A Two-Tiered Registry System to Regulate Spam

By Shelley Cobos*

TABLE OF CONTENTS

INTRODUCTION

Although the Internet has emerged as an invaluable tool for conducting business in both our personal and business lives, some substantial problems have emerged that may threaten its very existence.[1] On the forefront of such problems is unsolicited commercial e-mail ("UCE") sent to unwilling recipients.[2] The most egregious form of UCE is "spam."[3] The problems associated with spam range from personal annoyance with small economic costs[4] to business disruptions with large economic repercussions.[5] Internet Service Providers ("ISP")[6] are likely the biggest sufferers of spam in terms of economic

---

* J.D., UCLA School of Law, 2003; B.S./B.S., University of California, Irvine, 1995. Special thanks to Security Exchange Professor Lynn M. LoPucki, my advisor for this comment. I also thank Kat Paterno, Michelle Alig, Robin Baessler, Christian Dodd, Eric Herbert, and Sara Jasper for their editorial support.

[1] *See* William S. Galkin, *The Law of Spam*, 1 COMPUTER LAW OBSERVER 20, Nov. 1996 (stating that "[s]pam has been credited with the power to bring down and destroy the Internet") *at* http://www.netlegal.com/vol1Is18.html (last visited July 28, 2003).

[2] *See* Anne Chen, *Stop the spam madness – Firm deploys filter to keep improper e-mail out,* eWEEK, Sept. 3, 2001, at 49 (interviewing David Ferris of Ferris Research, Inc. who estimates that unsolicited commercial e-mail will increase to 44 percent a day by 2005).

[3] "Spam" is distinguishable from "UCE." While both are unsolicited and commercial in nature, spam is really *fraudulent* in nature. *See* FTC Public Hearing Release, *Unsolicited Commercial Email (spam) May Chill Consumer Confidence in Online Commerce: FTC*, Nov. 3, 1999 *available at* **http://www.ftc.gov** (defining spam as "deceptive unsolicited commercial e-mail) (last visited July 28, 2003). Additionally, the words "bogus" and "scam" are used in most of the FTC's "The Dirty Dozen Spam Scams" list, connoting the fraudulent nature of spam, *available at* http://www.ftc.gov (last visited July 28, 2003). *But see* ALAN SCHWARTZ & SIMSON GARFINKEL, STOPPING SPAM 1 (Deborah Russel ed., O'Reilly & Associates, Inc. 1998) (defining spam as "an unsolicited, unwanted message sent to [the recipient] without [the recipient's] permission"). For purposes of this comment "spam" will be distinguished from "UCE" as particularly egregious or fraudulent UCE.

[4] *See* Michael A. Hiltzik, *The Spam Busters: A self-appointed global army is fighting the mass Internet mailings that annoy users and crash systems*, THE LOS ANGELES TIMES, Apr. 16, 2001, at A1 (reporting that "144,000 subscribers of Pacific Bell's Internet service repeatedly lost access to their e-mail for hours because servers were clogged with spam").

[5] *See* Laura Frewin, *E-business – Tarring e-mail pests with their own brush*, NETWORK NEWS, Jul. 25, 2001 *available at* WESTLAW, AllNews File (2001 WL 8762679) (quoting Lyris CEO John Buckman "'Spam is a big problem for businesses. Mail servers get overloaded and this can slow the system or even cause it to crash'").

[6] An Internet Service Provider is a company that provides individuals and business access to the Internet. An ISP has the equipment and the telecommunication line access required to have a point of presence on the Internet for the geographic area served. It is in the interest of ISP's to combat spam for two reasons: 1) loss of customers due to spam complaints and 2) a forced purchase of increased bandwidth to deal with very large volumes of e-mail. Additionally, the cost of personnel to control and administer spam-fighting tools can quickly add up. *See, e.g.,* Sharon Gaudin & Suzanne Gaspar, *The Spam Police; Tactics used by self-appointed spam fighters come under fire*, NETWORK WORLD, Sept. 10, 2001,. at 58 ("AOL Time

costs. ISPs have already begun protecting themselves from voluminous spam e-mails by employing filtering mechanisms[7] and by suing particularly arrant spammers on theories of trespass to chattel, breach of contract, and statutory violations.[8] The ISPs, however, are not the only ones suffering from the weight of voluminous and fraudulent commercial e-mail advertisements. It appears that most e-mail recipients regard spam as an annoyance with little economic or social value[9] and a number of mechanisms have already arisen to try and stop it.

