An Architecture for Spam Regulation

David Dickinson*

* B.S. Computer Science, 2002, Indiana University – Bloomington; J.D. candidate, 2005, Indiana University School of Law – Bloomington. I wish to thank Professor Fred Cate for his helpful comments and suggestions.

"Architecture becomes the tool of law when the direct action of the law alone would not be as effective." –Lawrence Lessig[1]

I. INTRODUCTION

Both legal and technical attempts to regulate spam[2] have proliferated in recent years. As the problem of spam has grown to 12.4 billion messages per day,[3] legislatures, Internet service providers ("ISPs"), and software developers have all tried various responses. Legislative responses have culminated in the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act") of 2003.[4] Numerous e-mail clients now include spam filters, and ISPs are using both technical and legal means to strike back at spammers. Indeed, the Online community appears quite united in its contempt for spam.

In spite of the numerous attempts to regulate spam, the problem has not diminished. The spammers continue to win the war in spite of the Internet community's best efforts. The recent CAN-SPAM Act has had little effect.[5] Legislative responses are limited by jurisdictional obstacles to

1. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 512 (1999).

2. Spam can be broadly defined as junk e-mail. For an overview of how the term has evolved to describe the problem of junk e-mail, see John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 336-38 (2003).

3. Spam Statistics 2004, *at* http://www.spamfilterreview.com/spam-statistics.html (citing statistics for 2003) (last visited Sept. 13, 2004).

4. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at scattered sections of 15 U.S.C.) [hereinafter CAN-SPAM Act 2003].

5. *See, e.g.*, Grant Gross, *Anti-spam Bill Won't End Junk Email*, IDG News Service (Dec. 26, 2003), *at* http://maccentral.macworld.com/news/2003/12/26/antispam/index.php ?redirect=1072424647000 [hereinafter *Anti-spam Bill*]; Grant Gross, *State Spam Laws and the New CAN-SPAM*: *The Federal Anti-spam Law Takes Precedence Over Most State Anti-spam Provisions*, INFOWORLD (Feb. 27, 2004), *at* http://www.infoworld.com/article/ 04/02/27/09FEspamstates_1.html ("In the first days of January, after the law went into effect, spam-filtering companies measured no decrease in spam being sent across the Internet.") [hereinafter *State Spam Laws*]; Cade Metz, *Can E-Mail Survive?*, PC MAG. (Feb. 17, 2004), at 55, *at* http://www.pcmag.com/print_article/0,2048,a=117514,00.asp [hereinafter *Can E-Mail Survive*]; *FTC: 'Can Spam' Law Only a Mild Deterrent*, FOX NEWS

enforcement and the technical measures taken by spammers to disguise their source and identity. Technical approaches to dealing with spam, such as spam filters and blacklists, have probably been more successful, but have also faced their share of problems. Spam filters often struggle with filtering too much or too little.[6] Furthermore, filters fail to deter future attempts, and spammers often find ways to circumvent the filters. Blacklists and similar approaches represent an Online form of vigilantism with many side effects.[7] Innocent parties often have their messages blocked,[8] and there are few safeguards to make sure that parties are only being blacklisted for good cause.[9] David Sorkin has suggested that the "[c]oordination of technical and legal mechanisms seems to be the most promising approach to the spam problem."[10] Despite the fact that many people would agree with Sorkin, legislative and technical approaches to stopping spam have yet to be coordinated. Sorkin suggests that this is because the consensus required for such coordination is unlikely to be achieved.[11]

This Note argues that the universal low regard for spam makes such coordination possible. Instead of making architectural changes that enforce a particular legislative approach to spam, the focus should be an architectural approach that enables both ISPs and end-users to more effectively identify and filter unwanted spam. The law is not excluded from this solution, rather it has an important role to play in enabling it.

This Note begins by outlining the techniques employed by spammers to evade both technical and legal countermeasures, then goes on to explore the costs spam shifts from mailers to recipients. The First Amendment constraints placed upon any regulatory model are outlined, followed by a suggested regulatory and architectural framework that could enable a

(Feb. 10, 2004), *at* http://www.foxnews.com/story/0,2933,110910,00.html; Eric J. Sinrod, *Junk E-mail Runs Rampant Despite CAN-Spam Act*, USA TODAY (Mar. 25, 2004), *at* http://www.usatoday.com/tech/columnist/ericjsinrod/2004-03-25-sinrod_x.htm; Daniel Nasaw, *Federal Law Fails to Lessen Flow of Junk E-Mail*, WALL ST. J., Aug. 10, 2004, at D2.

6. Hiawatha Bray, *As Spam War Heats Up, Many Valid E-mails Are Getting Lost*, BOSTON GLOBE, Feb. 18, 2004, at A. 14, *available at* http://www.boston.com/business/technology/articles/2004/02/18/as_war_on_spam_heats_up_many_valid_e_mails_are_getting_lost/.

7. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 347 (2001).

8. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 679-82 (2003).

9. *Id*. at 677-79.

10. Sorkin, *supra* note 7, at 384.

11. *Id*.

substantial reduction in spam while leaving filtering decisions in the hands of individual e-mail users. The suggested architectural framework builds upon several authentication-based systems being proposed by private industry, but suggests key changes that can be made to afford more First Amendment protection to e-mail and to allow individuals greater autonomy in determining what e-mail they will receive.

II. BACKGROUND

A. The Spammers' Tools

In order to understand the problem of spam, it is helpful to understand the methods employed by spammers to exploit the e-mail medium. E-mail operates on the Simple Mail Transfer Protocol ("SMTP").[12] The protocol was written in 1982,[13] well before the problem of spam was a concern. As a result, SMTP was not designed with the problem of spam in mind. No allowances were made for the need to authenticate users, verify identity, and guarantee message privacy or integrity. The only way recipients can determine the source of spam is to rely upon the "From:" field and "Received:" headers.[14] A sample, excerpted from *Stopping Spam*, is shown below:

12. *See* ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM 48 (1998). This simple example shows a header in SMTP version 1.0. Subsequent versions of SMTP have made these headers considerably more complex through the addition of extensions, but have failed to make the process of identifying the true source of an e-mail any easier. *See generally* J. Klensin, *RFC 1869: SMTP Service Extensions*, THE INTERNET SOCIETY: Internet Engineering Task Force (Nov. 1995), *at* http://www.ietf.org/rfc/rfc1869.txt.

13. *See* Jonathan B. Postel, *RFC 821: Simple Mail Transfer Protocol*, THE INTERNET SOCIETY: Internet Engineering Task Force (Aug. 1982), *at* http://www.ietf.org/rfc/rfc0821.txt. SMTP has been updated to version 1.1, but the protocol remains largely insecure. J. Klensin, *RFC 2821: Simple Mail Transfer Protocol* at 64, THE INTERNET SOCIETY: Internet Engineering Task Force (Apr. 2001), *at* http://www.faqs.org/rfcs/rfc2821.html [hereinafter *RFC 2821*].

> SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so that the "spoofed" behavior cannot be detected by an expert is somewhat more difficult, but not sufficiently so as to be a deterrent to someone who is determined and knowledgeable.

Id.

14. The situation is complicated by the use of "Return-Path" and "Resent-From" headers used by later variations of SMTP. Nevertheless, the analysis is largely unchanged. These headers are also susceptible to forgery. *See generally RFC 2821*, *supra* note 13, at 64-65; P. Resnick, *RFC 2822: Internet Message Format* at 27-29, THE INTERNET SOCIETY: Internet Engineering Taskforce (Apr. 2001), *at* http://www.faqs.org/rfcs/rfc2822.html.

