted spammers under traditional consumer protection laws. *See* Reuters, *Fraud Bust for 'Buffalo Spammer'* (May 14, 2003) (available at <http://www.wired.com / news / business / 0,1367,58842,00.html>); Mike Brunker, *Anatomy of a Penis Pill Swindle*, MSNBC (June 5, 2004) (available at <http://msnbc.msn.com/id/3077050/>) (spammer nets seventy-four million dollars before being caught by Arizona attorney general). Missouri, Viriginia, and New York have pending spam cases at the time this article goes to press. *See* Brian Morrissey, *Missouri Files First Spam Suits*, InternetNews.com (Oct. 10, 2003) (available at <http://www.internetnews.com/IAR/article.php/3090181>); Roy Mark, *Virginia Hits Spammers With Felony Charges* (Dec. 11, 2003)

they have proven essentially impossible to cost-effectively enforce. Again, remember the old adage: without enforcement there is no law. So if we want the legal system to have any positive effect on the problem of spam, the first step needs to be ensuring that the next-generation statutes are as easy to enforce as possible. To this end, new anti-spam laws must 1) decrease the cost of tracking down spammers, 2) decrease the costs of trial, 3) increase the likelihood of success at trial, or 4) increase the social benefit of a victory. Ideally, they would accomplish all four goals.

III. THE FLAWS OF STATE LAWS

A. High Tracking Costs

Understanding the specifics of existing anti-spam laws from the perspective of the cost–benefit analysis helps explain why the laws have met with such limited success. To begin, there is little in today's cannon of anti-spam law that helps decrease the costs of tracking down a spammer.[47] This is not surprising because, of the four numbers in the cost–benefit analysis, the cost of tracking down a spammer is the hardest for law to influence.[48] The challenge of tracking down a spammer is substantially a technological issue. Just as improvements in crime scene technologies help prosecutors more effectively try murders, the development and deployment of reliable tools and standards to identify the sender of a message will help prosecutors effectively try spammers.[49]

In addition to improvements in technology, there are some steps anti-spam law can take to decrease the cost of tracking down spammers.

(available at <http://www.internetnews.com/IAR/article.php/3288131>); Marguerite Reardon, *Microsoft, New York launch spam lawsuits*, CNET News.com (Dec. 18, 2003) (available at <http://news.com.com/2100-1028-5128806.html>).

47. The manager of the high-tech unit in the Washington State Attorney General's office acknowledged that spam cases are "very labor-intensive" and that "[i]nvestigative resources are drained pretty quickly." *See* Beth Taylor, *Anti-spam Law Fails to Deter Junk-mail Marketers*, Pudget Sound Bus. J. (available at <http://www.bizjournals.com/seattle/stories/2002/12/23/focus1.html>).

48. One proposal that does hold promise for decreasing the cost of tracking down spammers was put forward by Stanford Law professor Lawrence Lessig. *See* Lawrence Lessig, *Code Breaking: A Bounty on Spammers*, CIO Insight (Sept. 16, 2002) (available at <http://www.cioinsight.com/article2/0,3959,1454839,00.asp>). His proposal is for the government to offer bounties for individuals who take the time to track down spammers. *Id.* This seems like a potentially sensible approach that can be grafted onto any other anti-spam provision in order to decrease the cost of tracking spammers. The *CAN-SPAM* Act requires the FTC to study Lessig's bounty-hunting proposal. *See* 15 U.S.C. § 7711(1)(A).

49. This sentiment is reflected by Paula Selis, the Washington State Assistant Attorney General, arguably the prosecutor who has had the most success enforcing any anti-spam law. *See* Selis, *supra* n. 2 (expressing that over time she believes enforcement authorities will get better at tracking down spammers).

Unfortunately, existing statutes have either ignored or directly contravened such measures. For example, if instead of having to trace the individual who actually sent the message the law were written to attach liability to the Internet service provider ("ISP") that hosted and directly facilitated transmission, then the job of the prosecutor would be substantially easier. Identifying the ISPs that host spammers and facilitate their activities is relatively trivial. If a statute were written to impose liability on these ISPs, it would instantly align their incentives with those of the prosecutor, causing ISPs to carefully check their customers' credentials and quickly terminate those whom they find sending unsolicited commercial electronic mail.[50] Instead, several state anti-spam laws take exactly the opposite approach: they specifically exempt ISPs from any liability for the actions of users on their networks.[51] While politically this may make sense,[52] from the point of view of a prosecutor it removes an easy target from the screen and does little to discourage ISPs from helping to hide the identities of spammers.

Another way in which spam law could make tracking spammers easier is to expand under the law who is considered a "spammer." While all spam statutes attach liability to the actual sender of unsolicited electronic mail, they generally do not directly attach liability to businesses knowingly being promoted by the spam. These businesses have contracted with the actual spammers to send out their messages, effectively engaging in a conspiracy.[53] What is important is that it is often much easier to find the businesses being promoted than the person who

50. It is not clear that ISPs incentives are currently aligned this way. In fact, there is some evidence that large and small ISPs are willing to take large payments off the books, known as "pink contracts," from spammers. *See* Paul Festa, *PSINet Assailed as Spam Contract Surfaces*, CNET News.com (Nov. 6, 2000) <http://news.com.com/2100-1023-248211.html>; *see also* Paul Festa, *AT&T Admits Spam Offense After Contract Exposed*, CNET News.com (Nov. 3, 2000) <http://news.com.com/2100-1023-248067.html>.

51. Nineteen states specifically exempt ISPs from liability for the transmission of spam through their network: Arizona, Arkansas, Connecticut, Idaho, Illinois, Indiana, Iowa, Kansas, Maryland, North Carolina, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Virginia, West Virginia, and Wyoming. While there are some rational reasons for not imposing increased costs on ISPs, they are in the best position to identify spammers and take steps to stop them before they gain access to bandwidth to send their messages. Legislators should weigh this benefit in the spam fight against the drawbacks of increasing ISPs' costs and not simply grant blanket immunity for ISPs.

52. Remember that large ISPs were the primary lobbyists for traditional anti-spam laws. *See supra* n. 5.

53. A case for traditional conspiracy theory law can likely be made, but it is easier when the statute directly reflects the law. Moreover, a statute drafted in this way would clearly put businesses on notice that hiring an agent to do your spamming for you does not absolve you of liability.

presses the send button to deliver the promotion.[54] If a statute were to make businesses liable for contracting with spammers, the law could substantially dry up the demand for spammers' services. Unfortunately, most existing anti-spam laws have not taken this approach.[55] The result is that prosecutors are typically forced to track down the actual sender rather than begin prosecutions with the lower-hanging fruit.

Again, while it is difficult for the law to help decrease the cost of tracking down spammers, it is important to note that most existing anti-spam laws do not even take the few steps possible to help. Going forward, this will remain the most difficult number in the cost–benefit equation for legislation to positively influence. However, legislators should remain cognizant that when drafting new laws it is always important to, at the very least, do no harm and, whenever possible, provide tools to prosecutors in order to help track down and identify all the parties responsible for sending spam.

B. The Cost of Trial and Likelihood of Its Success

The next two numbers in the cost–benefit equation are the cost of prosecuting a trial and the likelihood of success at that trial. Similar considerations affect both these numbers: driving up the costs of prosecution and driving down the likelihood of success, or, hopefully, vice versa. It makes sense, therefore, to consider the factors that affect these two numbers in tandem. The cost of trial and its chance of success are affected first by the actual provisions of the various laws, and second by constitutional limitations imposed over the law.

---

54. These individuals are often easier to track down and prosecute because their business requires them to have a physical presence. They must have a mechanism to collect money from customers, they often have to have a place to fulfill orders, often have a stable Web site, and generally have a more difficult time moving their operations. In fact, a recent study by Microsoft found that at least sixty-two percent of spam messages advertised products that needed to be based in the United States in order to be commercially viable. *See* Geoff Hulten, MIT Spam Conference, *Filtering Junk Mail on a Global Scale*, (MIT Room 26-100, January 16, 2004) <http://www.spamconference.com/> (accessed Jan. 30, 2004). Examples of these products that require a domestic presence in order to be spam-advertised include the likes of financial services, insurance services, herbal supplements, college diplomas, magazines, etc. *Id.* On the other hand, some products such as pornography and software, as well as most spam-based frauds, do not require a domestic presence. *Id.* As a result, it is likely that these non-domestic spam messages will always present the greatest problem to prosecutors in terms of tracking them down and stopping them.

55. While state anti-spam laws have generally not included such a provision, there is some hope on the Federal level. Sen. McCain (R-AZ) introduced an amendment to the *CAN-SPAM* Act that allows prosecutors to file charges against the individual whose products are being advertised by the spam message if they knowingly used the spammer as their agent. *See* 15 U.S.C. § 7706.

1. *Expensive Statutory Choices*

In terms of the actual provisions, existing anti-spam laws have made a number of choices that make the prosecutor's job extremely difficult. The most popular provision of state anti-spam law has been to ban the transmission of fraudulent header information.[56] But what is "fraudulent header information"? At trial this is almost certain to be a question of fact that must be presented to a jury. That, in turn, means prosecutors have to explain to a jury what an electronic mail header is and, at least to a limited extent, how the SMTP protocol works.[57] This poses quite a challenge even for a technically savvy prosecutor. Moreover, existing laws often require prosecutors to prove "fraud," a relatively burdensome standard.[58] For instance, compare these requirements to those mandated for enforcement of do-not-call legislation.[59] Under do-not-call statutes, states must simply answer three questions at trial: 1) was the victim of the solicitation's phone number on the list? 2) did the victim receive the phone call? 3) was there any preexisting relationship that entitled the defendant to place the call? States have been extremely successful in enforcing their do-not-call laws in part because the cases are factually easy to prove and can often be resolved by summary judgment motion and without impaneling a jury.[60] Anti-spam cases, by contrast,

56. *See e.g.* Rhode Island, R.I. Gen. Laws § 6-47-2 (the statute bans any message that "fraudulently misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message").

57. While SMTP stands for "Simple Mail Transfer Protocol," it is hardly "simple" for the average juror (or prosecutor) to understand. The protocol is the *de facto* standard for electronic mail transmission across the Internet. It regulates what is included in an electronic mail message, including the transmission and routing information. Spammers often insert incorrect data into the transmission information in order to hide their identity. *See* Jon Praed, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, May 2, 2003).

58. A finding of fraud typically requires a prosecutor to prove: 1) a false representation 2) of a fact 3) that is material and 4) made with knowledge of its falsity and the intention to deceive and 5) which representation is justifiably relied on. *See* W. Page Keeton, et. al., *Prosser and Keeton on the Law of Torts* §§ 107-09 (5th ed. 1984). This is a higher standard than is typically required by most consumer protection laws. *See* Selis, *supra* n. 2 ("since spam is the number one consumer complaint these days, why give spammers what essentially amounts to a lower burden than a higher one?").

59. This is an appropriate comparison as do-not-call laws also are designed to protect consumers from unwanted communication and were developed along the same timeline as anti-spam laws. In 1997, there was only one do-not-call law (Florida) and one anti-spam law (Nevada). Six years later there are forty-two do-not-call laws and thirty-six anti-spam laws.

60. Paula Selis, the Washington State Assistant Attorney General, made this point at the FTC's Spam Forum: "[W]hen we created a do-not-call list what it did for us is that . . . it enables us to go in and file what's called a summary judgment motion. We didn't have to prove anything, all we had to show was that Joe Blow's name was on the list, he got the call . . . judgment in favor of the state." *See* Selis, *supra* n. 2.

are factually difficult to prove and therefore create far more challenging trials for prosecutors.

Additional standard provisions of traditional anti-spam laws also place a difficult burden on prosecutors. As discussed above, many laws mandate that messages contain a mechanism whereby individuals can opt out of future solicitations and that messages be sent with a valid return address. Both of these provisions put prosecutors up against the clock. An opt-out mechanism may or may not have worked at the moment the message was sent out, but months later an investigator looking into a spam complaint has no way to know for sure.[61] Evidence in a spam case quickly becomes stale, and prosecutors do not necessarily have the mechanism or the means to preserve it adequately. This almost inevitably gives spammers a potential defense.[62]

Finally, nearly every state anti-spam law allows commercial marketers to send messages to individuals with whom they have a "preexisting business relationship."[63] Spammers regularly claim recipients have in fact opted in to their solicitations, thereby establishing a "business

---

61. A version of this basic concern was specifically expressed by eight state attorneys general in a letter urging Congress to not pass the *CAN-SPAM* Act. *See* Letter from Christine O. Gregoire, Wa. Atty Gen, et. al., S.877, *The CAN-SPAM Act of 2003* (Nov. 4, 2003) (available at <http://www.epic.org/privacy/junk_mail/spam/agltrs877.pdf>) (signed by the attorneys general of California, Kansas, Maryland, Nevada, Texas, Vermont, Virginia, and Washington).