Before the legislators enacted consumer protections against spam, filtering was the principal ways by which fraudulent UCE was dealt. Software was developed to filter out unwanted and fraudulent UCE using pattern-matching heuristics.[10] Filtering was also accomplished by subscriptions to "black lists" that listed domain name addresses of

---

Warner…spends up to 15% of users' monthly fees fighting spam. AT&T spends $35,000 per month, and WorldCom has 30 people dedicated to spam").

[7] Filtering mechanisms include both software that filters out unwanted spam and subscription to spam-friendly blacklists maintained by grass-root organization such as Mail Abuse Prevention System (MAPS). *See infra*, notes 25-41 and accompanying text.

[8] *See*, e.g., America Online, Inc. v. Nat. Health Care Discount, Inc., 121 F.Supp.2d 1255 (N.D. Iowa 2000) (holding that National Health Care Discount's contract e-mailers were liable to ISP America Online under the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act, and the theory of trespass of chattels for sending unsolicited bulk e-mail advertisements without authorization); CompuServe Inc. v. Cyber Promotions Inc., 962 F.Supp. 1015 (S.D. Ohio 1997) (holding defendant liable in tort under a theory of trespass to chattel to ISP CompuServe for failing to comply with CompuServ's request to stop sending unsolicited e-mail and for deliberately evading plaintiff's efforts to stop the mailings).

[9] *See* John S. Quarterman, *A Bad Spam Law*, MATRIX NEWS, Vol.8, July 1998, at 7 (stating that "[s]pammers cause ISPs and others to carry mass unpaid traffic that the vast majority of recipients do not want") *available at* http://www.mids.org/mn/807/spamlaw.html (last visited July 28, 2003); *but see* Mike Koller, *Direct E-Mail Without Spam – Schwinn divides newsletters by demographic and tracks reader behavior*, INTERNETWEEK, Oct. 1, 2001, at 12 (reporting that Schwinn saved $169,200 in annual savings be sending out 40,000 electronic newsletters rather than the traditional print newsletters).

[10] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 139 (stating that approaches to blocking spam at the system level "rely on…sophisticated pattern-matching heuristics to determine whether a given message might be spam"). For a simple example, consider a filter that would filter out anything in the subject line that began with "ADV," where ADV denoted an advertisement. The specific technology involved in these systems is beyond the scope of this comment. For a more complex explanation of filtering heuristics, see Marko Balabanovic, Yoav Shohan, & Yeogirl Yun, *An Adaptive Agent for Automated Web Browsing*, STANFORD UNIV. DIGITAL LIBRARY PROJECT *at* URL:http://historical.ncstrl.org/litesite-data/stan/CS-TN-97-52pdf (Feb. 1, 1997) (last visited Jan. 14, 2002).

"spammers, spam relays, or spam-friendly service providers,"[11] of which all messages originating by that domain name are blocked from ever reaching the recipient.

Spam legislation first emerged in the state of Nevada in 1997.[12] Since then, seventeen other states have enacted similar legislation.[13] Some of these statutes have been challenged on the constitutional ground that they either violate the First Amendment right of free speech or that they violate the dormant Commerce Clause.[14] While these laws are important steps in the fight against spam, their practical effectiveness remains to be seen.[15]

All of the mechanisms employed to fight spam are legitimate attempts to put reigns on the out-of control spamming industry. None of these measures, however, have the desired effect of stopping the most brazen of spammers. These are the spammers that use deceptive practices to send their UCE;[16] they are particularly skilled at circumventing road blocks created to stop their unwanted messages from ever reaching the recipient. For example, spammers employ such mechanisms as: forging headers to disguise the origin of the UCE;[17] putting in deceptive subject lines to trick the recipient into opening up their