> From you@earth.solar.net Sat May 9 12:40:45 1998
> Received: from jupiter.solar.net (jupiter.solar.net [1.4.4.7]) by pluto.solar.net (8.8.7/8.8.7) with SMTP id KAB00332 for <chrism@pluto.solar.net>; Sat, 9 May 1998 12:40:45 -0600
> Received: from earth.solar.net (earth.solar.net [1.4.4.4]) by jupiter.solar.net (8.8.8/8.8.8) with SMTP id MAA00395 for <chris@jupiter.solar.net>; Sat, 9 May 1998 12:40:40 -0600
> Date: Sat, 9 May 1998 12:40:30 -0600
> From: you@earth.solar.net
> To: Chris <chris@jupiter.solar.net>
> Subject: Steel Pulse concert date
> Message-ID: <19980509124030.0113@earth.solar.net>
> X-Mailer: QUALCOMM Windows Eudora Pro Version 4.0
> X-UIDL: 179c97f481a77a5da1a8109409a00afe
> **Hi Chris!**[15]

The "From:" field is the most obvious method of identifying the sender, but it is also a very unreliable way. It can be easily forged by the message sender.[16] Spammers rarely use an address they can be reached at in the "From:" field, and quite often, the address has either been made up or is the e-mail address of some innocent party. The "Received:" headers are a more useful method of identifying spammers. A "Received:" header is added by each host that relays the message from its source to its eventual destination. Each of these headers lists the name and address of a system that relayed the message, as well as the name and address of the system that just passed it the message. Spammers cannot prevent intermediary systems from adding these headers. The headers still provide only minimal protection because a thorough examination of the "Received:" header will be required to identify the real source of the message.

Two well-known techniques utilized by spammers to confuse message recipients are using open relay sites[17] to send their messages[18] and adding "Received:" headers of their own creation when sending a message. Open relay sites are servers that allow themselves to be used by unknown computers to send e-mail messages. Mail can be traced back to these relays, but it is unlikely that the relay operator will be able to identify the system that passed it the message. While servers that allow relaying are

15. SCHWARTZ & GARFINKEL, *supra* note 12, at 55-56.

16. *Id*. at 86.

17. In technical terms, an open relay site allows spammers to send their spam by asking the relay system's Mail Transport Agent, rather than the spammer's own agent, to deliver e-mail. *See generally id*. at 90-91.

18. *Id*. at 88-91.

becoming less common as a result of the spam problem, they still exist and are well-known by spammers. These relay sites are often blacklisted, meaning that certain ISPs will not accept messages from them.[19] While this is helpful, it has the effect of blocking not only spam, but also legitimate messages by other senders that may depend on the relay for mail transport.[20]

The second technique is the adding of bogus "Received:" headers. However, this technique is less effective. The bogus headers add erroneous information, but are not able to prevent the addition of accurate "Received:" headers. This means a recipient can rely on the header that his own server added (jupiter.solar.net in the example) and work back from one header to the next, identifying whether the server is one he trusts at each step.[21] The message "id" can be used to verify the authenticity with the administrator at each intermediary. Eventually, the false headers can be identified.

Unfortunately, identifying the source mail server does not identify the person and computer that actually authored and sent the message. In some instances, the administrator of the source server will be able and willing to identify the culprit, but in others, an administrator will be unwilling or unable to do so. Regardless of how many ISPs are now actively disabling the accounts of their customers who are sending spam, there are still ISPs and open relays in the United States and abroad that are unwilling to cooperate.

Spammers have been growing increasingly bold in their attempts to send spam. A new technique being relied upon is to create spam zombies. Spam zombies are computers owned by innocent third parties that are hacked and used by spammers to send spam.[22] The owners of these spam zombies are typically unaware that their machines have been taken over until their ISP terminates their account.[23] The hacker who exploits these third-party computers may be difficult or impossible to identify.

The architecture underlying e-mail has not been conducive to effective spam regulation. Spam can often be filtered or blocked, but the underlying architecture of e-mail provides an effective barrier between law enforcement and the perpetrators of spam. Before spam can be effectively

19. Sorkin, *supra* note 7, at 347-48.

20. *Id*. at 347-50.

21. SCHWARTZ & GARFINKEL, *supra* note 12, at 91-93 (outlining this general method).

22. Associated Press, *Your Computer Could Be a 'Spam Zombie'* (Feb. 18, 2004), *at* http://www.cnn.com/2004/TECH/ptech/02/17/spam.zombies.ap/index.html [hereinafter *Spam Zombie*].

23. *Id*.

regulated, there must first be changes to the architecture underlying e-mail. The architecture must be adapted to provide the ability to identify and authenticate the senders of spam.

B. The Case for Spam Regulation

The magnitude of the spam problem has grown steadily since the emergence of the World Wide Web. During the one year from the summer of 2001 to the summer of 2002, spam increased by 450 percent.[24] Spam is highly problematic because it frequently features pornographic content; unsolicited, commercial advertisements; and fraudulent, get-rich-quick schemes; all sent from a carefully disguised source. Spam also represents a computer security risk.[25] Mass e-mails are a frequent source of computer viruses.[26] Increasingly, these viruses then turn infected computers into spammers.[27] Legitimate businesses have avoided the use of unsolicited spam to a large extent. They are motivated by the fear of generating ill will among potential customers or concerns about the possible legal consequences. Even ISPs have played a significant role in reducing the amount of legitimate commercial spam by prohibiting the sending of spam as a condition in their subscriber agreements.[28] As a result of the predominantly nefarious content, the majority of spammers cannot claim any substantial protection under the First Amendment for the speech contained within the spam messages.[29]

The sending of spam results in a substantial shifting of costs from advertisers to ISPs and e-mail recipients. In 2003, spam is estimated to have cost companies worldwide $20.5 billion.[30] Spammers are able to send messages for minimal cost—the cost of their Internet access and mailing lists.[31] The costs of relaying messages, storing them, and downloading them

24. Michael B. Edwards, *A Call to Arms: Marching Orders for the North Carolina Anti-Spam Statute*, 4 N.C. J.L. & TECH. 93, 93 (2002).

25. Sorkin, *supra* note 7, at 339-40.

26. *See* Tony Bradley, *Solving the Spam Epidemic: Can You Legislate Spam Away?*, ABOUT.COM (May 16, 2004), *at* http://netsecurity.about.com/cs/emailsecurity/a/aa051604.htm. (concluding, in April 2004, that 9.2% of global e-mails contained some form of virus).

27. *See Spam Zombie*, *supra* note 22.

28. Sorkin, *supra* note 7, at 343.

29. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563-64 (1980).

30. ORGANISATION FOR ECONOMIC DEVELOPMENT AND CO-OPERATION, BACKGROUND PAPER FOR THE OECD WORKSHOP ON SPAM, at 14, *at* http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final (Jan. 22, 2004).

31. This cost is estimated to be .0032 cents per message. *See* Edwards, *supra* note 24, at

are borne by others. The extent of other forms of commercial advertising that occurs is limited by the cost of the advertising. With e-mail, the cost is higher on the recipients than on the advertisers, with an estimated margin of $270 million for spammers versus an inflicted cost of $8-10 billion on the rest of the world in 2002.[32] Given this cost imbalance, there is no effective economic limit on the amount of spam that can occur, other than the limits of the ability of end-users to shoulder the costs.

Congress previously addressed the issue of cost-shifting in the Telephone Consumer Protection Act of 1991 ("TCPA").[33] The TCPA prohibited the sending of unsolicited advertisements via fax. A First Amendment challenge to the Act failed in *Destination Ventures v. FCC*.[34] The Ninth Circuit held that Congress did not exceed its authority by restricting the ability of advertisers to shift the costs of advertising onto consumers. The cost of an unsolicited fax advertisement was only between three and forty cents per sheet, but the Court found that this was enough to justify Congress' decision to regulate.[35]

While the cost shifting imposed by the present volume of spam messages may seem trivial to many individual users, the continuous and steady growth of the problem gives cause for concern. The spam problem threatens to reach far beyond commercial messages. Mailing lists are already inexpensive to obtain,[36] and there is nothing to prevent the possessor of a list from posting it to the Web. Every Internet user would be empowered to speak and have the whole world listen. While most users would show better judgment, a few would be sure to abuse it. Those who have been on mailing lists where various persons have carried out their discussions by using the reply-all option will appreciate the potential for disaster if this were to occur with millions of people on the list (while most users might realize that they were being quite obnoxious by doing this, a listserv could make this act completely innocent and transparent). Multiply this potential for mass-mailing abuse with the ability to send large video or multimedia files and one can quickly see that e-mail could be destroyed as an effective medium of communication when spam is carried to the extreme. What is now just an annoyance could soon threaten to overflow

93.

32. *Id*. at 93-94.

33. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2000).

34. Destination Ventures, Ltd. v. FCC, 46 F.3d 54 (9th Cir. 1995).

35. *Id.* at 56-57.