62. Even legitimate electronic mail marketers have begun to speculate about this as they look into the requirements of complying with *CAN-SPAM*. A direct marketing magazine explained to its readers:

> When you send commercial e-mail with an opt out, see to it that the mailbox for opt outs is small or full before the campaign begins. When people opt out, their messages will bounce, but they probably will not have the interest to keep pursuing the opt out. . . . If the FTC comes sniffing around in a year or two, apologize, plead incompetence and promise to clean up your act. The commission likely will let you off the hook cheap. Just don't circle this paragraph and leave a copy in your files.

Robert Gellman, *Don't Pin Enforcement Hopes on FTC*, DMNews (Jan. 28, 2004) (available at <http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=26324>).

63. *See e.g.* Ohio Rev. Code Ann. § 2307.64(A)(9):

> 'Pre-existing business relationship' means that there was a business transaction between the initiator and the recipient of a commercial electronic mail message during the five-year period preceding the receipt of that message. A pre-existing business relationship includes a transaction involving the free provision of information, goods, or services requested by the recipient. A pre-existing business relationship does not exist after a recipient requests to be removed from the distribution lists of an initiator pursuant to division (B) of this section and a reasonable amount of time has expired since that request.

10 Me. Rev. Stat. Ann. § 1497(1)(C): "'Unsolicited commercial e-mail' means an e-mail, other than an e-mail sent at the request of the recipient, sent via an e-mail service provider to 2 or more recipients in this state with whom the sender does not have an existing business relationship. . . ."

relationship."[64] At trial, determining whether they are telling the truth is an extremely fact-intensive inquiry that once again is likely to require substantial costs on the part of the prosecution. Unfortunately, under traditional anti-spam law this appears unavoidable. The definition of "spam" that most people agree on is an unsolicited commercial electronic mail message where the sender and recipient do not have a preexisting business relationship.[65] Legislators are loathe to limit legitimate businesses from communicating with their existing customers.[66] Still, if there were a way to draw a brighter line, states could save substantial costs and thereby make prosecution much more likely.

It should be noted that at most trials a prosecutor would likely be able to demonstrate a pattern sufficient to show illegal behavior. However, this misses much of the point. The issue is not exclusively whether the prosecutor can win in the end. Instead, what is initially important is that uncertainty under these laws serves to drive up the cost of prosecutions and drive down their chance of success. As a result, prosecutors running the cost–benefit analysis on a potential case under traditional anti-spam law find the scale naturally tips away from filing a prosecution.[67] Until prosecutors feel comfortable bringing cases, there is no way the law will make any progress controlling spam.

2. *Constitutionally Imposed Burdens*

In addition to the statutory choices that have driven up the costs of prosecution under traditional state anti-spam laws, constitutional requirements limit states' ability to regulate unsolicited electronic mail. Like the statutory hurdles, these concerns may not stand as absolute bars on enforcing existing state anti-spam law; nevertheless, they will inevitably be raised by nearly every spammer who faces prosecution.[68]

64. *See* Timothy Muris, FTC Chairman, Opening Remarks, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, April 30, 2003).

65. *See* InsightExpress and Unspam, *2003 Comprehensive Spam Survey*, <http://www.unspam.com/fight_spam/information/survey_general.html> (updated Oct. 15, 2003).

66. *See* Tim Lemke, *Congress Pressured on E-mail*, Wash. Times (Nov. 17, 2003) (available at <http://washingtontimes.com/business/20031116-111217-2114r.htm>).

67. You can hear this natural tendency when you listen to law enforcers talk about their priorities. As Paula Selis, Assistant Attorney General for the State of Washington, stated at an FTC forum on spam, "[t]here are a lot of criminal cases out there , and when you are facing . . . property crimes versus physical crimes versus terrorism and you have to choose among them because you have limited resources, what oftentimes happens is that you're going to go to the more serious crimes first." Selis, *supra* n. 2.

68. In fact, spammers have raised these arguments and have met with some success defeating claims. *See e.g. AOL v. Beyer*, Civ. Act. 30-474-A, Or. Granting Defs.' Mot. to Dismiss 1–4 (Dec. 24, 2003) (spam complaint by AOL against accused Florida spammers dismissed because the court found they had not purposefully availed themselves of the jurisdiction in order to establish personal jurisdiction); *see also Washington v. Heckel*, No. 98-2-25480-7, 36 (Wash. Super. Ct. Mar. 10, 2000) (oral transcript) (recognizing that the

This further increases the cost of a trial and drives down the likelihood of success. Consequently, prosecutors are less likely to bring a case when they weigh the cost-benefit equation.

The constitutional concerns stem from three areas of the Constitution: 1) the Due Process Clause,[69] 2) the Commerce Clause,[70] and 3) the First Amendment.[71] The first two areas present a problem for the same reason. Electronic mail addresses are jurisdictionally anonymous. This means that from an address alone it typically is impossible to tell where its user is located and what jurisdiction's laws apply.[72] The problem is reminiscent of the often-reproduced Peter Steiner cartoon that appeared in *The New Yorker* magazine.[73] The cartoon depicts two dogs sitting in front of a computer. One dog says to the other, "On the Internet, nobody knows you're a dog." While the cartoon is an amusing commentary on the anonymity afforded by the Internet, it more importantly illustrates a problem faced by prosecutors attempting to enforce state anti-spam laws. When spammers send messages to a particular electronic mail ad-

---

electronic mail addresses do not "recognize geographical boundaries"); *Washington v. Heckel*, No. 98-2-25480-7, 2000 WL 979720, 1 (Wash. Super. Ct. Mar. 10, 2000) (order granting summary judgment) (commerce clause argument raised by accused spammer arguing he could not tell the jurisdiction that applied to a particular electronic mail address). The Washington Supreme Court eventually overturned the lower court's decision in *Heckel*. *Washington v. Heckel*, 24 P.3d 404 (2001). However, part of the reason for that was the establishment of a registry of electronic mail addresses that exist within the state of Washington by the Office of the Attorney General. *Id.* at 411 (registry available at <http://registry.waisp.org/>) (accessed Jan. 30, 2004).

69. U.S. Const. amend. XIV, § 1. "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of laws." *Id.*

70. U.S. Const., Art. I, § 8, cl. 3 reads in relevant part: "The Congress shall have Power . . . to regulate Commerce . . . among the several States." The restriction on a state's power to regulate interstate commerce is often said to fall under the "dormant Commerce Clause." *Gibbons v. Ogden*, 22 U.S. 1 (1824) (Supreme Court's first suggestion of the "dormant" Commerce Clause).

71. U.S. Const., Amend. I reads in relevant part: "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."

72. Imagine the electronic mail address spamlawyer321@hotmail.com. From that information alone, where is the user of that electronic mail address located? More importantly, whose jurisdiction applies? Is it Redmond, Washington, where Microsoft, the owner of Hotmail, is headquartered? Is it Santa Clara, California, where Hotmail's servers are primarily located? Is it Chicago, Illinois, where one of the authors of this article resides, or Salt Lake City, Utah, where the other author lives? This jurisdictionally anonymous nature of electronic mail creates a number of constitutional and enforcement problems. This is true on the state level, but also on the federal level. Hotmail users can be located in any country in the world. Moreover, a European AOL address looks identical to one based in the United States.

73. Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, 69 The New Yorker 20, 61 (July 5, 1993).

dress, they have no way of knowing what state's jurisdiction they are targeting. Put another way, the cartoon's tagline could read: "On the Internet, nobody knows you're a Utahan." Marketers sending a message to a particular electronic mail address have not *purposefully directed* their messages into any particular jurisdiction. As a result of this jurisdictional anonymity, most spammers simply ignore the law and plead that they have no way to comply. Alternatively, a hypothetical law-abiding spammer[74] finds the only way to ensure compliance with the law is to choose the state with the strictest requirements and apply those requirements to every message sent. Both of these scenarios create problems for prosecutors under the Constitution.

First, under the Due Process Clause, the Constitution requires that in order to be subject to a state's laws an individual must have minimum contacts with the prosecuting state.[75] Interpreting this requirement in light of the Internet, courts have held that a state can only assert personal jurisdiction if a defendant has "purposefully directed" communications into the forum state.[76] In the context of anti-spam laws, if spammers cannot determine the location of recipients based on their electronic mail addresses, then a court is unlikely to find spammers have met this requirement.[77] As a result, at trial a spammer is likely to mount a defensible constitutional challenge when prosecuted under traditional anti-spam laws. Again, even if the defense is not ultimately successful, fighting a constitutional challenge drives up the costs of a prosecution and drives down the likelihood of success.

Similar analysis applies to the Commerce Clause.[78] Remember from above that since it is impossible to determine the jurisdiction of

74. Hypothetical because, at this time, it is not clear that such a creature exists.

75. *See Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476 (1988) (holding that in order to be subject to a state's jurisdiction a commercial actor's efforts are "purposefully directed" toward that state); *see also Intl. Shoe Co. v. Washington*, 326 U.S. 310 (1945); *Miller Brothers Co. v. Maryland*, 347 U.S. 340, 344-45 (1954).

76. *See e.g. Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 419 (9th Cir. 1997) (holding that in order to assert jurisdiction an online business must do more than send mere solicitations); *Gator.com Corp. v. L.L. Bean, Inc.*, 341 F.3d 1072 (9th Cir. 2003) (holding that an online business must be substantially interactive in order to have jurisdiction attach); *see also Quill Corp. v. North Dakota*, 504 U.S. 298 (1992) (applying personal jurisdiction standards requiring substantial contacts to the mail-order business, as close to a personal jurisdiction case involving an Internet-based business as the Supreme Court has come).

77. Lack of personal jurisdiction is the ground on which a court recently dismissed a case brought by AOL against alleged Florida spammers who sent messages into Virginia. *See AOL v. Beyer*, Civ. Act. 30-474-A, Or. Granting Defs.' Mot. to Dismiss 1–4 (Dec. 24, 2003).

78. *See e.g.* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L. J. 785, 786–87 (2001) ("the dormant Commerce Clause argument, if accepted, threatens to invalidate nearly every state regulation of Internet communications").

recipients based on their electronic mail addresses, the only way for a hypothetical law-abiding spammer to guarantee compliance with the law is to pick the state with the strictest standards and apply those to every message. The result of this is that the state with the strictest laws can effectively legislate beyond its borders and set the national standard for spam.[79] This assumes state requirements are not in conflict with one another. If they are conflicting, it can make compliance literally impossible.

A perfect example of this situation exists in the context of anti-spam law. The state of Missouri requires any unsolicited messages containing pornography to be labeled with a subject line containing "ADV:ADLT" as the first eight characters.[80] Pennsylvania, on the other hand, requires any pornographic spam to be labeled with a subject line containing "ADV-ADULT" as the first nine characters.[81] Finally, Texas requires the phrase "ADV: ADULT ADVERTISEMENT" to begin the subject line of any messages containing pornography.[82] It is technically impossible to construct one electronic mail message containing pornography that complies with all three state laws. Combine this with a sender's inability to determine the jurisdiction that applies to an electronic mail address, and these state laws create an inconsistency that makes compliance impossible. Courts have regularly held that state laws effectively regulating beyond the state's borders, or laws that create irreconcilable conflicts between state regulations, are disallowed under the Commerce Clause.[83] Again, these constitutional defenses drive up the costs of an anti-spam trial and drive down its likelihood of success.

There is one qualification worth mentioning. Both the Due Process Clause and the Commerce Clause analyses do not apply to intra-state spam. Having established domicile in a state, spammers have purposefully availed themselves of the jurisdiction and can thereby be subject to

79. In other Internet contexts, courts have recognized this as a problem. For example, in *American Libraries Assn. v. Pataki*, the New York court held that allowing state regulation of Internet content risks "a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed." 969 F. Supp. 160, 168–69 (S.D.N.Y. 1997).

80. Mo. Rev. Stat. § 407.1144(3).

81. 18 Pa. Consol. Stat. § 5903(c)(2).