---

[11] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 142.
[12] *See* NEV. REV. STAT §§ 41.705 – 41.735.
[13] California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Louisiana, Missouri, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, Washington, and West Virginia have all enacted state statutes regulating spam.
[14] *See* State of Washington v. Heckel, 143 Wash.2d 824 (2001) (holding that Washington Statute on Commercial Electron Mail Chapter 19.190 did not violate the dormant Commerce Clause and was therefore constitutional).
[15] *Compare* Farhad Manjoo, *She's the Sexiest Geek Alive*, WIRED NEWS, June 21, 2001, *at* http://www.wired.com (last visited July 28, 2003) (reporting that California resident Ellen Spertus won a judgment in a small claims court against Kozmo.com for sending UCE) *and* Jeffrey Benner, *Wham, Bam, Thank You Spam*, WIRED NEWS, Dec. 12, 2001, *at* http://www.wired.com (last visited July 28, 2003) (reporting that Washington resident Bennett Haselton won judgments totaling $2000 against spammers under the Washington anti-spam statute) *with* Steven Chase, *Spam under attack*, THE GLOBE AND MAIL, Apr. 5, 2001, at T1 (quoting Internet legal expert professor Michael Geist as asserting that legislation will not make a "huge difference").
[16] *See*, Frewin, *supra*, note 5 (reporting that "[s]pammers typically send over 100,000 messages at a time and - to avoid angry replies - not from their own systems").
[17] *See generally*, SCHWARTZ & GARFINKEL, *supra,* note 3.

UCE;[18] using open relays[19] of third party transmitters without their consent indicating that the UCE came from the non-consenting party;[20] and listing an invalid reply e-mail address circumventing recipients' attempts to unsubscribe from future mailings.[21] A mechanism for legitimizing commercial e-mails through federal regulation that is able to regulate and distinguish legitimate UCE from spam within the Internet community has yet to be employed.

The anti-spamming community disagrees about which legal measures are the most appropriate to control UCE.[22] There is even disagreement about how to define spam, whether spam is distinguishable from UCE, and the scope of protection either should be given, if any. Some classify all UCE as spam and therefore wish to annihilate it completely; others have a more reasonable view recognizing that not all UCE senders are spammers.[23] They do, however, agree on one thing: a universal solution is needed to regulate spam.[24] An appropriate solution would legitimize those businesses wishing to take advantage of e-mail marketing while preventing spammers from taking advantage of

---

[18] *Id*.
[19] See, *infra*, note 41.
[20] *Id*.; *also see*, Frewin, *supra*, note 5 (stating that "[i]ncidents of spam mail relaying on are on the rise" and stipulating that the .gov domain accounts for 38 percent and .co.uk domain accounts for 28 percent).
[21] *Id*.
[22] *See generally,* Matrix.net, Inc.'s website *available at* http://www.mids.org/nospam (last visited July 28, 2003). Matrix.net is an Internet performance analyst company that tracks, analyzes, and measures bits of information on the Internet. Their interest in reducing spam is high, since their products are designed to increase efficiency of businesses in e-commerce. In their "NoSpam" webpage, they list CAUCE as a resource to combat spam along with the stipulation that they "don't agree with their approach of new [spam] laws, but [they are] listed anyway."
[23] *See* Steve Hill, *Unwanted. Unwelcome. Unstoppable?*, INTERNET MAGAZINE, Vol. 3, Dec. 2001, at 64 (reporting that MEP Michael Cashman distinguishes spam as "'rain…[t]hey don't care where it lands'" from UCE, which according to Cashman "'is based on research from the marketers and is targeted.'" Cashman is a member of the European Citizens Freedoms and Rights, Justice and Home Affairs Committee, "which is currently considering legislation on spam").
[24] *See* Chris Oakes, *Free Spam Killing for the Masses*, WIRED NEWS, July 19, 1999 *at* http://www.wired.com (last visited July 28, 2003) (quoting CAUCE (Coalition Against Unsolicited Commercial E-mail) spokesman John Mozena as saying "'[Bright Light's filtering system] is a good stop-gap until we're able to find a more global solution to spam.'").

the practically unregulated Internet. Such a solution could potentially be obtained through a central registry system.