36. *See* Sam Vaknin, *The Economics of Spam*, ELECTRONIC BOOK WEB (July 23, 2002), *at* http://12.108.175.91/ebookweb/discuss/msgReader$1533 (claiming that a list of ten million e-mail addresses costs only 100 dollars).

inboxes and clog the arteries of the Internet on a very large scale. As Sorkin suggests, e-mail users could be pushed to adopt other means of electronic communication.[37]

III. LEGAL HISTORY

The spam problem has spurred a steady stream of different responses. Early attempts focused on common law remedies and self-regulation. As these approaches failed to dissuade spammers, many private parties tried to develop technical solutions. The mixed results of technical approaches led states to craft legislation targeting spam. Most recently, the European Union and United States Congress have begun to address the spam problem through legislation. Because these legislative responses have been met with limited success,[38] private industry has turned its full attention to solving the spam problem through a number of competing responses.[39]

A. Common Law Remedies

In the absence of governing legislation, there have been a number of cases where common law causes of action have been applied to strike back at spammers. In *Compuserve Inc. v. Cyber Promotions Inc.*,[40] a district court found an ISP could claim trespass to chattels where a spammer had sent unsolicited commercial e-mail, even after being advised that certain recipients did not want to receive these messages.[41] Trespass to chattels was found "to include the unauthorized use of personal property."[42] Compuserve successfully argued that it had been harmed by losing customers who were upset by the amount of spam they were receiving and that the high volume of unsolicited commercial e-mail was preventing Compuserve's customers from having full access to the services they were paying Compuserve to provide.[43]

Some courts have taken a more restrictive view of the applicability of common law remedies. In *Intel Corp. v. Hamidi*,[44] the Supreme Court of California found that trespass to chattels should not encompass "electronic

37. Sorkin, *supra* note 7, at 338-39. The concern for the long-term viability of e-mail is increasing. *See, e.g.*, Metz, *supra* note 5.

38. Sinrod, *supra* note 5.

39. Paul Roberts, *Competing Technologies Could Shake Up E-Mail*, INFOWORLD (Mar. 1, 2004), *at* http://www.infoworld.com/article/04/03/01/HNcompeting_1.html.

40. 962 F. Supp. 1015, 1015 (S.D. Ohio 1997) .

41. *Id*. at 1020-24.

42. *Id*. at 1020.

43. *Id*. at 1019, 1022-23.

44. 71 P.3d 296 (Cal. 2003).

communication that neither damages the recipient computer system nor impairs its functioning."[45] This holding raises serious questions about the robustness of common law remedies as a means of blocking spammers. Individual cases of spam will rarely cause any material damage or impairment to recipient systems. The harm caused by spam is more a result of aggregation. While a single, unwanted message may be a mere annoyance, hundreds or even thousands of unwanted messages sent to an individual can cripple e-mail as an effective medium of communication for that user. Fortunately, the mixed success of common law responses to spammers are becoming irrelevant in light of the increasing availability of statutory remedies at both the state and federal level.

B. Legislative Responses

Governments around the world are recognizing the dangers posed by spam. Numerous states have acted to proscribe spam. As of September 2004, thirty-four states have acted to restrict spam in various forms of legislation.[46] A number of European Union ("EU") directives have also targeted spam.[47] The EU E-Commerce Directive requires that "Member States shall lay down in their legislation that unsolicited commercial communication by electronic mail must be clearly and unequivocally identifiable as such as soon as it is received by the recipient."[48]

Most recently, the United States passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act").[49] The CAN-SPAM Act prohibits fraudulent mass e-mails.[50] It also specifically targets false or misleading transmission of information and deceptive subject headings.[51] It requires that opt-out requests be honored and that the spammer be able to receive mail at his return address.[52] The CAN-SPAM Act calls for the Federal Trade Commission ("FTC") to

45. *Id*. at 300.

46. David Sorkin, *State Laws*, *at* http://www.spamlaws.com/state/summary.html (last revised Dec. 16, 2003).

47. Magee, *supra* note 2, at 362-73 (describing the EU Data Protection Directive, Distance Selling Directive, Telecommunications Directive, E-Commerce Directive, and Electronic Communications Privacy Directive).

48. *Id*. at 368 (citing Council Directive 2000/31/EC of 8 June 2000 on Certain Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1).

49. CAN-SPAM Act 2003, *supra* note 4.

50. 15 U.S.C. 7704.

51. *Id*.

52. *Id*.

consider the creation of a national Do-Not-E-mail registry.[53] As a result of the CAN-SPAM Act, many state anti-spam laws may be preempted.[54] In the wake of the CAN-SPAM Act, the FTC has promulgated a rule requiring that sexually explicit e-mails bear the heading "Sexually-explicit:" in their subject line.[55] The CAN-SPAM Act also solves the potential dormant Commerce Clause challenges posed by state anti-spam regulation by regulating spam at the federal level.[56]

As the recent wave of spam regulation demonstrates, the question posed by spam is not whether spam should be regulated, but how it can be regulated effectively. The problem has continued its steady growth and managed to evade both technical and legal solutions.

C. First Amendment Concerns

The First Amendment will place constraints upon any attempt to regulate spam. Legislators must be extremely careful as they decide whether to regulate all unsolicited bulk e-mail or just all unsolicited commercial e-mail. As decisions to filter messages move out of the hands of government and into the hands of private parties, however, the First Amendment becomes less of a factor. The right of one individual to speak does not carry with it the right to make others listen. Nor does it include the right to force private parties to facilitate an advertiser's speech.

Unsolicited commercial e-mails have been afforded little protection under the First Amendment. In *Compuserve*,[57] the private ISP (Compuserve) made a successful trespass against chattels claim against Cyber Promotions on the basis of Cyber Promotions' continued sending of spam, even after receiving requests to cease and desist.[58] The Court held that the legal measures taken by Compuserve to block spam did not violate

53. § 7708. The FTC has since abandoned this section because of concerns over technical feasibility. *See* Grant Gross*, FTC Declines Do-Not-Spam List*, PC WORLD (June 15, 2004), *at* http://www.pcworld.com/news/article/0,aid,116536,00.asp.

54. § 7707. *See also State Spam Laws*, *supra* note 5.

55. Label for Email Messages Containing Sexually Oriented Material, 69 Fed. Reg. 21024 (Apr. 19, 2004) (to be codified at 16 C.F.R. pt. 316), *available* http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf. *See also* REUTERS, *FTC: Porn Spam Must be Labeled* (Apr. 13, 2004), *at* http://zdnet.com.com/2100-1105_2-5190959.html.

56. *See generally* Michael B. Edwards, *A Call to Arms: Marching Orders for the North Carolina Anti-Spam Statute*, 4 N.C. J.L. & TECH. 93, 107-13 (2002) (applying the *Pike* test to the North Carolina anti-spam statute).

57. Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

58. *Id*. at 1017.

the First Amendment.[59] As an ISP, Compuserve was a private actor, and the sending of spam had been found to be a trespass against private property. The First Amendment could not be applied to Compuserve as a private actor or used to compel the appropriation of private property to deliver Cyber Promotions' messages.[60] The Court's holding was limited to the context of a private actor engaging in the filtering. The issues of anti-spam legislation and government involvement in filtering remain contentious issues.

Where commercial speech is regulated by a government entity, the *Central Hudson* four-part test is applicable.[61] As a prerequisite for First Amendment protection, the speech must be lawful and not misleading. A large quantity of spam fails to meet this prerequisite for First Amendment protection. When spam does qualify as protected speech, there must be a substantial governmental interest served by the regulation, and the regulation must directly advance the governmental interest. Finally, if the regulation is to be upheld, it must be narrowly tailored to the governmental interest that it seeks to advance.[62]

The government has a compelling interest in regulating the subset of spam that is lawful and not misleading. Spam in all of its forms leads to a shifting of costs from sender to receiver. Commercial cost shifting was found to be compelling in *Destination Ventures*.[63] The issue of greater concern in crafting spam regulations is the need to tailor the regulation to the substantial governmental interest at stake. Congress' decision to target only unsolicited advertising was upheld in *Destination Ventures*.[64] The regulation of all unsolicited bulk e-mail, instead of all unsolicited commercial e-mail, must survive strict scrutiny. A broader attempt to regulate non-commercial bulk e-mail would need to be narrowly tailored to the need to protect minors from pornography, improve computer security, and maintain the viability of e-mail as a means of personal and solicited commercial communication.

59. *Id*. at 1025-26 (citing Cyber Promotions, Inc. v. America Online, Inc. 948 F.Supp. 436 (E.D. Pa. 1996)).

60. *Id*. at 1026.

61. Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980).