82. Tex. Bus. & Com. Code Ann. § 46.003(1).

83. The Supreme Court regularly strikes down state laws that would create an inconsistent patchwork of state laws that are difficult or impossible for interstate operators to comply with. *See e.g. Kassel v. Consol. Freightways Corp.*, 450 U.S. 662 (1981); *Raymond Motor Transp., Inc. v. Rice*, 434 U.S. 429 (1978); *Bibb v. Navajo Freight Lines, Inc.*, 359 U.S. 520 (1959); *S. Pac. Co. v. Arizona*, 325 U.S. 761 (1945). In addition, the Court has upheld several instances of state laws that have a burdensome effect beyond a single state's borders. *See e.g. Healy v. Beer Institute*, 491 U.S. 324 (1989); *Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth.*, 476 U.S. 573 (1986); *Edgar v. MITE Corp.*, 457 U.S. 624 (1982); *see also American Libraries*, 969 F. Supp. 160 (S.D.N.Y. 1997).

its laws.[84] Moreover, interstate commerce is not implicated if an in-state spammer sends to an in-state resident.[85] This explains why nearly all of the few successful prosecutions have been by attorneys general bringing cases against their own state's resident spammers.[86] While it appears possible to enforce traditional anti-spam laws more easily against intra-state spam, clearly it is less than ideal. Relying on intra-state-only prosecution overly limits a prosecutor's potential targets and allows spammers to forum shop for a state where the political will is such that they will not face prosecution. Effectively, this raises the cost of tracking down a spammer and substantially reduces the likelihood that a prosecutor will be willing to bring a case.

In addition to the Due Process Clause and the Commerce Clause, one constitutional concern remains: the First Amendment. In spite of this being the least persuasive defense of the three, the First Amendment is likely to be raised by every defendant.[87] Again, the result is that even if the defense is not completely successful, it increases the costs of prosecution and drives down the likelihood of success. In the leading case on the issue, the Supreme Court was reluctant to allow regulation of speech delivered via the Internet because "[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident' . . . odds are slim that a user would come across a sexually explicit sight by acci-

84. Personal jurisdiction is always established in a defendant's home state. *See Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

85. One example comes from the California case of *Ferguson v. Friendfinders*. 94 Cal. App. 4th 1255 (1st Dist. 2002). The California court held that the state's statute applied only to "e-mail users who send [spam] to California residents via equipment located in California." *Id.* at 1264–65. As a result, the *Ferguson* court held the dormant Commerce Clause was not implicated by California's anti-spam statute when applied against in-state spammers. *Id.* at 1265.

86. The California Attorney General brought a successful prosecution against an in-state spammer under the state's anti-spam law. *See supra* n. 6. In addition, attorneys general in New York and Arizona have received judgments against in-state spammers, although under traditional consumer protection, not specifically anti-spam law. *Id.* The notable exception is the state of Washington. In *Washington v. Heckel* the Washington State Attorney General against an Oregon defendant. 24 P.3d 404 (Wash. 2001), cert. denied, 534 U.S. 997 (2001). The Washington Supreme Court upheld the state's statute in part because the state provided spammers a mechanism for verifying what electronic mail addresses belonged to Washington residents through a registry. *Id.* at 411 (registry available at <http://registry.waisp.org/> (accessed Jan. 30, 2004)).

87. *See e.g. Fox v. Reed*, No. 99-3094 (E.D. La., Mar. 15, 2000) (accused spammer not only raised First Amendment claim, but sued the prosecutors for violating civil rights by abridging his free speech). The risk of the First Amendment challenge being raised has only increased after a recent California Supreme Court decision defending the right of a sender to communicate unsolicited, although not commercial, electronic mail. *See Intel v. Hamidi*, 71 P.3d 296 (Cal. 2003) (defendant not liable for trespass of plaintiff's electronic mail servers due to First Amendment right to send communications).

dent."[88] This general tendency by the Court has prompted some commentators to speculate that anti-spam laws would be struck down as in violation of the First Amendment.[89] However, upon reading the Court's analysis it is immediately clear that it does not apply to spam, which, by definition, appears unbidden and often contains sexually explicit content.[90] Unfortunately, even though the state is likely to triumph, a First Amendment challenge will be determined on a case-by-case basis.[91] For example, while states regulating pornographic spam may be afforded more leeway, when states target mortgage spam they may not.[92] This, like the other constitutional challenges, turns what needs to be a simple, easy prosecution into an expensive, difficult trial. In the end, although it is unlikely to be a broadly successful defense, the fact that there is some uncertainty under the First Amendment further raises costs.

C. The Social Benefit to Prosecuting a Spammer

Thus far, this article has examined only the cost side of the prosecutor's cost–benefit equation. Lowering costs is important to increase the likelihood of prosecution, but it is also possible to raise the potential social benefit and achieve the same result. Murder prosecutions, for instance, are generally very expensive, yet prosecutors believe the social benefit is important enough that they are willing to bear the high cost.[93] In the spam context, legislatures have attempted to increase the social benefit of a prosecution by increasing the penalties imposed on spam-

88. *Reno v. ACLU*, 521 U.S. 844, 886–87 (1997).

89. *See* R. Jonas Geissler, *Whether 'Anti-Spam' Laws Violate The First Amendment*, 2001 J. Online L. art. 8 (2001); *see also* Center for Democracy and Technology, *A Briefing On Public Policy Issues Affecting Civil Liberties Online*, 7 CDT Policy Post 4 (June 1, 2001) (available at <http://www.cdt.org/publications/pp_7.04.shtml>).

90. It appears generally accepted that anti-spam laws would survive a First Amendment challenge. *See e.g.* Joshua A. Marcus, *Commercial Speech on the Internet: Spam and the First Amendment*, 16 Cardozo Arts & Ent. L.J. 245 (1998). The labeling requirements are likely at the greatest risk of being struck down under the First Amendment, although even these are generally applied only to commercial speech, which enjoys a lower standard of protection. *Id.* at 258.

91. *See e.g. Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 601–602 (1982) (holding that First Amendment cases need often be decided on a case-by-case basis, especially when the interest of a minor or other vulnerable groups is at stake).

92. *Id.* at 602.

93. This issue has been examined at length when comparing capital murder trials versus those where the death penalty is not sought. Even though capital murder trials are significantly more expensive to bring, and less likely to succeed, prosecutors still decide to bring them because they decide the social benefit is worth the increased costs. *See e.g.* Samuel R. Gross, *ABA's Proposed Moratorium: Lost Lives: Miscarriages of Justice in Capital Cases*, 61 Law & Contemp. Prob. 125 (1998).

mers found guilty of violating the law.[94] Spammers, however, are generally "judgment proof," and even with a successful prosecution, a state is unlikely to recover much of the judgment awarded.[95] As a result, while on paper the potential social benefit per prosecution has increased, in practice the increases in fines have done little to encourage prosecutions.

However, the social benefit of a prosecution is not merely derived from fines. Each spammer eliminated from the network has a value to every legitimate electronic mail user. Quantifying that value, unfortunately, seems prohibitively difficult. Studies have estimated the general cost of spam to businesses,[96] and certainly prosecutors would quickly bring a case if they thought it could cure the entire problem. But, this business-centered characterization discounts the problem and may actually make prosecutors less likely to bring a case. Spam is typically portrayed as little more than an annoying, if pervasive, nuisance.[97] Even

94. For example, in 1997 when Nevada passed the first anti-spam law the fine per message received in violation of the statute was ten dollars. By 2003, when Michigan passed its anti-spam law, the fines in new statutes had increased to $500 per message received in violation of the statute. Mich. Comp, Laws § 445.2504(b)(i). In addition, Michigan and Virginia have mandated criminal penalties, including jail time, for certain offenses. *See* Mich. Comp, Laws § 445.2507(1)–(2); Va. Code Ann. § 18.2-152.3:1(B).

95. *See* Jon Praed, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, May 2, 2003) (AOL's anti-spam attorney said that by the end of a prosecution spammers "can't write a big check" to pay the judgment); *see also* Deborah Scoblionkov, *Washington Nabs A Spammer*, Wired News (Oct. 23, 1998) (available at <http://www.wired.com/news/politics/0,1283,15786,00.html>) (one defendant prosecuted by the State of Washington was effectively bankrupted by the trial).

96. *See e.g.* Jay Lyman, *Spam Costs $20 Billion Each Year in Lost Productivity*, TechNewsWorld (Dec. 29, 2003) (available at <http://www.technewsworld.com/perl/story/32478.html>) (citing a Basex study estimating annual cost of spam at $20 billion to U.S. businesses); Paul Roberts, *Report: Spam Costs $874 per Employee per Year*, InfoWorld (July 1, 2003) (available at <http://www.infoworld. com/article/ 03/07/01/HNspamcost_1.html>) (cites Nucleus Research study finding spam costs the average company $874 annually); Associated Press, *Study: Spam costs Businesses $13 Billion*, CNN.com (Jan. 5, 2003) <http://www.cnn.com/2003/TECH/biztech/01/03/spam.costs.ap/> (citing a Ferris Research study finding the cost of spam to U.S. businesses is $8.9 billion annually).

97. Even as politicians pass laws against spam, it is generally described as a "nuisance" rather than a serious problem. *See e.g.* John Leyden, *UK Govt Fouls up Anti-Spam Plans, Say Experts*, The Register (Sept. 18, 2003) (available at <http://www.theregister.co.uk/content/6/32914.html>); *How to fight the nuisance: Four-step program*, Atlanta Journal Constitution (Dec. 16, 2003) (available at <http://www .ajc.com/business/content/business/1203/16spamsites.html>). The public's perception of spam seems almost schizophrenic. The distinction appears to be that while general commercial messages appear to be viewed as merely a nuisance, explicit adult messages often upset electronic mail users enough to change their entire perception of the problem. *See* Deborah Fallows, *Spam: How it is Hurting E-mail and Degrading Life on the Internet*, Pew Internet & American Life Project (Oct. 22, 2003) <http://www.pewinternet.org/reports/toc.asp?Report=102>. The difference between the percentage of users bothered by pornographic spam and those bothered by any other type of solicitation is substantial. *Id.* at 29. In fact, the Pew study concludes: "So extreme was the reaction to pornography that eliminating it alone among all unsolicited

when its costs are tabulated, they are quantified as business expenses that can be solved with investment in better filtering technology.[98] Prosecuting one spammer in one jurisdiction is seen as a mere drop in the bucket because it will do little to decrease the costs to businesses overall.[99] Because no spammer is responsible for a substantial percentage of the economic damage, and the damage is only seen as economic, under the current characterization there is little perceived social benefit from filing a single case.[100]

Saving businesses a few dollars is hardly the sort of problem that sets a prosecutors' blood boiling.[101] Compare the generic characterization of the spam problem under traditional anti-spam laws with the promises delivered by legislators when they originally announce those laws. Politicians promise to protect children from explicit pornography, the elderly from scams and fraud, and teachers from distractions within their classrooms.[102] All of these are laudable goals with high social benefits, the sort of causes that would almost certainly motivate prosecutors to file cases. But, in the end, the traditional anti-spam laws have applied equally to every type of electronic mail user. As a result, any teeth the law may have had are by necessity filed dull.

Paradoxically, part of the answer to the puzzle presented earlier of how to get prosecutors to bring a case may be that the next generation of anti-spam law needs to limit its focus to particular types of spam and particularly vulnerable electronic mail users. With that in mind, the

---

electronic mail would go a long way toward softening spam's negative impact on Internet users." *Id.* at 42.

98. *See e.g.* Saul Hansell, *Diverging Estimates of the Costs of Spam*, N.Y.Times (July 27, 2003) (available at <http://www.nytimes.com/2003/07/28/technology/28SPAM.html>); Robert Jaques, *Spam Will Cost Business $20.5bn This Year*, Vnunet.com (June 10, 2003) (available at <http://www. vnunet.com/ News/1141508>).

99. There is no evidence, for example, that the amount of spam entering Washington state has decreased after the state's successful prosecutions. *See* Ellen Perlman, *The E-Mail Mess*, Governing.com (Jan. 2004) <http://governing.com/articles/1spam.htm>.

100. As the Washington state Assistant Attorney General explains: "[T]he question is what the competing problems that those prosecutors are having to grapple with—budgets, other cases that involve physical crimes as opposed to property crimes." Selis, *supra* n. 2.

101. *See* Selis, *supra* n. 2 (With regard to enforcing spam law, Assistant Attorney General Selis said: "It's all well and good to have a law on the books [but] the perception, unfortunately, is that the big guys . . . might be able to take care of themselves in the civil arena").