Part I of this Comment will review the advantages and disadvantages of the current mechanisms in place to regulate spam. Part II proposes a two-tiered registry system under federal control by which legitimate UCE may be separated from illegitimate spam so that the Internet's potential will not be rendered superfluous. Part III will explore the limitations of such a two-tiered registry system due to the topology of the Internet. The final part concludes this Comment.

Part I: CURRENT MECHANISMS TO CONTROL SPAM

A. Filtering by Software

Filtering is the most common mechanism currently used for controlling spam.[25] Any individual e-mail account holder can accomplish simple filtering by customizing his e-mail account to block specified senders, or by creating general rules using key words that block specific content. ISPs have employed filtering software that use key word filtering to stop spam from ever reaching its recipients. Some filtering software works by using specified key words to filter out unwanted mail.[26] Other software uses 'rule-based' filters that are programmed to reject any e-mail that does not conform to the established rule.[27] Yet other software uses pattern-matching heuristics to scan e-mail that could potentially be spam.

---

[25] *See* Raymond B. Everett, *Guerrilla Warfare: A System Administrator's Perspective on Unsolicited Commercial E-Mail*, Comments for the FTC Consumer Privacy Hearings 1997, at 2.19 (discussing filtering mechanisms as the most used technological developments to stop spam) *available at* http://www.everett.org/testimony/ftc (last visited July 28, 2003).

[26] *See, e.g.*, the website www.lyris.com/products/mailshield for a brief description of rule-based filtering.

[27] For example, a rule can be written "Reject the message if [text] appears in the Subject," where [text] can equal a derogatory word.

The principle problem with filtering software that uses rule-based filtering is that it can be indiscriminate.[28] For example, suppose one wants to explore safe sex options and searches the Internet for relevant information. The person is expecting to receive e-mail responses to inquiries made on the subject. If one uses the key word "sex" for a particular rule-based filter, the filter will not discriminate between an e-mail message that has the word "sex" in it with an e-mail that has the word "sex-change operation" in it. Thus, for obvious reasons, rule-based is not always effective.

Another problem with filtering software is that it uses the resources of the system administrator[29] to control spam. While many ISPs employ filtering mechanisms that bounce unresolved or rejected e-mail, a system administrator is still needed to review the message to determine if the e-mail was bounced due to a misconfigured computer.[30] Additionally, in businesses whose principle focus is not with the Internet, there must be personnel available to review the filtered out messages.[31] Thus, personnel costs needed to manage filtering software accrue to the businesses which may become costly to the business.

B. Filtering by Norms

Another type of filter employs the use of lists. These filters principally work by automatically blocking any e-mail message sent by a specific domain on a designated

---

[28] *See* Joyce Slaton, *What's the Worst &*#% Filter*, WIRED NEWS, Sept. 21, 2001, *at* http://wired.com (last visited Aug. 1, 2003)(quoting Digital Freedom Network Internet Development Director Alan Brown as saying that censorware [filtering software] is "ineffective at best;" and providing an example of how filtering can be ineffective with the following illustration: A would-be user named Sherrill Babcock was rejected as a registrant for censorware available at BlackPlanet.com. However, she was a successful registrant when she used the last names Babpenis and Babdildo).

[29] A system administrator is the person responsible for configuring, administering, and maintaining computers, networks, and software systems.

[30] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 7.

[31] *See* Anne Chen, *Stop the spam madness – Firm deploys filter to keep improper e-mail out,* eWEEK Sept. 10, 2001 at 49 (reporting that Rockwood Specialties, Inc. IT Director Mark Yankowskas "carefully review

list.[32] Currently, the most widely used[33] is the Realtime Blackhole List ("RBL") by the Mail Abuse Prevention System ("MAPS"), a nonprofit organization created to fight the problem of spam. MAPS is a grass roots organization that collects names of "spam-friendly" sites via complaints and adds them to their RBL.[34] While there is no legal authority backing MAPS,[35] their power to control spam comes from the fact that large ISPs actually purchase and employ their lists as a means of controlling spam.