62. *Id*. This tailoring requires the regulation to be no more extensive than necessary, but it does not have to be the least restrictive means of regulation. Bd. of Trs. of the State Univ. of N.Y. v. Fox, 492 U.S. 469, 480 (1989).

63. Destination Ventures, Ltd. v. FCC, 46 F.3d 54, 56 (9th Cir. 1995).

64. *Id*.

Recent attempts to protect individuals from unwanted telemarketing have underscored the difficulty in tailoring an interest in speech regulation to a regulatory solution. The FTC recently attempted to create a national Do-Not-Call Registry as part of a revision to the Telemarketing Sales Rules.[65] The revised rules imposed fines for telemarketers that called numbers on the Do-Not-Call Registry "to induce the purchase of goods or services."[66] A federal district court struck down the revised rules on First Amendment grounds.[67] It held that unlike the circumstances in *Rowan v. United States Post Office Department*,[68] where the right to refuse certain unwanted solicitations was upheld, the government had not enabled consumers to choose which solicitations to block.[69] Only commercial, and not charitable, solicitations could be blocked. However, both were held to be protected speech.[70] Because it was not the individual that was making the choice as to which calls to block, the court held that the revised rules amounted to an unconstitutional governmental restraint on speech.[71]

The Court of Appeals for the Tenth Circuit reversed the district court and upheld the constitutionality of the Do-Not-Call Registry.[72] The Tenth Circuit was satisfied that individuals were making autonomous choices similar to those in *Rowan* under the revised rules.[73] It found that the distinction between commercial and non-commercial speech appeared to be reasonable because commercial solicitations are more likely to result in fraud,[74] and have done more to invade individual privacy than non-commercial solicitations.[75] The Tenth Circuit's holding is quite significant due to a provision in the CAN-SPAM Act that calls for the FTC to consider the creation of a national "Do-Not-E-mail" registry.[76] In light of the Tenth Circuit's decision, a "Do-Not-E-mail" registry is also likely to withstand

65. 16 C.F.R. § 310.4(b) (2003).

66. *Id*. at § 310.4(b)(1)(iii)(B).

67. Mainstream Mktg. Servs. v. FTC, 283 F. Supp. 2d 1151 (D. Colo. 2003).

68. Rowan v. United States Post Office Dep't, 397 U.S. 728 (1970).

69. *Mainstream Mktg. Servs.*, 283 F. Supp. 2d at 1168.

70. *Id*. at 1167.

71. *Id*. at 1168.

72. Mainstream Mktg. Servs. v. FCC, 358 F.3d 1228 (10th Cir. 2004), *cert. denied*, 2004 LEXIS 5564 (U.S. Oct. 4, 2004).

73. *Id*. at 1237-38.

74. *Id*. at 1237, 1240.

75. *Id*. at 1238-39 (stating that "the First Amendment does not require that the government regulate all aspects of a problem before it can make progress on any front").

76. CAN-SPAM Act 2003, *supra* note 4, at §7708. The FTC has since responded that a Do-Not-E-mail registry is not worth pursuing. *See* Grant Gross, *FTC Declines Do-Not-Spam List*, PC WORLD, June 15, 2004, *at* http://www.pcworld.com/news/article/0,aid,116536,00.asp.

First Amendment scrutiny.

It is unlikely that any First Amendment challenge to the CAN-SPAM Act will be successfully asserted. The CAN-SPAM Act does not even attempt to proscribe unsolicited commercial or adult-oriented e-mails, opting instead to only require spammers to honor opt-out requests. These opt-out requests must be made separately for each unwanted solicitor and are analogous to those upheld in *Rowan*.

The First Amendment question is most easily resolved when filtering is performed by a private actor, namely the ISP or the intended spam recipient. The ISP, when a private actor, is immune from First Amendment attack.[77] Advertisers are also unable to wield the First Amendment to guarantee the right to have their messages heard by consumers. The First Amendment does not compel consumers to view any unwanted communication.[78]

The best regulatory framework for spam will be one that shifts content-based filtering decisions into the hands of private parties. Attention has increasingly turned to private industry to provide a solution to the spam epidemic.

D. Industry's Response

A number of corporations are determined to defeat spam, and their responses are growing increasingly complex. Initial responses to spam have focused on fighting it at the receiving end. Spam filters and blacklists are the primary examples. The next approach is to fight spam at its source. Two general approaches to fighting spam at the source are increasing the cost of sending spam and creating the ability to authenticate and identify the senders.

Microsoft has suggested a couple of approaches aimed at reducing the volume of spam by increasing the cost of sending e-mail.[79] The first approach is to charge postage for every e-mail message sent.[80] The second approach is to increase the "cost" by requiring a payment in central processing unit ("CPU") cycles, for example requiring a complex computation before each message can be sent.[81] Sending bulk e-mail would become a much more time-consuming process.

77. *See* Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 1026 (S.D. Ohio 1997).

78. *See* Rowan v. United States Post Office Dep't., 397 U.S. 728, 737 (1970).

79. *See generally Can E-Mail Survive*, *supra* note 5.

80. *Id*. at 66.

81. *Id*. at 67.

These cost-increasing approaches attempt to place commercial e-mail on a more equal footing with other forms of solicitation, such as telemarketing and direct mailings. In theory, the number of these types of solicitations are limited by the costs imposed on the seller. For everyone using e-mail, this approach has the unfortunate side effect of increasing user costs. In particular, it increases the costs for anyone who wishes to send bulk mail, regardless of whether it is commercial or solicited. It is also unclear whether increasing the costs associated with sending spam will really reduce spam to a more acceptable level. The recent proliferation of do-not-call lists suggests that even relatively costly forms of advertising can rise to the level of an unwanted intrusion. Finally, simply increasing the costs of sending e-mail does not necessarily empower more effective spam regulation. Microsoft has recently backed away from this approach.[82]

Rather than increasing the cost of sending e-mail, another approach is to attempt to authenticate the legitimacy of the sender's address before allowing messages to be sent.[83] Yahoo has proposed a system called "DomainKeys" that will use digital signatures and the public key infrastructure to verify that a message actually was sent by the domain listed in the "From:" field (for example, in joeuser@aol.com, "aol.com" is the domain).[84] Another system with the same goal is the Sender Policy Framework ("SPF").[85] SPF attempts to match the Internet Protocol ("IP") address listed as the source of an e-mail with the IP addresses actually used to send e-mail from that domain.[86] This approach is primarily effective against the use of open relays and spoofed (or forged) sender addresses. SPF is more efficient than other systems relying on public key cryptography, but also needs to rely on blackhole lists to be really effective.[87] Finally, Microsoft has proposed "Caller-ID for Email,"[88] an

82. *See, e.g.*, Kevin Murphy, *Gates Backs Away from Postage Stamps Idea in Spam Vision*, COMPUTER BUS. REV., June 29, 2004, *at* http://www.computerbusinessreview.com/research_centres/59984863230a118e80256ec20032dda4.

83. Hiawatha Bray, *Tech Experts Say Spammers Are on the Run*, BOSTON GLOBE, Jan. 26, 2004, at C3, *available at* http://www.boston.com/business/technology/articles/2004/01/26/tech_experts_say_spammers_are_on_the_run/ [hereinafter *Spammers Are on the Run*].

84. Alex Salkever, *Yahoo's Risky Antispam Gambit*, BUS. WEEK ONLINE (Jan. 13, 2004), *at* http://www.businessweek.com/technology/content/jan2004/tc20040113_3442_tc047.htm.

85. SENDER POLICY FRAMEWORK, *What is SPF?*, *at* http://spf.pobox.com/howworks.html (last visited Sept. 1, 2004) (providing a general overview of SPF).

86. Wong & Lentczner, SENDER POLICY FRAMEWORK, *A Convention to Describe Hosts Authorized to Send SMTP Traffic* (Feb. 2003), at 3, *at* http://spf.pobox.com/draft-mengwong-spf-00.txt (Internet draft, expiration date July, 2004).

87. *See generally* SENDER POLICY FRAMEWORK, *Executive Summary*, *at* http://spf.pobox.com/execsumm.html (last visited Sept. 1, 2004).

authentication-based solution that was recently merged with SPF in a new standard called "Sender ID."[89] None of these authentication-based solutions are promising to identify the sender of a message. Instead, they try to make sure that a message has been sent from the domain from which it claims to have been sent.