102. *See e.g.* 149 Cong. Rec. S 15938, 15947 (daily ed. Nov. 23, 2003) (Sen. Leahy speaking on the importance of the *CAN-SPAM* Act for protecting children); 149 Cong. Rec. S 13012, 13032 (daily ed. Oct. 22, 2003) (Sen. Dorgan speaking about the important impact anti-spam law has on protecting children); *see also* Sen. Charles Schumer, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, April 30, 2003) (speaking about his children and using the Internet for their schoolwork when introducing Senate Bill 1231 at the FTC Forum).

next section of the article turns its attention to one such proposal: a Children's Protection Registry.

IV. THE NEXT GENERATION: A CHILDREN'S PROTECTION REGISTRY

If states wish to remain relevant in the fight against unwanted electronic messages, they must pass laws that overcome the challenges that have prevented existing anti-spam statutes from being enforced. A Children's Protection Registry holds this promise. Such a measure increases the social benefit of prosecuting a spammer, increases the likelihood of a prosecutor's success at trial, decreases the costs of bringing that trial, and, if properly drafted, can even decrease the cost of tracking down spammers. As a result, unlike previous anti-spam laws, prosecutors will be more likely to enforce a Children's Protection Registry statute. Enforceability is the essential first step to any effective law. This is especially true with a problem like spam, which, in order for law to affect, will require a number of small and rapid strikes by prosecutors. Finally, while the name suggests such a Children's Protection Registry would only protect children, it is important to remember that spammers who are sending messages to kids are also targeting the rest of us. If children's electronic mail addresses are effectively designated legal landmines for spammers, then the net protection afforded by the registry could be broader than it originally appears.

This section discusses the details of a Children's Protection Registry. First, it walks through a model proposal and discusses its critical features. Second, it evaluates the proposal with the prosecutor's cost–benefit analysis equation in mind. Attention is paid to the problems that existing anti-spam laws have faced and the ways in which this next-generation proposal addresses them. Finally, this section examines the additional benefits, and any potential drawbacks, of such a registry.

A. Model Legislation

The model legislation proposed herein[103] is designed first and foremost with one goal in mind: to encourage as many effective spam prose-

103. TITLE I—PROTECTION OF CHILDREN FROM INAPPROPRIATE MESSAGES
SEC. 101. ESTABLISHMENT OF THE CHILDREN'S PROTECTION REGISTRY

(a) IN GENERAL—The Office of the Attorney General shall establish a Children's Protection Registry (referred to in this section as the 'Registry') in which any Contact Points to which children may have access may be registered by a parent or legal guardian as off limits from certain categories of commercial messages (as defined below).

(b) REGISTRATION BY PARENT—The Attorney General shall permit a parent, legal guardian, or other person with control or authority over Contact Points to which minor children have access to register those Contact Points with the registry.

cutions as possible. Having witnessed the failure of traditional anti-spam laws because prosecutors do not believe the cost–benefit analysis weighs in favor of bringing a case, the model statute takes a completely different approach. In creating a Children's Protection Registry, the in-

---

(c) REGISTERABLE CONTACT POINTS—The registry may contain entries for the following kinds of Contact Points: (1) electronic mail addresses, (2) instant message identities, (3) telephone numbers, or (4) facsimile numbers.

(d) THE ADDITION OF NEW TYPES OF CONTACT POINTS—The Office of the Attorney General may, from time to time and as messaging technology develops, designate additional types of Contact Points that may be listed on the Registry.

(e) PROHIBITION ON INITIATING INAPPROPRIATE COMMERCIAL MESSAGES TO REGISTERED CONTACT POINTS—Except as otherwise authorized by the Attorney General in regulations prescribed under this section, it shall be unlawful for a person to initiate any message or other communication, or contract with a third party to initiate such a message or communication, to any registered contact point if the message or communication:

(1) advertises products or services that a minor child is prohibited by law from purchasing, or

(2) contains or advertises adult content or links to such content.

(f) COMPLIANCE—The actual or implied consent given by the minor does not create a defense to liability under paragraph 101(e).

(h) FEES—The Office of the Attorney General shall include in its regulations a method for assessing fees on marketers for use of the Registry that are sufficient to establish, administer, and maintain the Registry.

SEC. 102. ENFORCEMENT

(a) REPORTING OF VIOLATIONS—For purposes of the enforcement of paragraphs 101(e), the Office of the Attorney General shall establish procedures to permit the reporting of violations of this section, including appropriate links on the Internet web site of the Attorney General and the use of a toll-free telephone number (commonly referred to as an '800 number') for such purposes.

(b) CRIMINAL PENALTY—

(1) IN GENERAL—The violation of this act shall be considered a computer crime. The Attorney General may impose a criminal penalty of up to 3 months in jail and $10,000 in fines for each violation of paragraph 101(e). For purposes of this paragraph, each message in violation of paragraphs 101(e) shall constitute a separate offense.

(2) UNAUTHORIZED USE OF REGISTRY—The Commission may impose a criminal penalty of up to 1 year in jail and $500,000 in fines for each unauthorized use of the Registry.

(c) CIVIL PENALTY—

(1) PRIVATE ENFORCEMENT—On behalf of registered children, parents or Internet Service Providers (ISPs) may recover actual damages for messages sent to a registered Contact Points in violation of paragraphs 101(e). In lieu of actual damages, a parent or ISP may recover $1,000 per violation. For purposes of this paragraph, each message in violation of paragraph 101(e) shall constitute a separate offense.

(2) ATTORNEYS FEES—the court may, in its discretion, award costs and reasonable attorney fees to the prevailing party.

SEC. 103. SAFE HARBOR FOR REASONABLE PROCEDURES

No person shall be in violation of this Act if:

(1) the Contact Point has been on the Registry for less than 30 days; or

(2) the person reasonably relies on the Registry provided by the Attorney General and takes reasonable measures to comply with this Act.

tent is to provide enhanced protection from inappropriate messages targeted at the most vulnerable Internet users. This is in stark contrast to traditional anti-spam laws, which have taken an omnibus approach: attempting to offer undifferentiated protection to every address from every kind of unsolicited electronic mail message. The focused approach of the Children's Protection Registry, however, recognizes the most significant and disturbing aspect of the spam problem and addresses it head on.[104] This is important because while the new Federal anti-spam law sets a base level of protection enjoyed by electronic mail addresses nationwide, it provides no enhanced protection for children from inappropriate messages or extra penalties for the spammers who target them.[105] This is a critical hole in the legislation left for states to fill, making the passage of Children's Protection Registries their logical next step.

In order to offer enhanced protection to children, or any particular group of online users, some sort of registry is critical. You must identify who is a child before you can offer protection to children. Explained another way, remember the Peter Steiner cartoon about the dogs on the Internet discussed above.[106] Not only is it impossible to determine what recipients are Utahans based on their electronic mail addresses, it is also impossible to tell which addresses belong to children, which to adults, and, of course, which to dogs. The solution is to allow protected users to publicly declare their status. Under the proposal, parents can list their children's contact points on the centralized Children's Protection Registry. Once the registry is in place, spammers will be on notice of a recipient's protected status. If they continue to send inappropriate messages to a registered address, then the law will regard them as targeting children and they will face substantial liability. Philosophically, this is no different than a law requiring a tavern owner to check patrons' IDs before serving them alcohol.

---

104. Pornographic spam messages are clearly the most troubling to users. *See* Deborah Fallows, *Spam: How it is Hurting E-mail and Degrading Life on the Internet*, Pew Internet & American Life Project (Oct. 22, 2003) (available at <http://www.pewinternet.org/reports/toc.asp?Report=102>). Moreover, surveys reveal that among the legislative proposals for dealing with spam, the public has the strongest support for protecting children from inappropriate messages. *See* InsightExpress and Unspam, *2003 Comprehensive Spam Survey*, (available at <http://www.unspam.com/fight_spam/information/survey_personal.html>) (updated Oct. 15, 2003) (ninety-four percent of parents believe children deserve enhanced protection under anti-spam laws, ninety-six percent believe parents should be able to block their children's electronic mail address from receiving pornographic material, and ninety-four percent believe spammers should face enhanced prosecution for targeting children with inappropriate messages).

105. *See* 15 U.S.C. §§ 7701–16.

106. Two dogs sitting in front of a computer, one says to the other: "On the Internet nobody knows you're a dog." *See supra* n. 73.

It is important to note what constitutes an "inappropriate message." The model legislation has drafted the definition loosely so it can be tailored to a particular state's community standard. Generally, the intention of the proposed statute is to focus on material and services minors cannot purchase legally in the offline world: pornography, alcohol, tobacco, gambling, prescription drugs, and other materials states deem harmful to children. Most states already have statutes making it illegal to target children with solicitations for these products.[107] The Children's Protection Registry simply allows the force of these statutes to be extended to electronic methods of communication. To this end, states should conform the language of the model legislation so it incorporates their own statutes regulating the materials that, under their existing law, may not be legally sold to children.

In addition, the proposed Children's Protection Registry differs from traditional anti-spam laws because it does not limit itself to electronic mail. This makes more sense than an artificial restriction to electronic mail, especially as technology evolves and the problem of spam changes over time. There is little reason that the particular medium over which an inappropriate message is sent would have any effect on the potential for damage done by the message. Pornographic messages delivered to children via instant messenger, mobile phone, or some other electronic means are as likely to have a negative impact as a pornographic message delivered via electronic mail. Why limit the scope of the law to a particular medium instead of targeting the underlying offending behavior? Up to this point, legislators have generally ignored spam sent over other electronic communications media because these media have not been overwhelmed by spammers.[108] However, there is evidence that this reprieve is ending, and spam, especially pornographic spam, is coming to instant messenger clients, mobile phones, and other electronic communi-

107. *See e.g.* Ala. Code § 6-5-160 (1998); Cal. Pen. Code, §§ 313-313.5 (2002); Mich. Comp, Laws § 722.676 (2003); N.J. Stat. § 2C:34-2 (2003); N.Y. Penal Laws § 235.20 (2003); Utah Code Ann. § 76-10-1206 (2001).

108. There have been a couple of exceptions where governments have passed laws outlawing unsolicited messages sent to mobile devices. *See* Lisa M. Bowman, *Calif. Bans Mobile Phone Spam*, CNET News.com (Sept. 20, 2002) (available at <http://news.com.com/2100-1023_3-958789.html>). *CAN-SPAM* also bans some unsolicited messages sent to mobile devices. *See* Sandra Block, *Lawmakers Set to Pull Trigger on Spam*, USA Today (Nov. 23, 2004) (available at <http://www. usatoday.com/news/washington/2003-11-23-spam_x. htm>). Australia, Japan, and Europe were hit early by a flood of unsolicited mobile messages. As a result, they have all passed measures restricting unsolicited messages sent to mobile devices. *See* ZDNet Australia Staff, *Australia's Spam Act to Become Law in April*, CNET News.com (Dec. 19, 2003) (available at <http://news.com.com/2100-1028_3-5129683.html>); *see also* Evan Cramer, *The Future of Wireless Spam*, 2002 Duke L. & Tech. Rev. 0021 (Oct. 28, 2002) (available at <http://www.law.duke.edu/journals/dltr/articles/2002dltr 0021.html>).

cations systems.[109] The model statute attempts to get ahead of tomorrow's problem by covering these alternative messaging systems today. Moreover, it intentionally provides leeway to the departments enforcing the law so that they can protect new communications systems as they are developed without having to return to the legislature.

Finally, a key difference from traditional anti-spam laws is that the model statute is not restricted to regulating unsolicited messages. Solicited or unsolicited, senders of messages deemed by the community to be inappropriate for children are obligated to check against the Children's Protection Registry before mailing to any address. Since under most states' laws children cannot validly opt in to receiving material the community has deemed harmful to them, there effectively is no such thing as a preexisting business relationship that would authorize inappropriate messages to be sent.[110] Again, the analogy that applies is a tavern owner required to check patrons' IDs before serving alcohol. If an underage patron is served a drink, it does not matter whether the drink was ordered or just given to the minor. In either case the tavern owner is liable. Just as the community's interest in protecting children from alcohol justifies the extra burden imposed on taverns, the community's interest in shielding children from inappropriate messages justifies the additional burden required of the senders of such messages.