One problem with list-filtering is that it is indiscriminate and can filter out legitimate e-mails.[36] Rather prophylactic, these lists are really reactionary in nature because the spam-friendly sites are only added after an abuse is reported or a pattern of abuse is observed. Thus, the first-one-loses (or, alternatively, the first-one-gets-through) principle prevails because a spammer can easily do a mass mailing by registering with a new ISP.

Besides subscribing to such commercially available lists, ISPs use their own personnel to filter incoming spam from spam-friendly sites.[37] When identification of a spam-friendly e-mail server is made, unless the host ISP clears up the problem quickly,

---

every quarantined message" to avoid legal issues) *available at* http://www.eweek.com/article2/0,3959,88457,00.asp.(last visited Aug. 1, 2003).

[32] *See* Everett, *supra*, note 25 at 2.19 (characterizing AOL's PreferredMail as filtering spam through lists).

[33] *See* Gaudin and Gaspar, *supra*, note 6 (reporting that "as many as half of the ISPs in the U.S. use [MAPS RBL] to block e-mail from…alleged spammers"); *see also,* SCHWARTZ & GARFINKEL, *supra,* note 3 at 142.

[34] There are a number of ways in which spammers are added to the list, including sending unsolicited bulk e-mail, leaving an open-relay on network, and hosting web pages that are promoted by spam. *See* Sharon Gaudin and Suzanne Gaspar, *How the blacklist system works*, NETWORK WORLD, Sept. 10, 2001, at 62.

[35] *But see* Media3 Technologies, LLC v. Mail Abuse Prevention System, LLC, 2001 WL 92389 (D.Mass) (denying a preliminary injunction on the grounds that MAPS placement of Media3 on their RBL list did not constitute defamation because the statement appeared to be true, did not amount to intentional interference with existing and prospective advantageous business relations because Media3 did not provide evidence of imminent business loss, and did not amount to unfair business practices although 1500 untainted websites hosted by Media3 were included in the RBL listing).

[36] *See* Jeffrey Benner, *Fixing a Hole Where Spam Comes In*, WIRED NEWS, July 19, 2001 *at* http://www.wired.com (last visited Aug. 1, 2003) (stating that as the efforts to control spam increase, "more and more legitimate e-mail is getting blocked along with the junk").

[37] *Id.* (quoting Tom Geller as stating that "ISP's block each other constantly").

an ISP will block that site automatically.[38] When this happens, legitimate e-mail may be blocked, never to be recovered.[39] This has financial repercussions for businesses in terms of lost communication and can cause personal inconveniences to individual users.

Another problem associated with filtering is that many spammers use deceptive practices when sending UCE. Forging headers[40] and open relays[41], for example, effectively circumvent filtering mechanisms. While many ISP User Policies prohibit such practices, complying with the provisions is left to good faith. Not surprisingly, a spammer who uses deceptive practices to purvey unwanted spam is unlikely to abide by such policies.

Finally, some have come out against these normative lists because they are completely unregulated. One prominent Internet legal scholar calls MAPS "self-righteous spam police."[42] Other ISPs, who have unwittingly hosted a spammer have had their entire network blocked, inconveniencing many of their innocent customers.[43]

C. Legislation

---

[38] *Id*.
[39] *Id*.
[40] Headers contain information regarding the origin of the e-mail.
[41] Open relays are routes within a network which allow senders of e-mail messages to route their messages through without authorization. Spammers use open relays to bypass their ISP in order to avoid penalties for the violation of their User Agreement provided by their ISP. This is an attempt by the spammer to disguise the origin of their spam. The recipient of a spam that went through an open relay would believe that the spam originated from an otherwise legitimate host. For example, a spammer recently used an open relay of the FAA's domain site to purvey spam. *See*, Bill Duncan, *FAA Asleep at the Control Column?*, RISKS DIGEST Vol. 21, Iss. 73, Nov. 5, 2001 *at* http://catless.ncl.ac.uk/Risks/21.73.html(last visited Aug. 1, 2003).
[42] *See* David G. Post, *A New Legal Paradigm: What Larry Doesn't Get: Code, Law and Liberty in Cyberspace*, 52 STAN. L. REV. 1439 at 1441 (quoting Larry Lessig from his column the *Industry Standard*). Larry Lessig is an Internet law professor at Stanford Law School.
[43] *See Media3 Technologies, LLC*, 2001 WL 92389 (D.Mass); *also see* Gaudin & Gaspar, *supra*, note 6 (reporting that MAPS listed iBill's entire block of IP addresses on the RBL when one of their thousands of customers had allegedly spammed MAPS).