DomainKeys and Sender ID both promise to allow message recipients to verify that the sender of a message has sent the message from his own domain.[90] They do not actually guarantee that the identity or physical location of the sender is known. The idea is that bulk messages sent by persons who do not use their own domain (i.e., johndoe@yahoo.com sending a message through hotmail.com) will be easier to spot and filter. Those who simply send spam from their own domain can be traced back to their ISP, and the ISP can either deal with them appropriately or be blacklisted.[91] This is a purely technical solution. It is also a step in the right direction, but stops short of reaching its full potential.

DomainKeys and Sender ID both fail to address an array of problems posed by spam and create a number of legal concerns. Spammers can continue to create accounts for one-time use and quickly dispose of them. They can still hack into innocent third-party computers and use them for sending spam through the ISP of the compromised machine (spam zombies). Unsolicited and solicited messages will not be differentiated any more easily. A message bearing a valid "From:" address could be protected political speech, pornography, a phishing scam,[92] or any other category of

88. *See, e.g.*, MICROSOFT CORP., *Caller ID for E-Mail Technical Specification*, *at* http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx (last visited Sept. 1 2004); Michael Singer, *Microsoft Proposes Caller ID for E-mail*, INTERNET NEWS (Feb. 25, 2004), *at* http://www.internetnews.com/ent-news/article.php/3317611.

89. *See* Press Release, Microsoft Corp., Sender ID Specification Submitted to Standards Body for Consideration (June 24, 2004), *at* http://www.microsoft.com/presspass/press/2004/jun04/06-24SIDSpecIETFPR.asp. Microsoft and the Internet Engineering Task Force have since had a falling out over Microsoft's license terms and intellectual property claims. *See* Reed Stevenson, *E-Mail ID Plan Rejected*, REUTERS (Sept. 14, 2004), *at* http://story.news.yahoo.com/news?tmpl=story&cid=581&e=1&u=/nm/20040914/tc_nm/tech_microsoft_security_dc.

90. *See Yahoo! Anti-Spam Resource Center: Domain Keys, at* http://antispam.yahoo.com/domainkeys (last visited Oct. 5, 2004); *Sender ID Framework at a Glance*, *at* http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx (Sept. 30, 2004).

91. *See Yahoo! Anti-Spam Resource Center: Domain Keys*, *at* http://antispam.yahoo.com/domainkeys (last visited Oct, 5, 2004).

92. *See* Russell Kay, *Phishing*, COMPUTERWORLD, Jan. 19, 2004, at 44 ("Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account

content. ISPs may still refuse to provide or be unable to provide the identity of the sender. Senders from blacklisted domains will likely have messages filtered, not for their own bad behavior, but because their ISP has not dealt effectively with spammers. ISPs can have their domains blacklisted without any chance to defend themselves or clear their names.

Although these technical responses to spam are largely fragmented, computer industry leaders have recently begun cooperating to work toward a common solution to spam. Industry leaders, including Microsoft, America Online, and Yahoo!, have joined to form the Anti-Spam Technical Alliance ("ASTA").[93] The group recently released a "Technology and Policy Proposal."[94] The alliance calls for an authentication-based framework for reducing spam, but the specific technology to be adopted has not been decided. The alliance fails to demonstrate much concern for First Amendment freedoms or the need to exist as part of a legislative framework. The authentication-based solutions that have been proposed fail to protect anonymous speech.[95] They also fail to go the last mile by providing the ability to associate an electronic address with a real person. Without identifying the sender, legal enforcement is unrealistic. Authentication-based solutions in their currently proposed form do not appear likely to solve the spam problem. However, an authentication-based architecture could be extended to enable a more effective regulatory solution when the design decisions are made with a legislative and policy framework in mind.

IV. ARGUMENT

A. Governing Principles

Much of the difficulty in regulating spam is derived from the largely unregulable nature of the Internet in its present form. On the technical level, the Internet allows for great anonymity as to both identity and location. Its overwhelming scale and decentralized architecture make effective monitoring unfeasible. From a legal perspective, the Internet does not fall exclusively within any jurisdiction. Effective regulation of the Internet in its current form is impossible due to the uncertainty as to

numbers and passwords, credit card numbers and Social Security numbers.").

93. Press Release, Microsoft Corp., Anti-Spam Technical Alliance Publishes Recommendations to Help Stop Spam (June 22, 2004), *at* http://www.microsoft.com/presspass/press/2004/jun04/06-22ASTAPR.asp.

94. *Id.*

95. Anonymous speech has been afforded substantial First Amendment protection. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995).

location, jurisdiction, and identity. Yet, the Internet is not immutable. As Lessig argues,

> Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its . . . code. This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. And while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well.[96]

When the code of the Internet is changed to increase regulability, there will be inevitable trade-offs. Within the realm of spam regulation, as identity becomes more readily ascertainable, then some privacy is sacrificed. As the content of e-mail is labeled and categorized, the possibility of censorship emerges. Once location is easily determinable, every government with an interest in Internet regulation becomes empowered to regulate the content of the Internet in some way. An architectural change for one particular purpose may be leveraged to accomplish regulation beyond that particular purpose.[97] For this reason, it is necessary to carefully scrutinize every architectural change designed to increase the regulability of the Internet to ascertain its full ramifications.

Legislative attempts to regulate spam must also be scrutinized carefully for unwanted effects. Spam legislation threatens to legitimize spam by providing safe harbor for those who engage in it.[98] Most unwanted spam is perpetuated by a small number of disreputable but determined persons. While having already experienced exponential growth, the problem could be exacerbated if more reputable businesses began exploiting the e-mail medium more aggressively. Additionally, national regulatory efforts such as the CAN-SPAM Act can preempt stricter state laws. While anti-spam legislation is clearly needed to remedy the market breakdown that has allowed the spam problem to spin out of control, we must be cautious in implementing statutorily imposed architectural changes. Architectural changes aimed at improving Internet regulability may later be wielded to undermine the freedoms embodied by the Internet of today. It is with a precautionary tone that this Note begins to outline the architecture of a system that enables more effective spam regulation.

B. A Different Approach

The proposed architectural changes are grounded in the Online

96. Lessig, *supra* note 1, at 506.
97. *Id*. at 519.
98. Sorkin, *supra* note 7, at 382-83.

community's common disdain for spam. In real space, societal norms are able to shape behavior. In cyberspace, norms do not possess the same ability to shape individual behavior.[99] The spammer does not come face-to-face with his angry audience. Peer pressure loses its force. No matter how large the spam problem becomes and how upset its recipients are, the spammers are not effectively dissuaded. Rather than changing the Internet's architecture to mandate an end to spam, architectural changes can be implemented that will have the effect of establishing societal norms for e-mail. Messages that deviate from these norms become easier to filter. Laws should be passed to stimulate the creation of these norms, thereby using the law as a catalyst for a technical solution.

1. Technical Overview

As a preliminary step, a general technical approach to dealing with the spam problem must be adopted. This Note argues for leveraging an authentication-based framework to enable more effective spam regulation. This approach is manifested in a number of systems being developed by private industry,[100] and inevitably involves a means of authenticating either the sender or the domain from which a message is sent. Authentication can be costly to implement,[101] but the remainder of this Note argues that an authentication-based system is more desirable as a matter of law and policy. The authentication-based architecture proposed by this Note attempts to meld the tools provided by both law and technology. While grounded in a technological framework, this architecture utilizes a legal regime that enables it to overcome the obstacles to reducing spam that a solely technical solution would be unable to achieve.

This Note argues for an architectural system built around the ability to digitally sign[102] and authenticate e-mail using public key cryptography.[103]

99. *See generally* Lessig, *supra* note 1, at 503-05 (discussing why cyberspace creates challenges not encountered in real space).

100. *Spammers Are on the Run*, *supra* note 85.

101. Authentication requires a computational overhead for every message handled. *See generally* SearchSecurity.Com, *DomainKeys*, *at* http://searchwebservices.techtarget.com/gDefinition/0,294236,sid26_gci944600,00.html (last visited Sept. 1, 2004).

102. In technical terms, a digital signature "is a special case of a message integrity code, where the code can have been generated only by one participant." LARRY L. PETERSON & BRUCE S. DAVIE, COMPUTER NETWORKS: A SYSTEMS APPROACH 589 (2d ed. 2000).