B. Evaluating a Children's Protection Registry with the Prosecutor's Cost-Benefit Analysis

If you have read this far, some of the ways in which a Children's Protection Registry improves on the prosecutorial effectiveness of traditional anti-spam laws may already be evident. Remember that there are

109. Juniper Research recently estimated that pornographic messages delivered to mobile devices will constitute a $791 million industry by 2006; gambling messages delivered to mobile devices will constitute a $5.7 billion industry in the same timeframe. Juniper Research, *Mobile Gambling and Adults Content to Reach $6.5bn* (Dec. 2, 2003) (available at <http://www.in-sourced.com/article/ articleview/965/1/1/>). The Juniper study acknowledges that even senders of pornographic and gambling messages to mobile devices must make protecting children their top priority. *Id.* In addition to inappropriate messages sent to mobile devices, there has been a recent rise in instant messenger spam. *See* Anita Hamilton, *You've Got Spim!*, Time Mag. (Feb. 2, 2004) (available at <http://www.time.com/time/magazine/article/0,9171,1101040202-582320,00.html>). Dubbed "spim" these instant messenger messages often contain pornographic materials and can be more disruptive than electronic mail spam. *Id.* Disturbingly, children constitute some of the most frequent users of instant messenger services and therefore are especially vulnerable to inappropriate "spim." *See* eMarketer, *Marketing Online to Kids and Teens* (May 2001) (available at <http://www.mindbranch.com/listing/product/R203-043.html>) (discussing the high percentage of instant messenger users who are children).

110. To make this explicit, model legislation provides: "The actual or implied consent given by the minor does not create a defense to liability."

four key numbers a prosecutor uses to calculate whether to bring a case: 1) the cost of tracking down a spammer, 2) the cost of bringing a trial, 3) the likelihood of success at trial, and 4) the social benefit from a successful prosecution. The goal is to improve the social benefit and the likelihood of success while decreasing the cost of tracking down and bringing a case against a spammer. The model legislation is crafted specifically to achieve this goal and improve all four numbers over traditional anti-spam laws. As a result, even though the law is more limited in scope, in jurisdictions where it is enacted prosecutors will be more likely to bring successful cases against the most repugnant spammers.

1. *Increased Social Benefit*

To begin, it is immediately evident how the model legislation frames the limited area it regulates in such a way as to maximize the perceived social benefit. Prosecutors who successfully bring cases under this law can claim a victory in protecting their jurisdiction's children. Not only can this be a substantial political victory,[111] courts have long held that there is a legally recognized social interest in protecting children from inappropriate materials.[112] In addition, the model legislation recommends substantial fines that mirror the strictest of traditional anti-spam laws.[113] While many spammers will still be judgment proof,[114] any fines that are collected can provide substantial revenue for the state.[115] This means that as a result of the high fines and inherent value of protecting children, under the model statute the benefit side of the prosecutor's cost-benefit equation immediately starts with a substantially heavier weight than under traditional anti-spam laws. Even if the costs and likelihood of success of enforcing a Children's Protection Registry turn out to be the same as traditional anti-spam laws, prosecutors will have a

111. While this political benefit is hard to quantify, it is worth noting that in the 2000 Presidential election protecting children from inappropriate material online was a platform item for both Republican and Democratic parties. *See 2000 Republican Party Platform* <http://www.c-span.org/campaign2000/gopplatform.asp> (accessed Jan. 30, 2004); *2000 Democratic Party Platform* <http://www.democrats.org/about/2000platform.html> (accessed Jan. 30, 2004). Polls have also found that political support for stopping spam spans the entire political spectrum. *See* Henry Norr, *But We Don't Like Spam*, S.F. Chron. (Feb. 2003) (available at <http://sfgate.com/article.cgi?file=/chronicle/archive/2003/02/12/BU212882.DTL>).

112. *See e.g. Miller v. California*, 413 U.S. 15, 18 (1973).

113. These high fines seem more equitable to punish spammers for targeting children, rather than for simply sending unsolicited messages.

114. *See supra* n. 95.

115. Collecting fines for consumer protection statutes is not impossible. Remember that states have collected more than $4.5 million from violators of their do-not-call statutes. *See supra* n. 8.

greater incentive to bring cases. The model legislation is therefore more likely to have a positive effect on the spam problem.

2. *Increased Likelihood of Success and Decreased Trial Costs*

The good news does not end there. The costs of bringing a trial and the likelihood of success at trial appear significantly lower when enforcing the model legislation than traditional anti-spam laws. The statute is drafted to drive down the costs of trial as much as possible. Several fact-intensive inquiries that are required under traditional anti-spam laws are completely avoided under the model statute. For example, prosecutors are not forced to prove there was fraud, demonstrate whether an opt-out mechanism was functional, or explain to a jury complicated mail transfer protocols. More importantly, as discussed above, prosecutors do not need to face the most expensive potential inquiry at trial—they do not have to show that a message was "unsolicited" or face the defense that the recipient had a "preexisting business relationship" with the sender. Instead, only three questions need be answered: 1) Was the child's contact point on the registry? 2) Did the defendant play a role in sending a message to that contact point? 3) Was that message "inappropriate" as defined by the statute?[116] It is likely that a court can answer these questions as matters of law. As a result, prosecutors could resolve many cases by filing summary judgment motions and never empanel a jury.[117] As the Assistant Attorney General of Washington State explained, "[T]he utility of having a do-not-spam list [is that] it enables the enforcement authority to go in and get a pretty quick judgment without having to prove more."[118]

Furthermore, the model legislation cleanly and clearly resolves the thorny constitutional questions that have haunted traditional anti-spam laws. By its very nature, a registry announces the jurisdiction of any registered children's contact points. Spammers are put on clear notice of the jurisdiction they are purposefully availing themselves of when they send a message. This unambiguously resolves the Due Process Clause issue that challenged traditional anti-spam laws. Moreover, the registry clearly defines the geographical limits of a state's regulatory authority. An Illinois Children's Protection Registry, for example, would be limited

116. The last of the questions may require some factual analysis, but as Justice Stewart once observed about pornography, courts are likely to "know it when [they] see it." *See Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

117. This was the experience of many states with do-not-call laws. *See* Selis, *supra* n. 2 (describing state's success of getting quick judgments under do-not-call laws because of the low burden on prosecutors). Remember also that this is not only beneficial to prosecutors, it is also easier on defendants. Both sides have an interest in ensuring the costs of trial are as low as possible.

118. Selis, *supra* n. 2.

to the contact points of Illinois children. This means that states with a registry law do not regulate beyond their borders in such a way that may offend the Commerce Clause.[119] The theoretical law-abiding spammer discussed above is even able to comply with conflicting state regulations because the jurisdictional anonymity of electronic contact points has been removed.[120] In other words, even if an Illinois standard directly conflicted with a Utah standard, spammers attempting to comply with the law now have a mechanism to adjust their messages to the particular requirements of each jurisdiction.

Courts have already specifically affirmed the analysis above. Washington is the only state to have successfully enforced its anti-spam law against an out-of-state spammer. Part of the reason that the state has experienced this unique success is because of an electronic mail registry that it has maintained since 1997. Washington's residents may list their electronic mail addresses on the registry in order to publicly declare them subject to the state's jurisdiction. The Washington Supreme Court specifically upheld the state's anti-spam statute in part because the registry puts spammers on notice of Washington's law before they send to a registered address.[121] The court reasoned that if spammers are on notice of what laws apply to a class of addresses, then the Commerce Clause is not offended.[122] The model statute learns from the success of Washington and effectively creates a functionally similar mechanism to resolve the same constitutional concerns. The model statute will likely also overcome these constitutional challenges under the same analysis—decreasing the cost of trial and increasing the likelihood of success.

Additionally, while traditional anti-spam laws would likely survive a First Amendment challenge because they only target commercial speech, a Children's Protection Registry appears to be on even more solid ground.[123] There are two principal reasons for this. First, courts consist-

119. *See* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L. J. 785, 812 (2001) (a registry can help resolve the problems anti-spam laws have under the Commerce Clause).

120. *Id.*

121. *See Washington v. Heckel*, 4 P.3d 404, 411 (Wash. 2001).

122. *Id* (citing *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 143 (1970)). Other courts examining anti-spam laws have suggested that a registry can help resolve the constitutional issues caused by the jurisdictional anonymity of electronic mail addresses. For example, a court examining the California anti-spam statute suggested that a registry could associate an address with a geographic location. *See Ferguson v. Friendfinders*, 94 Cal. App. 4th 1255, 1265 (1st Dist. 2002). The court stated: "The record does not support the respondents' claim that it is impossible to determine the geographic residence of a [spam] recipient . . . lists of e-mail addresses already exist or can be created and utilized by senders of [spam]." *Id.*

123. One implication of this is that the statute can cover non-commercial speech and likely still survive constitutional scrutiny under the First Amendment.

ently allow states extra leeway in affording protection to children from inappropriate materials, even if state statutes place limits on some speech.[124] Second, and more tangibly, the Supreme Court has upheld a directly analogous statute.[125] The Federal Post Office currently maintains a registry of addresses that are off-limits to pornographic postal mail.[126] If children under the age of nineteen are present in the household, parents may list their address with the Post Office and the government agency will help prevent any inappropriate mail from being delivered.[127] In 1970, a forbearer to this statute was challenged as violating the First Amendment.[128] In no uncertain terms, the Supreme Court upheld the anti-postal solicitation registry and the right of the

124. *See infra* n. 152.

125. *See Rowan v. U.S. Post Off. Dept.*, 397 U.S. 728 (1970).

126. The Mail Preference Service is created by 39 U.S.C. § 3010 (2003). The statute provides:

(a) Any person who mails or causes to be mailed any sexually oriented advertisement shall place on the envelope or cover thereof his name and address as the sender thereof and such mark or notice as the Postal Service may prescribe.

(b) Any person, on his own behalf or on the behalf of any of his children who has not attained the age of 19 years and who resides with him or is under his care, custody, or supervision, may file with the Postal Service a statement, in such form and manner as the Postal Service may prescribe, that he desires to receive no sexually oriented advertisements through the mails. The Postal Service shall maintain and keep current, insofar as practicable, a list of the names and addresses of such persons and shall make the list (including portions thereof or changes therein) available to any person, upon such reasonable terms and conditions as it may prescribe, including the payment of such service charge as it determines to be necessary to defray the cost of compiling and maintaining the list and making it available as provided in this sentence. No person shall mail or cause to be mailed any sexually oriented advertisement to any individual whose name and address has been on the list for more than 30 days.

(c) No person shall sell, lease, lend, exchange, or license the use of, or, except for the purpose expressly authorized by this section, use any mailing list compiled in whole or in part from the list maintained by the Postal Service pursuant to this section.

(d) 'Sexually oriented advertisement' means any advertisement that depicts, in actual or simulated form, or explicitly describes, in a predominantly sexual context, human genitalia, any act of natural or unnatural sexual intercourse, any act of sadism or masochism, or any other erotic subject directly related to the foregoing. Material otherwise within the definition of this subsection shall be deemed not to constitute a sexually oriented advertisement if it constitutes only a small and insignificant part of the whole of a single catalog, book, periodical, or other work the remainder of which is not primarily devoted to sexual matters.

127. 39 U.S.C. § 3010(b).

128. *See Rowan*, 397 U.S. at 728. The original statute referenced in *Rowan* was 39 U.S.C. § 4009 (1967). That statute was passed December 16, 1967, but then reformulated as 39 U.S.C. § 3008 in 1971. Sections 3008 and 3010 are functionally similar. Both create a postal registry; however, the former allows individuals to block any mail, the later only addresses pornographic mail. Section 3010 is a closer analogy to the Children's Protection Registry. While the analysis from *Rowan* applies to 3010, it was also specifically upheld by

government to assist individuals in blocking unwanted materials.[129] Chief Justice Burger wrote for the unanimous Court:

> In effect, Congress has erected a wall—or more accurately permits a citizen to erect a wall—that no advertiser may penetrate without his acquiescence. . . . We therefore categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another. If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has the right to press even 'good' ideas on an unwilling recipient. That we are often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. . . . The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain.[130]

At its heart, the model legislation merely extends to the electronic context the same rights the Supreme Court has specifically affirmed offline. Because the First Amendment case appears clear, under the model statute a prosecutors' costs are further decreased while the likelihood of success is increased.

3. *Lower Tracking Costs*

Tracking a spammer down, the remaining cost to discuss, is the first cost a prosecutor faces when deciding whether to bring a case. As discussed above, the cost of tracking down a spammer is the most difficult of the numbers in the cost–benefit equation for the law to affect. Where possible, however, the model legislation contains measures to reduce these initial tracking costs. First, as suggested above, the model statute expands the definition of who constitutes a "spammer" by attaching liability not only to the actual sender, but also to any business that is knowingly promoted through inappropriate messages. It is typically easier to track down the businesses being promoted rather than the actual sender because they must maintain some presence in order to collect customers' money and fulfill orders.[131] Subjecting to liability the businesses that contract to promote themselves with spam will dry up the demand for spammers' services and thereby have a positive effect on the problem.[132]

---

a lower Federal court. *See Pent-R-Books, Inc. v U.S. Postal Service*, 328 F. Supp. 297 (E.D.N.Y. 1971). Both sections 3008 and 3010 are still in force today.