In a relatively short period of time, a number of states have enacted legislation to combat spam.[44] Most of the legislation is aimed at truthfulness requirements when sending unsolicited commercial e-mail. The majority of the legislation prohibits falsified headers, router information, and subject lines[45], or requires mandatory subject line identifiers (i.e., ADV for advertisement or ADV-ADLT for adult advertisement) and mandatory opt-out instructions. Some even prohibit the distribution of spam-friendly software.[46]

One anti-spam statute[47] has already been challenged on constitutional grounds. In the State of Washington v. Heckel[48], the Supreme Court of Washington overturned the lower court's ruling that Washington's Anti-Spam statute violated the dormant Commerce Clause. The Court held that "the local benefits of the Act outweigh any conceivable burdens the Act places on those sending commercial e-mail messages," and, thus, the Act did not violate the dormant Commerce Clause.[49] This holding is promising for state anti-spam statutes because it upholds a state's right to regulate spam in order to protect its citizen.[50] Moreover, pending federal anti-spam legislation that effectively

---

[44] *See*, *supra*, note 13.

[45] Headers are identifying information about the source of a sent email. For legitimately sent e-mail messages, they contain accurate information regarding the date sent, the sender, and the recipient, in addition to a subject line and unique message identification number. However, this information can be falsified by spammers. *See* GEOFF MULLIGAN, REMOVING THE SPAM: EMAIL PROCESSING AND FILTERING 10 (1999) (stating that "[i]t is a trivial task for anyone to insert their own forged headers and quite often users wishing to hide their true identity (such as spammers) will create messages with fake `From` addresses, `Message-Id` lines, and especially phony `Received` headers.").

[46] Louisiana Rev. Stat. §73.6(B) (2003).

[47] Rev. Washington Stat. §19.190.010-.050 (amended 1999). Under the statute, it is a crime to send a commercial e-mail that contains false or missing routing information, a false or misleading subject line, or to use a third-party domain name without authorization.

[48] *Heckel*, 143 Wash.2d 824 (2001).

[49] *Id*. at 840.

[50] *But see*, Brett Arquette, *E-mail bill may fail to curtail spamming*, eWEEK, July 9, 2001, at 49 (arguing that the Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 95) will not have much of an effect on curbing spam if one looks at the history of ineffectiveness of the Telephone Consumer Protection Act of 1991) *available at* http://www.eweek.com/article2/0,3959,464756,00.asp (last visited Aug. 1, 2003).

mirrors state anti-spam statute's focus on truthfulness requirements[51] could eventually make the dormant Commerce Clause argument a moot point. The problem with this legislation, however, is that it simply makes it unlawful to use deceptive practices when sending fraudulent UCE (considered spam because deceptive practices are employed). Thus, a consumer does not have a choice as to whether or not he wants to receive UCE.

A weakness in the current legislation is that it does not take into account the cost-shifting effects of spam which burden everyone but the spammer.[52] Additionally, the law is generally reactionary in nature: it provides a remedy or recourse after the illegal act has been committed. Finally, it is often burdensome for even the most savvy of consumer-victims to take action: he must spend his time, energy and money identifying the spammer and learning the legal nuances of the court system. These problems make current legislation only a partial solution.