103. Digital signatures and public key cryptography work as follows: The individual signing the message will have two keys (very large prime numbers), a private and a public key. The recipient must know the sender's public key, but not the private key. A message (in this case, a signature) is encrypted by the sending party using his private key. The recipient receives the encrypted message and is able to decode it into a readable signature

In basic terms, a sender of a bulk message will digitally sign his message using his private key. The recipient of his message will obtain the sender's public key from a certification authority[104] (to be administered by a federal agency) and use it to verify the authenticity of the signature. By signing a message, the sender will indicate his assent to a regulatory code of conduct for signed bulk e-mail. A similar system for authenticating signatures is employed by the Pretty Good Privacy ("PGP") system for securing e-mail.[105]

The system described up to this point uses an authentication-based framework similar to those being proposed by private industry. In particular, DomainKeys proposes utilizing the public key infrastructure to authenticate the source of messages by using digital signatures. However, DomainKeys does not promise to do much more than enable users to determine the true source e-mail address and domain. It does not establish the actual identity of a message sender. This Note proposes extending this architecture to integrate legal enforcement and protections, distinguish between solicited and unsolicited messages, and fully protect free speech.

2. Extending the Authentication-Based Framework

The public key infrastructure can be extended to generate not only signed e-mail messages, but also to generate opt-in and opt-out signatures. Opt-in requests will be generated by individuals who create a signed request using their private key, either by Web or e-mail. The signed requests will be sent to the specified bulk mailer, who will be able to verify the signature with the certificate authority and keep the signed request as proof of the opt-in request. This process can and should be automated by e-mail clients wishing to incorporate this filtering technology. The opt-out process can be similarly automated. Individuals can send a signed request

using the sender's public key. *Id.* at 570, 589.

104. A certification authority is "an administrative entity that is in the business of issuing certificates." *Id.* at 591. The certificates in this instance are digitally signed documents originating from the governing agency that tell one individual the public key of another individual. *Id.*

105. PGP runs in conjunction with an e-mail program to enable users to sign and encrypt their messages. The Author proposes a method for signing documents which is similar, but does not suggest adopting message encryption as part of the proposed system. Encryption, quite interestingly, has the effect of making things much more difficult for both spam filters and spammers. The Author does not suggest a system including PGP message encryption because message encryption poses substantial challenges to scalability. This Author also does not intend to adopt PGP's decentralized certification structure, and instead proposes a more standard hierarchical structure built around government administered certification authorities. *Id.* at 599, 601. For background information, please see The International PGP Home Page at http://www.pgpi.org.

using their private key. An automated, signed response must be sent back by the bulk mailer. This response serves as proof that the opt-out request has been received. If the automated response is not received from the bulk mailer, the individual's e-mail program should send an automated complaint to agency servers. The signed requests are important because they can be automatically retained to provide documentary evidence to each party of its compliance or non-compliance with agency regulations. A signature can also require the entry of a password, an additional step that would make the use of spam zombies to create signed messages considerably more difficult.

At the root of the Author's architectural model will be a governmental agency, possibly the Federal Communications Commission ("FCC") or another organization by delegation.[106] This agency will be required to formulate and enforce spam regulations; it will also need to administer an authentication system. This administration process will involve governing the certification authority and facilitating the issuance of public and private keys.

The middle tier of the Author's model includes ISPs and software developers. ISPs will need to be responsible for the actual issuance of public and private keys to account holders. Keys should only be issued to account holders with valid mailing addresses. ISPs are more capable than government agencies of obtaining valid names and addresses for their own account holders as a result of ISPs' existing financial relationships with their customers. From an enforcement perspective, valid identification and contact information is necessary. From an administrative perspective, this information needs to be obtained accurately, quickly, and inexpensively. Only the ISPs are in a position to do this because they should already have access to this information for account holders. The free Web-based e-mail accounts that have proliferated in recent years would not be able to send signed messages under this system.

Software developers will need to implement the technical aspects of this regulatory model. Most major e-mail programs already attempt to handle some spam filtering. The features the Author has suggested can be implemented into existing e-mail programs. Protocols for implementing this architecture should be promulgated by a federal agency in conjunction with private industry. The opt-in and opt-out processes can be automated by e-mail clients and Web browsers to make the implementation painless for users. It is imperative that these opt-in and opt-out requests must be

106. The FCC is suggested, instead of the FTC, because the proposed system does not distinguish between commercial and non-commercial e-mail.

integrated into the user's software, rather than relying on the opt-out links of today that are created solely by the sender of a bulk message. As part of the opt-in process, the user's software must first verify the legitimacy of the bulk mailer's key and ensure that it has not been revoked. Because this proposed architecture builds on top of existing technology, any software developer should be capable of implementing the new protocols.

The lower tier of the proposed model includes both the average e-mail user and bulk mailers. Both types of individuals will need public-private key pairs in order to be included in the system. In fact, the success of this architecture is heavily dependent upon the network effects that will result from its broad adoption by users. It is only after broad user adoption that a substantial number of bulk mailers will feel the need to participate.

3. Proposed Regulatory Framework

This proposed regulatory framework is in and of itself an opt-in approach. Individual e-mail users, spammers, and ISPs will be free to determine whether they wish to participate. The cost to enroll in this regulatory program must be free. To require a payment could have the effect of placing a prior restraint on speech. Enrollment would entail a voluntary agreement to abide by agency regulations whenever sending digitally signed bulk messages. The purpose behind creating a voluntary regulatory system is not to simply abolish spam, but to make e-mail filtering easier for those who want to make themselves relatively immune from spam. As more people enroll in the program, reputable spammers will have little choice but to enroll if they wish to avoid having their messages filtered. The eventual success of the system ultimately depends on a large number of e-mail users and a few ISPs participating. It is from this foundation that societal norms for e-mail behavior may begin to take effect.

Spam filters should be able to identify most bulk messages and, from that point, distinguishing between signed and unsigned messages should be relatively easy. Individuals will have the option to have all unsigned bulk messages filtered. In addition, spammers will have to indicate whether their signed messages are solicited or not. Once again, users will have the ability to have the unsolicited messages filtered if they wish. The filtering will ideally be performed by ISPs, although any intermediary that relays a message will be capable of verifying the authenticity of a signature and dropping messages found to have forged signatures or revoked licenses. Individuals will be able to set their account preferences for filtering through their ISP's software. The ISPs are in turn free to allow very fine-grained filtering options or none at all. Under ideal circumstances, ISPs will offer a wide range of filtering options. Some will take a very aggressive stance

towards spam, and others will choose not to participate in the regulatory program at all (and their account holders will have to turn to another provider if they want to participate).

All e-mail users, whether participants in this regulatory framework or not, must be free to send unsigned bulk messages. Their messages risk being filtered before reaching some users, but this filtering will be the result of individual preferences and not government censorship. Users will still be able to send anonymous messages in bulk. They can retain their anonymity and full rights of speech. It is only when signing a message using the government issued key that they must abide by the government regulations. Those who violate regulations for signed bulk messages will be subject to agency enforcement and adjudication.

4. Defining "Bulk"

A complicated prerequisite for regulating all bulk e-mail is to define "bulk." By stipulating a certain threshold for a message being classified as bulk, the door is effectively opened to find ways to avoid crossing the threshold while still sending the same volume of messages. For example, if the definition of bulk e-mail is an e-mail message addressed to 1,000 or more e-mail recipients, then the simple way to circumvent the definition is to send multiple messages with 999 recipients each. An alternative definitional approach is to define bulk in terms of a message sending rate, such as sending messages to 5,000 addresses during a twenty-four hour period. This approach is better in principle, but suffers from technical limitations. It places a substantial burden on participating ISPs to expect them to maintain complicated logs of all received e-mails during a specified time period.

A more effective approach is to allow individual users or ISPs to define bulk. Once again users could set individual preferences for a threshold number of recipients to be classified as bulk. ISPs could also participate by factoring in the total number of messages they have been receiving from a certain e-mail or IP address. By avoiding a regulatory threshold for bulk mail, it becomes more difficult to circumvent that threshold.

5. Enforcement Procedures and Penalties

Admittedly, placing spam regulation enforcement power in the hands of a U.S. federal agency may solve interstate enforcement issues, but does nothing to solve international jurisdictional issues. For this reason, the primary means of enforcement must be technical. Repeated violations of regulations while sending signed messages will result in license (key)

revocation. When ISPs or other intermediaries attempt to verify the validity of a signature, they will receive a message indicating that the license has been revoked. Messages should then be automatically dropped.