129. *Id.* at 738.

130. *Id.* at 738 (citations omitted). The Court's use of the term "domain" today seems prophetic when the decision is read in the context of spam and the Internet. The Court has continued *Rowan's* logic even as the commercial speech doctrine has matured. *See e.g. Frisby v. Schultz*, 487 U.S. 474 (1988) (upholding the state's ability to assist individuals enforce posted "no solicitation" signs).

131. *See supra* n. 54.

132. *Id.*

Second, as part of creating the registry, the model statute calls for the state to create a mechanism whereby recipients of inappropriate messages can easily report violators. While this could be done under traditional anti-spam law, prosecutors have faced the challenge of differentiating true spam messages from those the recipient simply did not want to receive. On the other hand, under the model statute a prosecutor can tell whether a reported message is in violation of the Children's Protection Registry merely by looking at 1) whether the message reported is considered "inappropriate" under the definition in the model statute, and 2) whether the message was sent to a contact point listed on the registry. This initial categorization helps prosecutors focus their resources appropriately on the messages that clearly break the law, effectively decreasing the costs of tracking down violators by easily eliminating false leads.

Finally, the legislation allows enforcement by parents and ISPs. While this so-called "private right of action" does not directly decrease a prosecutor's costs in tracking down a spammer, it does enable a number of other motivated enforcement authorities. Traditional state anti-spam law typically included a right for private individuals and ISPs to bring a lawsuit to enforce the law.[133] However, only a handful of cases, mostly either in small claims court or by large ISPs, have been successful under these private right of action provisions.[134] And, because of their small number, there is no evidence that the private cases served as much of a deterrent.[135] This, in part, is explained by the same difficulties prosecutors face filing cases. The expenses of bringing a case are even more difficult for an individual to bear. However, because the Children's Protection Registry decreases these costs, there are likely to be more successful private prosecutions.[136]

---

133. *See e.g.* Michigan, Mich. Comp. Laws § 445.2508 (2003).

134. ISPs have had some significant victories. *See Earthlink v. Carmack,* 2003 U.S. Dist. LEXIS 9963 (N.D. Ga. 2003); *AOL v. CN Productions,* 2002 U.S. Dist. LEXIS 1607 (E.D. Va. 2002); *Verizon v. Ralsky,* 203 F. Supp. 2d 601 (E.D. Va. 2002); Compuserve v. Cyberpromotions, 962 F. Supp. 1015 (S.D. Ohio 1997). Individuals have brought cases; however, they are typically able to receive only minor judgments that rarely can be collected. *See e.g.* Keith W. Kimmel, *Indiana Spam—How I'm Taking My Inbox Back* <http://www.indianaspam.com/> (accessed Jan. 30, 2004) (describing a handful of small, but successful, class-action lawsuits); *see also* SpamCon Foundation, *Suespammers Newsletter* <http://www.suespammers.com/> (accessed Jan. 30, 2004) (newsletter of a small group dedicated to suing spammers, typically in small claims court).

135. *Id.*

136. This follows the same basic model as the Federal anti-junk fax law, which individuals have had success enforcing, and, as a result, which have substantially decreased the number of junk faxes sent. *See* 47 U.S.C. § 227 (2003); *see also* David Kramer, Public Forum, *FTC Spam Forum,* (FTC Conf. Cent., Washington, DC, May 2, 2003). The law is clear and easy for private individuals to enforce. *Id.* As David Kramer, an attorney who helped draft California's anti-spam law, explained: "[The Junk fax] statute worked because of the

Overall, the model legislation was designed from the beginning to achieve the most important goal for any anti-spam measure: making prosecution as easy as possible. It is specifically drafted to increase the social benefit of a prosecution, increase the likelihood of its success, decrease the cost of bringing a trial, and decrease the cost of tracking down offenders. There is no doubt that trials under the model statute will still be challenging, but the challenge will be substantially decreased from what prosecutors face today under traditional anti-spam laws. In order for any law to be effective, its threat of liability must be real. States have an opportunity with a Children's Protection Registry to make a threat that spammers should, for the first time, take seriously.

C. Additional Benefits and Challenges

1. *"It Is Not An Anti-Spam Law"*

The most fundamental criticism of a Children's Protection Registry is likely that it is not really what people think of as an anti-spam law. In many ways this is as much a compliment as a criticism given the success (or lack thereof) of traditional anti-spam law. However, it is important to recognize that a majority of electronic mail users would receive no direct protection from such a registry. Even children, whose electronic contact points are eligible for protection under the registry, are not protected from all spam. The registry focuses on messages that are inappropriate for children, for example, pornography, gambling, alcohol, tobacco, and prescription drugs. Microsoft, and other legitimate businesses, could continue to send unsolicited advertisements for XBox or non-harmful products without any fear of liability.[137]

If the registry only protected children from these message then it may be worth adopting, but the model statute appears to have wider implications than are immediately apparent. To begin, it should be noted that the types of spam the registry regulates are what most upset Internet users. Porn spam, in particular, is especially reviled. The Pew Internet & American Life Project found that "[s]o extreme was the reaction to pornography that eliminating it alone among all unsolicited email would go a long way toward softening spam's negative impact on Internet users."[138] Spammers, by their nature, send to as many electronic

---

threat of private enforcement. The statute empowers people to sue for $500 to $1,500 for each junk fax they receive." *Id.*

137. Microsoft and other legitimate marketers have raised the concern that their legitimate messages may be blocked by strict anti-spam laws. Because these companies do not send inappropriate messages as defined by the model registry, they have nothing to fear from a Children's Protection Registry.

138. *See* Deborah Fallows, *Spam: How it is Hurting E-mail and Degrading Life on the Internet*, Pew Internet & American Life Project (Oct. 22, 2003) (available at <http://www.pewinternet.org/reports/ toc.asp?Report=102>).

contact points as possible. The Children's Protection Registry effectively scatters landmines throughout the universe of electronic contact points. If a porn spammer sends to any child's registered address then they face potentially business-ending liability. It does not matter that the model statute does not offer protection for every electronic mail user because the worst spammers will inevitably "step on" a landmine. When they do, prosecutors will prosecute and they and their pornographic messages will be blown out of business and off the network.

That is a positive first step, but the ripple effects of a Children's Protection Registry may extend much further. Spammers today operate on relatively small margins—sending millions of messages to get a few responses.[139] While inappropriate messages make up around twenty-five percent of all spam messages,[140] they are estimated to account for a majority of spam profits.[141] Most spammers appear to send a broad mix of messages, mixing more profitable "inappropriate" spam with more legitimate messages.[142] Increase the potential costs to sending inappropriate messages and overall spamming becomes significantly more risky or less lucrative. While a Children's Protection Registry would have no direct bearing on mortgage spams, without the money from pornography, Viagra, gambling, and weight loss pills, spammers' margins would be squeezed even thinner. Hopefully many, and especially those with the highest mix of inappropriate messages, would decide that it is not worth staying in the business. This may be wishful thinking, but the Children's Protection Registry holds more potential promise for this than any anti-spam law proposed to this point.

Finally, those senders who do want to continue sending unsolicited messages have a strong incentive to wash their mailing lists against the registry. To do so, they must come out of the woodwork and reveal their identity.[143] Once identified, spammers have transformed themselves from criminals hiding in the shadows to legitimate businesses voluntarily subjecting themselves to regulation. The net effect may be that prosecutors may have an easier time enforcing traditional anti-spam laws, such as *CAN-SPAM*, because the Children's Protection Registry has forced spammers to come forward.

---

139. *See* Gleick, *supra* n. 43.

140. *See* Brightmail, *Spam Percentages and Spam Categories* <http://www.brightmail.com/spamstats.html> (accessed Jan. 30, 2004).

141. *See id.*; *see also* Scott Richter, Public Forum, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, May 1, 2003).

142. *See* Gleick, *supra* n. 43.

143. More than that, the model legislation calls for a fee to be charged to marketers in order to wash their lists against the registry. This is similar to the method by which access to most states' do-not-call lists work.

2. *Technical Challenges*

An additional concern over a Children's Protection Registry is technical. If implemented improperly, the addresses on the registry could be stolen and misused by spammers. While the technical details are beyond the scope of this article, there are ways to implement the registry in such a way as to minimize these risks.[144] For example, instead of storing the actual addresses of registered children, the system could store merely a fingerprint of those addresses. Just as your fingerprint is unique to you but does not reveal your age, hair color, gender, or race, the fingerprints on the registry would be unique to a particular contact point but not reveal the actual address.[145] Even if the registry were hacked, the hacker would get nothing more than a list of otherwise worthless fingerprints. Implemented this way, when senders wanted to wash their own mailing lists through the registry they would take fingerprints of the addresses on their internal list and compare only those fingerprints against the registry. Matched fingerprints would show the senders what addresses to remove, but the system would never reveal any address to marketers that was not already on their internal list.[146] This implementation virtually eliminates the risk of the registry's contents being stolen or misused.

3. *CAN-SPAM Preemption*

Finally, the most serious concern challenging a state's implementation of a Children's Protection Registry involves existing anti-spam law. As was already discussed, the *CAN-SPAM* Act contains a provision preempting some state regulation of electronic mail. However, Congress specifically left some areas open for state regulation. The question is whether the model legislation has been preempted by the new Federal

144. *See* Carl Bialik, *Proposed Do-Not-Email Registry Could Pose Challenge For FTC* WSJ Online <http://online.wsj.com/article/0,,SB107178753630281500,00.html> (accessed Jan. 30, 2004) (companies have developed mechanisms to securely implement no-spam registries). For more information on secure implementations of a Children's Protection Registry, please contact Unspam, LLC. *Unspam Web site* <http://www.unspam.com> (accessed Jan. 30, 2004).

145. These fingerprints can be generated with a one-way hash function. One-way hashes are widely used and related to cryptography. However, unlike cryptography you can encode but not decode a one-way hash. More information on one-way hashing is available online. *See* RSA Security, *What is a Hash Function?* <http://www.rsasecurity.com/rsalabs/faq/2-1-6.html> (accessed Jan. 30, 2004).

146. Additional technical implementations can be put in place so as to prevent what are known as "dictionary attacks"—where a hacker simply generates billions of phony addresses and checks them against the registry to discover what addresses it contains. The technical details are beyond the scope of this article; however, information is available online. *See e.g. Unspam Web site* <http://www.unspam.com> (accessed Jan. 30, 2004).

law. The next section of this article is dedicated to answering that question.

V. *CAN-SPAM* PREEMPTION ANALYSIS

A. POLICE POWERS AND RESPECTING THE COMMUNITY'S STANDARDS

A Children's Protection Registry falls within the clear purview of lawmaking reserved to the states. To begin, the registry has two fundamental purposes: 1) to enable the parental right to protect children from materials considered offensive under the community's standards, and 2) to establish which children reside within the jurisdiction of the state and thereby fall under its umbrella of protection. Most states already have laws on the books that make it illegal to send inappropriate materials to children.[147] However, as already discussed, because in the electronic context it is currently impossible to tell which contacts points[148] belong to children and which belong to adults, let alone which belong to a particular state's jurisdiction, it is nearly impossible without a registry to establish online a constitutionally permissible mechanism to enforce these laws.[149] A Children's Protection Registry can specifically assist in allowing a state to assert its traditional police powers and protect its most vulnerable citizens. Such a registry helps a state solve the unique

147. *See supra* n. 107. The text of Utah's statute serves as a representative example of a law limiting the sale of materials that are deemed harmful to minors:

> (1) A person is guilty of dealing in material harmful to minors when, knowing that a person is a minor, or having failed to exercise reasonable care in ascertaining the proper age of a minor, he:
> (a) intentionally distributes or offers to distribute, exhibits or offers to exhibit to a minor any material harmful to minors;
> (b) intentionally produces, presents, or directs any performance before a minor, that is harmful to minors; or
> (c) intentionally participates in any performance before a minor, that is harmful to minors.
> (2) Each separate offense under this section is a third degree felony punishable by a minimum mandatory fine of not less than $300 plus $10 for each article exhibited up to the maximum allowed by law and by incarceration, without suspension of sentence in any way, for a term of not less than 14 days.
> (3) If a defendant has already been convicted once under this section, each separate further offense is a second degree felony punishable by a minimum mandatory fine of not less than $5,000 plus $10 for each article exhibited up to the maximum allowed by law and by incarceration, without suspension of sentence in any way, for a term of not less than one year.