6. Global Implementation

The system's global adoption will initially depend on allowing individuals to obtain a bulk e-mail license regardless of nationality. If the system gains popularity over the long run, it can be expanded to incorporate other nations' administrative agencies. The architectural root will necessarily remain in the United States to ensure that a consistent set of regulations remains in place, but the system can be expanded to incorporate numerous nations serving as certification authorities. As more nations begin to participate, international enforcement will expand from solely technical enforcement to encompass varying means of legal enforcement.

C. Scrutiny of Proposed Architecture

Any proposal to regulate spam should be subjected to stringent technical and legal scrutiny. The proposed architecture should be scrutinized according to a range of legal and technical considerations. Legal criteria should include narrow tailoring to spam, privacy preservation, transparency, the functionality of opt-out mechanisms, enforceability, and cost-effectiveness. These criteria are appropriate considerations for both the proposed architecture and other privately developed solutions.

1. Narrowly Tailored to Spam

Architectural changes should be no greater than required to enable more effective spam regulation. The fundamental problem in narrowly tailoring a system to spam is the difficulty in actually defining spam. Different people may have different ideas as to what types of messages they deem to be spam, and the differing views of spam are demonstrated by the different approaches that are being developed to stop spam. The authentication-based frameworks that have been proposed by industry may be effective in preventing spammers from using false return addresses and open relays, but this fails to reach a large amount of spam. For example, these solutions do nothing to address the spammer who uses a valid return address but refuses to honor opt-out requests. It also fails to slow down the use of spam zombies. The authentication-based solutions such as SPF will

also depend on the blacklisting of ISPs that fail to shut down spammers operating from their domain,[107] but as previously mentioned, this will result in e-mail being blocked from both the spammer and other innocent individuals using the same ISP. On the other hand, a postage-based approach directed at increasing the cost of sending bulk e-mail is both over- and underinclusive. It discriminates against solicited bulk e-mail and fails to deter messages sent through spam zombies. When a spammer takes advantage of a spam zombie, he does not end up paying the postage bill. Both of these approaches benefit from being content neutral, but fail to distinguish between solicited and unsolicited messages.

The system proposed by this Note easily complies with any narrow tailoring requirement. No filtering is mandated by the government. Both message senders and receivers are free to participate or abstain as they desire. The only classifications of messages imposed on those who participate is between unsolicited and solicited messages. Any decision to refuse unsolicited messages is made solely by message recipients. Instead of attempting to regulate the content of messages, this system simply provides e-mail users and ISPs with one key piece of information about messages that cannot otherwise be reliably obtained – namely, whether a message is unsolicited or not.

By differentiating between solicited and unsolicited messages, e-mail's potential as a means of mass communication is preserved. A system that solely targets bulk e-mail threatens to eliminate one of e-mail's greatest strengths: the ability to inexpensively and rapidly communicate with large numbers of people. Some individuals may wish to receive all forms of unsolicited bulk messages. The proposed architecture places the decision of whether to receive unsolicited messages squarely in the hands of e-mail recipients.

2. Privacy Preserving

An inevitable result of increasing Internet regulability by utilizing an authentication-based approach is to decrease privacy. Once senders are more easily traced and identified, privacy in one form has been lost. On the other hand, as users gain more control over what messages they receive, another form of privacy is enhanced. As a result, these two concerns must be balanced.

The proposed system does lead to the loss of some privacy. Signed messages are by their very nature not anonymous. This loss in privacy is

107. *See generally* SENDER POLICY FRAMEWORK, *Frequently Asked Questions*, *at* http://spf.pobox.com/faq.html#churn (last visited Sept. 2, 2004).

mitigated by both the optional nature of the system and the fact that only the sending of signed bulk messages is affected. Messages, even bulk messages, are not required to be signed. Unsigned messages simply have a greater probability of being filtered. The intent of the system is to motivate most senders of bulk e-mail to sign their messages, but the lack of a requirement that messages be signed is constitutionally significant.[108] Political speech, protest speech, and the like can still be sent anonymously. None of it is required to be filtered by law.

This is not to suggest that the simple preservation of the ability to send anonymous messages in bulk eliminates any concerns about lost privacy. By having a government-administered certificate authority, "big brother" will be able to connect signed messages with a name and address. Those who consider this to be an unacceptable sacrifice of privacy will be left to send unsigned messages or rely on other technical means such as PGP. Ultimately, this privacy trade-off is a necessary one. Without the ability to associate a signature with a name and address, there would be little hope of legal enforcement for the regulatory scheme.

Other aspects of the system are quite successful in preserving privacy, particularly the privacy of e-mail recipients. Users can filter unsolicited messages without ever having to indicate to their ISPs or a governmental authority which senders' messages they wish to solicit. The indication of whether a message is solicited is made by the sender, and the mechanisms of the opt-in system enable the sender to be held accountable for his affirmation. The threat of ISPs attempting to retain this information and use it for data-mining purposes remains. This threat should be dealt with by appropriate legislation prohibiting the retention of any solicitation information for any longer than is necessary to deliver a message.

3. Transparency

Giving users control over their inboxes requires that they know what types of messages are, and more importantly, what types of messages are not reaching their inboxes. A centralized filtering system that either relays or drops messages based upon the judgments of an undisclosed filtering algorithm undermines transparency. Blacklists are particularly vulnerable to claims of a lack of transparency.[109] IP addresses can be added to the

108. Anonymous speech has been afforded strong First Amendment protection. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (stating that "the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry").

109. Sorkin, *supra* note 7, at 356.

blacklists according to an unknown set of criteria, without concern for whether particular users may wish to receive messages from that address. The criteria for accepting or refusing e-mails should be user-controlled.

The proposed system enables more transparency by placing virtually all filtering decisions in the hands of intended message recipients. Blacklists and filters tend to operate under criteria unknown to users. By allowing users to set separate rules for unsigned bulk messages, unsolicited bulk messages, and solicited bulk messages, the end-to-end architecture of the Internet is maintained[110] and the transparency of the system is maximized.

Placing the system under administrative agency control guarantees greater legal and procedural transparency. Parties will enjoy the protections of the Administrative Procedures Act and due process when disputes over regulatory compliance arise. Unlike vigilante systems such as blacklists, parties will have notice of sanctions they face and will be given an opportunity to exonerate themselves.

4. A Functional Opt-out System

Spam messages have often provided an opt-out mechanism. Just as often these mechanisms have been non-functional or simply used to validate that an address is active.[111] Sometimes the system fails because return addresses have been spoofed. Often, it simply is not worth the trouble for spammers to remove names. If a message is sent to 5 million people, and 1 million reply with requests to be removed from the list, the time required to comply is too great if the process is not automated. A regulatory system needs to provide a standardized removal protocol that can be integrated into e-mail clients to provide immediate and verifiable removal.

Many would like to forego the burden of opting out by adopting a universal opt-in approach. The opt-in versus opt-out debate has proven to be particularly contentious in the European Union.[112] Some view this as a

110. End-to-end architecture refers to keeping the intelligence of the network toward the endpoints at the application level. The middle portions of the network should be simple and predictable to allow for a greater range of uses. This is because "complexity is the bane of scalability." Zittrain, *supra* note 8, at 686. The end-to-end architecture of the Internet is best preserved when filtering decisions are being made not by intermediaries, but rather by the intended recipients.

111. SCHWARTZ & GARFINKEL, *supra* note 12, at 72-74; Sorkin, *supra* note 7, at 352-54; Nasaw, *supra* note 5, at D2.

112. Magee, *supra* note 2, at 363.

choice between being an advocate for or an opponent of e-commerce.[113] The CAN-SPAM Act did not mandate the opt-in approach, but did call for the FTC to investigate the possibility of creating a universal opt-out choice (Do-Not-E-mail List).[114] Rather than explicitly choosing one approach or the other, the Author's approach aims to achieve the universal opt-out functionality (refusing all bulk e-mail) while still allowing a more refined opt-in or opt-out approach for those who prefer more fine-tuned control over the messages they receive.

This system's ability to handle opt-in and opt-out requests is one of its key strengths. It is fully automated and designed to protect both the message sender and recipient. Senders are able to prove when their messages were solicited, and recipients are able to provide proof that they have opted-out and that their request was received. This enables more efficient enforcement.