Utah Code Ann. § 76-10-1206 (citations omitted). This statute is provided here to serve as a reference for examples contained herein.

148. Remember that in the model legislation, "contact points" can be electronic mail addresses, telephone numbers, instant message identifiers, or any other semi-anonymous electronic mode of communications.

149. *See* Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L. J. 785, 812 (2001) (registry can create a mechanism whereby a state can enforce its particular laws in the email context).

problems created by the electronic distribution of inappropriate content and reasserts the community's values over all electronic media.

It is important to note that a state has a "compelling" interest in protecting its children from inappropriate materials.[150] I n proposing a Children's Protection Registry, it is this interest a state is specifically asserting. Because the state's interest is compelling, courts are likely to give broad leeway to the state when crafting and enforcing such laws. Moreover, the role of establishing what constitutes harmful material is specifically left to states. The Supreme Court has clearly explained that it is the local jurisdiction's community standard, within the confines of the First Amendment, not the federal government or any national standard, that determines what content is considered inappropriate.[151] As the Court has explained:

> Under a National Constitution, fundamental First Amendment limitations on the powers of the States do not vary from community to community, but this does not mean that there are, or should or can be, fixed, uniform national standards of precisely what appeals to the 'prurient interest' or is 'patently offensive.' These are essential questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 states in a single formulation, even assuming the prerequisite consensus exists . . . . To require a State to structure obscenity proceedings around evidence of a *national* 'community standard' would be an exercise in futility.[152]

The essential point is that the fundamental right to determine the public morality is reserved to the states and cannot be trumped by Congress.

Without a registry, however, states face a practical problem in the electronic context of defining its community standard for inappropriate messages as well as establishing the borders of its jurisdiction. That problem's solution is at the very heart a Children's Protection Registry. Such a statute effectively puts the universe of those who send inappropriate messages on notice of what electronic contact points fall under the state's umbrella of protection and establishes the rules that must be followed when sending to them. This effectively allows a state to define its borders in the electronic world and regulate what material may cross those borders. Generally, the ability to define and control access to its

150. *See U.S. v. American Library Assn.*, 539 U.S. 194, 238 (2003) (Kennedy, J., concurring) (holding that the protection of young library users from inappropriate material online is a "compelling" government interest); *see also Miller v. California*, 413 U.S. 15, 18 (1973) (holding that a state's interest in prohibiting access to obscene materials is "legitimate"); *Reno v. A.C.L.U.*, 521 U.S. 844, 869–870 (1997) (holding that "shielding" minors from exposure to indecent material is "compelling"); *New York v. Ferber*, 458 U.S. 747, 756–757 (1982).

151. *See Miller v. California*, 413 U.S. 15 (1973).

152. *Id.* at 30 (emphasis in the original).

borders has been upheld as a fundamental right of a state.[153] If a court were to overrule a state's right to create a Children's Protection Registry, it would effectively be designating electronic communications as unbound, and indeed unbindable, by the local community standard the Supreme Court has required states to set. This would force an entire class of communications to be regulated by a *de facto* national standard, which the Court has called "an exercise in futility."[154]

To illustrate the application of this principle, an analogous and compelling comparison exists between the model Children's Protection Registry and states' efforts to control child pornography. While the federal government has regulated the creation and distribution of material depicting children in a sexual manner, courts have consistently allowed states to continue to play a role in child pornography regulation.[155] For example, the Wisconsin appellate court evaluated the state's right to regulate the area of child pornography after Congress had arguably preempted state action.[156] The court stated:

> Child pornography, however, is a crime against us all—state *and* nation. Accordingly, as in the enforcement of our drug laws, where the 'interlocking trellis of Federal and State law . . . enable[s] government at all levels to control more effectively the drug abuse problem,' federal and state regulation of child pornography results in a partnership that enhances rather than retards the underlying goal of protecting children from sexual exploitation.[157]

Similar analysis is likely to be applied by a court evaluating a Children's Protection Registry. Like child pornography, the targeting of children by senders of inappropriate content causes similar potential harms[158] and is a "crime against us all—state *and* nation." Just like in the context of child pornography, the basis for this analysis stems from

153. *See United States v. Brown*, 333 U.S. 18 (1945) (holding that states, under their police powers, have right to control the importation of materials into their borders); *United States v. 12 200-Ft. Reels*, 413 U.S. 123 (1973).

154. *Miller*, 413 U.S. at 30.

155. *See e.g. State v. Bruckner*, 447 N.W.2d 376 (Wis. App. 1989); *Aman v. State*, 409 S.E.2d 645 (Ga. 1981); *New York v. Gilmour*, 678 N.Y.S.2d 436 (1998).

156. *Bruckner*, 447 N.W.2d at 386.

157. *Id.* (emphasis in the original, citations omitted).

158. A 2003 survey by the Symantec Corporation found that eighty percent of children receive inappropriate messages on a daily basis. *See* Symantec Corp., *Symantec Survey Reveals More Than 80 Percent of Children Using Email Receive Inappropriate Spam Daily* (June 9, 2003) (available at <http://www.symantec.com/press/2003/n030609a.html>). The survey revealed disturbing reactions children have when targeted by inappropriate messages: fifty-one percent of the respondents said that they have felt annoyed, thirty-four percent have felt uncomfortable, twenty-three percent have felt offended and thirteen percent have felt curious. *Id.* When they feel annoyed, uncomfortable, offended or curious after seeing inappropriate content, the survey found thirty-eight percent of the children surveyed do not tell their parents. *Id.*

the state's traditional police powers to define and control inappropriate materials based on the community standard. States continue to maintain this fundamental right so long as it is reigned within First Amendment limits, even in the shadow of specific federal involvement in the area. It is therefore likely that courts will extend the same rationale to this proposal as they have in the case of child pornography and allow a state to enforce a Children's Protection Registry law.

B. Specific Preemption Under *CAN-SPAM*

As has already been discussed, the *CAN-SPAM* Act[159] contains language that preempts some of the most restrictive state laws regulating unsolicited commercial electronic mail.[160] However, as the language of the Act indicates, Congress specifically intended to carve out areas where states may continue to regulate electronic communications. Even if a court applies the preemption language from *CAN-SPAM*, these carve outs allow state statutes such as the Children's Protection Registry. The Federal law's preemption language allows:

> (b)(2) State law not specific to electronic mail.—This Act shall not be construed to preempt the applicability of—
>
> (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
>
> (B) other State laws to the extent that those laws relate to acts of fraud or computer crime.[161]

A Children's Protection Registry, as drafted in the proposed model legislation, appears to survive under *CAN-SPAM*'s allowed exemptions to preemption. This argument is bolstered by the fact that the registry furthers the traditional state interest of protecting children and ensuring

---

159. 15 U.S.C. § 7707.

160. *Id.* at § 7707(b)(1). The operative preemption language is as follows:

> This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

161. *Id.* at § 7707(b)(2). The drafting of *CAN-SPAM*'s preemption provision was driven by a number of factors. The first goal of the language was to obviate portions of the California anti-spam law that were to take effect January 1, 2004. The California law provided for electronic mail users to opt in specifically to a Company's mailing list, the so-called "opt-in standard." However, the preemption language was drafted with an eye toward keeping Virginia's and Georgia's anti-spam laws effective. AOL of Virginia and Earthlink of Georgia had established anti-spam laws in accordance with their goals and enforcement strategy. Thus, they sought to limit the preemption language. The influence of these two entities on the drafting process leads to the conclusion that Congress' intent was not complete field preemption. To this end, Virginia's attorney general has specifically stated that the state's anti-spam law was carved out from preemption under *CAN-SPAM*. *NewsHour with Jim Lehrer*, Dec. 16, 2003.

parental rights. Because a children's protection registry falls squarely within the state's traditional powers, courts are instructed by precedent to read the *CAN-SPAM* preemption language narrowly, giving the state broad leeway when passing statutes such as the proposed model legislation.

1. *Preemption Analysis Generally*

Federal preemption of state law relies on the Supremacy Clause of Article VI of the United States Constitution, which proclaims that federal action "shall be the supreme Law of the Land." In examining preemption of state laws by federal laws, courts have looked to whether there has been either express preemption or field preemption. That is, federal statutes must either 1) specifically foreclose a particular type of regulation by the states,[162] or 2) those regulations must be implied due to the breadth and depth of the congressional scheme that occupies the legislative field.[163] In the case of *CAN-SPAM*'s preemption language, Congress' carve outs indicate the intent to allow states some continuing role in regulating electronic mail. Because of this, "express" preeemption, not the broader "field" preemption standard, is likely to be used if a court evaluates a Children's Protection Registry under the Federal law's preemption language.

Regardless of which preemption standard is used, courts have given deference to states in their traditional areas of regulation. One of those powers falling specifically under the state's authority is the exercise of the so-called "police power." Although the boundaries of "police power" are not always clear, the state police power has historically extended, at minimum, to public health, safety, and morals.[164] States have been allowed broad latitude with respect to this police power.[165]

The general rule the Supreme Court has articulated when looking at whether a Federal law preempts state law is that

> in a field which the States have traditionally occupied . . . [the Court starts] with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.[166]

---

162. *See e.g. Cipollone* v. *Liggett Group, Inc.*, 505 U.S. 504, 517 (1992).

163. *See e.g. Fidelity Fed. Sav. & Loan Assn.* v. *De la Cuesta*, 458 U.S. 141 (1982). *See generally Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 541 (2001).

164. *See Beer Co. v. Massachusetts*, 97 U.S. 25, 33 (1878).

165. *See e.g. West Valley City v. Streeter*, 849 P.2d 613 (10th Cir. 1993) (holding that a more restrictive Utah statute regarding cockfighting was not preempted by a federal provision because they could be read consistently and that such a restriction fell under the traditional confines of the state's police power).

166. *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947) (the Supremacy Clause "starts with the assumption that the historic police powers of the States [are] not to be

A Children's Protection Registry, which establishes state and parental rights in the role of protecting children from being targeted by inappropriate content, falls squarely within the state's police powers. These powers have traditionally included a state's ability to control access to obscene materials as well as the relationship and protections afforded between parent and child.[167]

Courts have held that federal preemption language is to be read narrowly in situations where federal law expressly regulates an area traditionally occupied by the states.[168] Put another way, courts are willing to allow state laws to survive even in the face of specific federal preemption when the federal law attempts to regulate traditional areas of state power. Thus, when examining the Children's Protection Registry, there is likely to be a strong presumption in favor of state regulation. Given this, even when evaluated under the *CAN-SPAM* preemption language, the state will be given wide latitude in crafting laws designed to protect children and ensure parental rights. It is important to keep this wide latitude in mind when evaluating the two specific exemptions to preemption allowed under the Federal law.

2. *CAN-SPAM Exemption for Laws not Specific to Electronic Mail*

CAN-SPAM specifically exempts from preemption "[s]tate laws that are not specific to electronic mail."[169] It is important to remember that the Children's Protection Registry, as conceived in the model legislation, is explicitly not specific to electronic mail. Instead of generally regulating the medium of electronic mail, the registry is instead focused on the content being sent and the parties to which that content is directed. As discussed above, this seems like a more rational approach, focusing on the inherent problem as opposed to the traditional anti-spam law's focus on the medium of electronic mail. A Children's Protection Registry does not cover electronic mail specifically, but rather any electronic medium over which inappropriate messages can be delivered (*e.g.* cellular telephone, instant messenger, fax, etc.).[170] In fact, the statute could be

superseded by . . . Federal Act unless that [is] the clear and manifest purpose of Congress"); *see also Medtronic, Inc. v. Lohr,* 518 U.S. 470, 485 (1996) (quoting *Rice,* 331 U.S. at 230).

167. *See Paris Adult Theater I v. Slaton,* 413 U.S. 49, 57 (1973) (holding that there are legitimate state interests at stake in stemming the tide of commercialized obscenity); *Barnes v. Glen Theater Inc.,* 501 U.S. 560, 569 (1998) (holding that the traditional police power of the states in the public health, safety, and morals permits state regulation of nude dancing); *Rose v. Rose et. al,* 481 U.S. 619, 625 (1987) (holding that the parent–child relationship is the exclusive purvey of state authority) (citing *In re Burrus,* 136 U.S. 586, 593–594 (1890)); *Egelhoff v. Egelhoff,* 532 U.S. 141, 151 (2001); *Lorillard Tobacco v. Reilly,* 533 U.S. 525 (2001).

168. *See Rice,* 331 U.S. at 230.