5. Enforceability

The lack of a legal remedy against those who perpetuate the spam problem is not the reason the spam problem has grown unchecked. Examples of legal remedies include the implementation of state anti-spam laws, the application of common law remedies, [115] and efforts to regulate spam undtertaken by both the United States and the European Union. While the jurisdictional issues and the technical difficulty in identifying spammers have contributed to the failure, the high cost of enforcement relative to small damages in individual cases of spam have made spam even more difficult to control. Legal enforcement must be quick and efficient, and private lawsuits should not be exclusively relied upon. Administrative enforcement is more desirable both from the standpoint of cost and efficiency, as well as the ability to bring technical resources to bear in tracking down spammers. The proposed system utilizes both technical and legal means of enforcement. The technical enforcement will involve revoking the license (keys) of those who violate the regulations for sending signed messages. Legal enforcement will include both procedural safeguards for those accused of violations and damages for those found to have committed violations. The technical enforcement should be very effective. Anyone who participates in the system is subject to technical

113. *Id*. at 363-64.

114. The FTC ultimately advised against the creation of a Do–Not-E-mail List. *See* Grant Gross, *FTC Declines Do-Not-Spam List*, PC World (June 15, 2004) *at* http://www.pcworld.com/news/article/0,aid,116536,00.asp.

115. Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1015 (S.D. Ohio 1997) (discussing trespass to chattels).

enforcement–jurisdiction is irrelevant. In contrast, only those in the United States or other participating nations will be subject to legal enforcement as a practical matter.

Technical enforcement should be adequate to maintain the proper functioning of the system. It will have the effect of removing violators from the system, but of course this does not prevent violators from sending spam. Violators will still be able to keep sending unsigned spam, or may try to register for another license. In realistic terms, solely relying on technical enforcement should reduce the amount of e-mail reaching participants' inboxes, but it does not necessarily reduce the amount of spam being sent. Legal enforcement is more likely to dissuade spammers. Ideally, the risks of legal enforcement will begin to outweigh the financial benefits of spamming.

6. Cost-Effectiveness

Elaborate systems for regulating spam quickly become very expensive. The burden imposed should be outweighed by the harm that would be caused by the unrestricted flow of spam over the Internet. In evaluating cost-effectiveness, the total cost of spam must be considered. Such costs include: payment for spam-filtering services and software, legal actions against spammers, and the social costs associated with spam, such as unsolicited pornography sent to minors.

The proposed system imposes high financial and technical costs. It requires governmental administration and enforcement. It asks ISPs and software developers to expand the functionality of their products and services. Nevertheless, these financial costs are justified by the increasing costs inflicted by unwanted spam. One technical cost imposed by the proposed system is that it does not claim to be able to stop the sending of spam. It instead focuses on enabling e-mail users to avoid ever receiving the unwanted spam messages. Spam can still be sent and passed across the Internet, all the way to the recipient ISP before finally being dropped by the ISP on the basis of a recipient's e-mail receiving preferences. Only in the limited circumstance where a signature is forged can a message bedropped by the sending e-mail server or an intermediary before it consumes bandwidth and storage space at the receiving end. This system does take some steps to minimize its technical costs. Most significantly, only signed and bulk messages will be affected by the changes. Unsigned messages may be treated just as they were before, although ISPs may begin to presumptively filter unsigned, bulk messages. Most personal messages will likely not be signed and have no need to be signed.

The only way to avoid imposing these technical costs is to place prior

restraints on the senders of spam. Examples of prior restraints include legislation prohibiting the practice and requiring postage for the sending of e-mail. Recent experience suggests that legislative restrictions are ineffective. Requiring postage would be effective in reducing bulk mail generally, because it does not distinguish between solicited and unsolicited messages, or even commercial and non-commercial messages. The disadvantage to requiring postage for e-mail is that it will discourage all attempts to send bulk e-mail. However, some bulk e-mail may be socially desirable. The postage approach appears to be overbroad in its impact (socially, even if not legally).

D. Avoiding the Pitfalls of ICANN

The suggested approach places control largely in the hands of a federal administrative agency. This approach leads to increased transparency, efficient administrative adjudication, and greater public accountability. However, this approach also does its share to complicate the solution. A privatized solution, perhaps administered by the Anti-Spam Technical Alliance, could largely bypass First Amendment scrutiny. Private arbitration could ultimately be much less expensive than that required by the Administrative Procedures Act ("APA"). An alternative to the agency-administered approach would be a privatized model in the form of the Internet Corporation for Assigned Names and Number ("ICANN").

ICANN is a private, nonprofit corporation that was created to administer the Internet's Domain Name System ("DNS"). The DNS system was created with grants from the United States military and National Science Foundation.[116] As international concern grew over leaving DNS exclusively in the hands of the United States, ICANN was formed for the express purpose of managing DNS.[117] ICANN's prominence as a type of private government overseeing the Internet has been the subject of much criticism.[118] Critics argue that ICANN has been impermissibly delegated administrative power to make policy without having to conform to the requirements of the Constitution and APA.[119]

Even if it is assumed that ICANN is solely a private organization, as some have argued, and not in any form a state actor, it then would be

116. A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 21-22 (2000).

117. *Id*. at 23-24.

118. *See, e.g.*, *Id*.; A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, 2003 U. ILL. L. REV. 1 (2003). *But see* Edward Brunet, *Defending Commerce's Contract Delegation of Power to ICANN*, 6 J. SMALL & EMERGING BUS. L. 1 (2002).

119. Froomkin, *supra* note 116, at 33-34.

subject to antitrust regulation.[120] ICANN has been permitted to operate as a monopoly. Once viewed as a monopoly, ICANN's mandatory dispute resolution policies and treatment of potential competitors becomes problematic.[121] ICANN has recently been targeted in an antitrust lawsuit filed by Verisign.[122] ICANN's future legitimacy remains in doubt due to widespread criticism and legal attack. The Internet's governing bodies of the future will need broad multinational support to obtain longevity and true legitimacy. At present, an agency-administered approach appears to be a safer solution than a privatized model.

V. CONCLUSION

Legal and technical responses to spam, working individually, have been ineffective in solving the problem. A more effective response will require combining legal and technological tools. Technology can enable more effective law enforcement by improving the ability of e-mail users to reliably identify message senders. Enforcement becomes possible. Technology can also be used to protect both e-mail recipients and senders by providing documentation of each party's compliance with regulations. The law can also work to make technological solutions more effective. By prosecuting those who break laws in the course of sending spam, spammers are more strongly dissuaded than they ever could be by filtering or other technological measures. When law and technology are each utilized with the goal of making the other part of the solution more effective, the whole becomes greater than the sum of its parts.

This Note has suggested a possible architecture for combining technological and legal means to reach a more effective result. Many details have been omitted and would need to be more fully developed for the system to be implemented. The purpose of this Note has not been to develop a perfect solution, rather it has been to demonstrate that the spam problem is too large and complex to be effectively solved by either the legal or technical communities acting alone. Architectural changes must be grounded in a solid legal and policy framework. Laws must be drafted not with the purpose of ending spam, but rather with the purpose of enabling technological solutions and providing for their enforcement.

In the realm of spam, it is the widespread disdain for spam that should be leveraged to attack the problem. There is no need to mandate an end to

120. Froomkin & Lemley, *supra* note 118, at 3.

121. *Id.* at 5.

122. Nick Wingfield, *VeriSign Files Antitrust Suit Against Web-Address Overseer*, WALL ST. J., Feb. 27, 2004, at A3.

spam when most consumers and commercial entities would voluntarily adhere to a set of spam regulations. The network effects of such a collaboration can ultimately be more effective than a purely legislative solution. As a critical mass of e-mail users voluntarily adhere to a regulatory framework, those who do not adhere become easier to identify. Spammers will stand out from the crowd and be more easily filtered. Law and technology can combine to make this collaboration between consumers and commercial entities possible.

Any attempt to combine legal and technical approaches to spam is presently inhibited by the abundance of competing technological and legal regimes that deal with spam. An architectural change to e-mail will require standardization. At present, there is no agreement for a new standard, although private cooperation is increasing. The involvement of a federal agency in adopting a standard could improve the likelihood of a standard being agreed upon, as well as legitimize its adoption. From that point, the door would be opened to broader international adoption and a cooperative technical and legal approach to reducing spam. Whether such cooperation will be achieved remains to be seen. The first step is for the legal and technical communities to initiate an open dialogue on how to develop their solutions with the needs and abilities of the other community in mind.