169. 15 U.S.C. §7707(b)(2)(A).

170. *See supra* n. 103.

drafted, if necessary, to never specifically mention electronic mail.[171]

On its face, this appears to be sufficient to pass through the preemption exemption that Congress intended to provide to states under *CAN-SPAM*. Again, since the concept of the Children's Protection Registry statute is to provide a mechanism for parents to protect their children's otherwise anonymous contact points, electronic mail or otherwise, the fundamental idea of the registry not only falls under the traditional conception of the state's police power, but it is also "not specific to electronic mail."

Courts evaluating the statute will likely bear in mind the Supreme Court's guidance on preemption of those laws that fall within the state's traditional police powers. Specifically, the Court has held that when interpreting such language we should focus on the specific wording of preemption clauses, interpreting them narrowly in light of the presumption against preemption.[172] Following the advice of looking at the language of the preemption clause, a court is likely to focus on the definition of the term "specific to." In this case, the term "specific" could mean any law that specifies electronic mail (a standard which would not favor the state), or it could mean any law that exclusively regulates electronic mail (a standard which would favor the state). Legal definitions appear to favor the latter. For example, Black's Law Dictionary defines the term "specific" as: "Precisely formulated or restricted; definite; explicit; of an exact or particular nature . . . tending to specify, or to make particular, definite, limited or precise."[173] Under this definition, a children's protection language statute, as drafted in the model legislation, should survive a challenge under *CAN-SPAM*. The model legislation is not "particular, definite, limited or precise" to electronic mail. Instead the model legislation focuses on the basic issue—the sending of inappropriate messages to children—rather than the medium over which those messages are sent.

Equally compelling are the consequences of a court choosing to define "specific to" as broadly meaning "specifying." Using this definition would result in *CAN-SPAM*'s preemption language expanding to affect a number of state statutes Congress never intended to strike down. States have a number of statutes specifying the regulation of electronic mail. For example, many states regulate the use of electronic mail as a me-

171. However, this feels a bit like game playing on the part of a legislature that a court is likely to see through. The model legislation drafts the Children's Protection Registry to be as clear as possible, including the mention of "electronic mail" among the contact points that the law covers.

172. *Cipollone*, 505 U.S. at 516–17; *see also Rice*, 331 U.S. at 230.

173. *Black's Law Dictionary* 1398 (6th ed., West 1990) (citing *People v. Thomas*, 156 P.2d 7, 17 (Cal. 1945)).

dium for the sending of shareholder stock information.[174] The requirements under most of these statutes are slightly different for a corporation sending to an electronic mail address than sending to a postal address.[175] However, it is clear that these shareholder protection statutes, like the Children's Protection Registry, are not "particular, definite, limited or precise" to electronic mail. Instead, their intent is to regulate electronic mail as part of a larger scheme to protect shareholders, just as the registry serves to regulate electronic mail as part of a larger scheme to protect children. It seems difficult to draw the line of preemption in such a way as to strike down a Children's Protection Registry without also striking down the protections afforded by state statutes such as these. Again, it is important to remember that when interpreting specific preemption of state police powers, a court should choose the definition that favors the state and, when possible, not strike down the statute.[176] Given this and the potential side effects of striking down a Children's Protection Registry, it seems likely that a court would allow such a statute to stand.

Finally, even if there were a successful preemption challenge, the Children's Protection Registry proposal could likely be redrafted as merely an enforcement mechanism for already existing state statutes. As outlined above, within most states there exist statutes regulating the dissemination of pornography and other inappropriate materials to minors.[177] There is no evidence from the Congressional Record relating to *CAN-SPAM* that Congress intended to preempt existing state laws such as these.[178] A Children's Protection Registry, when redrafted in this

174. *See e.g.* Alaska Stat. § 10.06.410 (2003) (regulating when a corporation can communicate with shareholders via electronic mail); Del. Code Ann. tit. 8 § 219 (2003) (regulating the disclosure of electronic mail addresses by corporations); Fla. Stat. § 607.0141 (2003) (regulating when a corporation can communicate with shareholders via electronic mail); Haw. Rev. Stat. § 414-4 (2003) (regulating the manner in which a corporation may communicate with its shareholders over electronic mail); Mass. Gen. Laws ch. 156D, § 1.41 (2004) (regulating when a corporation can communicate with shareholders via electronic mail); Minn. Stat. § 302A.436 (2003) (same); Nev. Rev. Stat. § 78.370 (2003) (same); N.Y. Corp. Laws § 605 (2003) (same); N.D. Cent. Code, § 10-19.1-01 (2003) (same); Okl. Stat. tit. 18 § 1075.2 (2003) (same); Tex. Bus. Corp. Code Ann. § 2.25-1 (2004) (same); Va. Code Ann. § 13.1-610 (2003) (same).

175. *Id.*

176. *Cipollone*, 505 U.S. at 516–17; *see also Rice*, 331 U.S. at 230.

177. *See supra* n. 107.

178. Quite the opposite, the Congressional Record indicates that the intent of Congress was to preempt only state laws in so far as it was impossible for marketers to determine what state laws applied to which addresses. This is not relevant to a children's protection registry since it inherently reveals the jurisdiction that applies to each child on the state's registry. The Congressional Record reporting a summary of the sense of the Congress reads:

> State law prohibiting fraudulent or deceptive headers, subject lines, or content in commercial e-mail would not be preempted [under *CAN-SPAM*]. [Where preemp-

way, aims only to create an identity mechanism in order to allow the enforcement of existing laws. For a court to find that a registry crafted in this way is preempted would strip the existing state laws of a mechanism for enforcement when content is delivered via electronic mail or any other semi-anonymous, electronic medium. This would effectively preempt not only the registry law, but also substantially neuter the existing state laws protecting children. Again, this clearly is not within Congress' intent.

3. *The Computer Crime Exemption*

In addition to the Children's Protection Registry being allowed because it is not "specific to" electronic mail,[179] *CAN-SPAM* also allows regulation of spam so long as the states laws "relate to acts of fraud or computer crime."[180] Violations of the Children's Protection Registry can rightly be classified as criminal and fit squarely within the definition of a "computer crime."[181] Again, it is important to remember that most state laws already deem it a crime to distribute pornography or other inappropriate content to children, regardless of the medium.[182] It makes little sense for a type of behavior to be acceptably defined as "criminal" in the physical world and yet not be considered "criminal" within the digital world. Moreover, violations of the Children's Protection Registry will almost certainly involve some form of computerized device. While the term "computer crime" is not defined under *CAN-SPAM*, it appears likely that a court would conclude that violations of the Children's Protection Registry squarely fall under this definition.[183]

The model legislation calls for both criminal and civil penalties for violation of the Children's Protection Registry. In cases where Congress appears to have preempted a state's right to impose civil penalties, but

---

tion applies it does so in part because] in contrast to telephone numbers, e-mail addresses do not reveal the State where the holder is located. As a result, a sender of e-mail has no easy way to determine with which State law to comply [On the other hand,] the legislation clarifies that there would be no preemption of State laws that do not expressly regulate e-mail, such as State common law, general anti-fraud law, and computer crime law.

Sen. Rpt.108-102 (2003).

179. 15 U.S.C. § 7707(b)(2)(A).

180. *Id.* at § 7707(b)(2)(B).

181. The model legislation defines the violation of the Children's Protection Registry as a "computer crime" in the text of the statute, making it as clear as possible for a court interpreting the act. *See supra* n. 103.

182. *Id.*

183. It is worth noting that Virginia's anti-spam statute calls for certain criminal penalties for sending unsolicited commercial electronic mail into the state, which they define as a "computer crime." Testimony in the Congressional Record indicates it was the intent of Congress, at the behest of Virginia-based America Online, to specifically exempt criminal penalties under Virginia's statute from being preempted. Sen. Rpt. 108-102 (2003).

exempts from preemption criminal penalties, courts have often allowed the totality of the statute to survive preemption.[184] Even under circumstances where a court has not allowed a state to keep its entire statute due to the preemption of one portion, the remedy has been to sever the preempted portions from the legislation and allow the remaining provisions to survive.[185] While not ideal, this "worst case scenario" would still allow a state's attorney general to exercise effective protection from inappropriate content targeted at the state's children.

Finally, to make this explicit and easy for courts, the model legislation specifically identifies the violation of the children's protection registry as a "computer crime." Given the latitude that states are permitted in the face of preemption language, as well as the criminal penalties set forth in the statute, a court holding that the proposed legislation falls within the "computer crime" exemption appears very likely.

VI. CONCLUSION

There is no denying that states have a compelling interest in protecting their citizens from unwanted, and especially inappropriate, messages. The first anti-spam law passed by Nevada six years ago tried to satisfy this interest, but from the beginning its design was hampered by an inability for it to be cost-effectively enforced. Without cost-effective enforcement it is impossible for laws such as Nevada's to have a positive effect on today's spam problem. Unfortunately, state after state followed the same basic approach that has never worked. This helps explain why, in spite of spam's massive increase in volume and the deafening public outcry to stop it, there have been so few prosecutions by states under their existing statutes. The next generation of these laws must learn from the mistakes of the first and do everything possible to reduce the cost of tracking down spammers, reduce the costs of trial, increase the likelihood of success at trial, and increase the social benefit of bringing such a trial.

A Children's Protection Registry is promising as the next generation of state anti-spam statutes because, foremost, it is designed to solve the enforcement problems illuminated by the first generation of anti-spam laws. Importantly, such a registry reduces the complexity of anti-spam prosecutions to three simple, bright-line questions: 1) Was an electronic contact point on the registry? 2) Did the contact point receive a message

184. *See Goldstein v. California*, 412 U.S. 546 (1973) (holding that even though the federal government had passed extensive copyright regulation, California is not automatically preempted from creating further civil protections from copyright holders).

185. *See e.g. Exxon v. Eagerton*, 462 U.S. 176 (1983) (holding that even though portions of a state act were clearly preempted, the remaining portions of the state statute remained in force); *see also Garley v. Sandia Labs*, 236 F.3d 1200 (10th Cir. 2001) (same).

which is considered "inappropriate"? 3) Did the defendant send the message? Enforcement authorities do not need to prove there was fraud in the headers of a message, they do not need to explain mail transfer protocols to a jury, they do not need to demonstrate whether an opt-out mechanism was functional, and they do not even need to show a message was "unsolicited." Moreover, a Children's Protection registry does not face the same constitutional challenges that have hampered or driven up the costs of enforcing existing anti-spam laws. As a result, trials are cheaper, more efficient, and therefore more likely to be brought.

Equally important is that a Children's Protection Registry is designed with a compelling purpose: to protect children from the worst kinds of spam. It breaks down and focuses liability on the spam problem's nastiest core, thereby providing more incentive for prosecutors to bring a case. While initially it seems the benefit of such legislation would be limited to the addresses to which children have access, its ripple effects could extend much further. Such a registry would, in effect, scatter liability landmines throughout the electronic communications universe. If spammers continue to indiscriminately send inappropriate messages, they will face substantial risk of liability for when they inevitably target a child. When the liability from the Children's Protection Registry law helps remove a spammer from the network, then all of its users, whether child or otherwise, benefit.

While the Federal government has recently provided a baseline of protection for electronic mail, no one believes the *CAN-SPAM* law will have much more than a limited effect on the problem.[186] The Federal statute simply mimics the first generation of state laws, which have already been shown to be ineffective. Most disturbingly, *CAN-SPAM* provides no enhanced protection for children from the worst kinds of messages. If any law is going to have any possible effect on spam, states need to discover it by exercising their role as "laboratories of democracy" and experiment with new approaches. Eventually an approach may show itself to be particularly successful, and at that time it may be appropriate to adopt it at the Federal level. Until then, however, the current Federal framework specifically leaves holes for states to fill and limits its preemption in such a way as to allow for innovative new state regulations. In many ways this should be viewed as a mandate. States should not cede their control of the anti-spam space to Federal lawmakers. Instead they should experiment with innovative new regulations in order to maintain their traditional police powers, protect chil-

186. Even the sponsors of the legislation called it merely a "first step" and not a "silver bullet" in dealing with spam. *See e.g.* 149 Cong. Rec. S 15938, 15944 (daily ed. Nov. 23, 2003) (Sen. Wyden, one of the principal sponsors of *CAN-SPAM*, speaking about its limitations).

dren, establish parental rights, and set the local moral standards—even for messages that arrive online. While other approaches may be possible, for states eager to stay relevant in the fight against unwanted and inappropriate electronic messages, a Children's Protection Registry is a sensible legislative choice for the next generation of state anti-spam laws.