Part II: A PROPOSAL TO REGULATE SPAM: A TWO-TIERED REGISTRY SYSTEM

A. System Overview

The mechanisms that have arisen to combat spam have had some effect on their uncontrolled proliferation, but the serious problem of voluminous UCEs that threaten the usefulness of the Internet remains.[53] Businesses and fraudulent purveyors of UCE want to

[51] For example, pending legislation for the 108th Congress include the Ban on Deceptive E-mail Act of 2003 (S. 1052), prohibiting falsification or forgery of any electronic mail transmission information; the CAN-SPAM Act of 2003 (S. 877), mandating that identification, opt-out and physical address be included in any unsolicited e-mail transmission; and the Anti-Spam Act of 2003 (H.R. 2515), prohibiting commercial electronic email with false or misleading headers or subject headings For a brief summary, *see* spamlaws.com *at* http://spamlaws.com/federal/summ107.html (last visited Sept. 25, 2003).

[52] Cost-shifting is the externalization of costs associated with an activity in which one person profits at the expense of another. *See* SCHWARTZ & GARFINKEL, *supra*, note 3, at 6-11 (discussing the costs of spam on those other than the spammer).

[53] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 4-6 (arguing that "[t]he biggest problem with spam is that if it continues to grow unchecked, its electronic deluge threatens to crowd out all other legitimate messages,

send it, most businesses and individual users do not want to receive it without a method to opt-out.[54] The spammers of the world, however, have tainted the marketing potential of UCE by using fraudulent practices to purvey their mail.[55] Because of this, legitimate businesses are shying away from using UCE as a marketing tool.[56] On the other hand, there needs to be a control mechanism that will legitimize UCE to a certain extent so that legitimate businesses can still utilize this valuable marketing tool to reach those wishing to receive their electronic advertisements.

A sensible proposal is a system in which the ISP acts as a control stop for the delivery of UCE.[57] The ISP would be subject to federal regulation in the form of licenses issued to any ISP that sends and receives e-mail messages through their server. The scope

---

making the electronic commons of the 21st century an unusable cesspool of useless marketing messages."). The authors also assert that the very low costs associated with spam gives no incentive for spammers to target or control the output of their messages, thereby passing the costs off to everyone else – cost-shifting. Cost-shifting is considered an inefficiency of the free market, and, if not controlled, is detrimental to the economy. *See also*, CAUCE, *About the Problem: Cost-Shifting at* http://www.cauce.org/about/problem.shtml (last visited Aug. 13, 2003).

[54] *See*, *supra*, note 9.

[55] *See* Testimony of David Moore of 24/7 Media, Hearing on the Unsolicited Commercial E-mail Act of 2001 (H.R. 95) Before the Senate Communications Subcommittee, Apr. 26, 2001 (asserting that "enforcement mechanisms [regulating spam] should deter spammers from encroaching on the privacy of consumers and not penalize legitimate marketers who are adhering to the standards") *available at* http://www.senate.gov/~commerce/hearings/0426moo.PDF (last visited Aug. 13, 2003). 24/7 Media is a provider of online marketing and advertising solutions and services.

[56] *See* Testimony of Jerry Cerasale, House Telecommunications Subcommittee Hearing on Spam, Sept. 28, 1998 *available at* http://www.techlawjournal.com/congress/slamspam/80928cer.htm (last visited Aug. 13, 2003) (stating that "many current uses of unsolicited e-mail are not appropriate for legitimate marketing…[and] these current uses may well be poisoning the well of commercial e-mail in the minds of consumers.") Jerry Cerasale is the Senior Vice President, Government Affairs for the Direct Marketing Association, an organization that promotes and regulates direct marketing via mail, phone, and now the Internet. *See also*, Testimony of David Moore, *supra*, note 54, (asserting that the "interactive marketing industry has been tainted by the actions of disreputable marketers who use deceptive practices in sending unsolicited commercial electronic mail.").

[57] Presently, the State of Washington has a registry system implemented that allows a resident of Washington to opt-out of UCE and also requires a sender of UCE to check the registry to verify that an address on his marketing e-mail list is not registered. If the sender of UCE sends his mail to a registrant on the registry, he will suffer criminal penalties. However, the procedure is quite cumbersome. The sender must input each e-mail address individually and then wait for an e-mail address that will indicate whether or not the e-mail address is registered. For more information on the registry, visit http://registry/waisp.org/ (last visited Jan. 14, 2002[unable to find this site). The constitutionality of the Washington Anti-Spam statute, of which the registry was its practical application, was the issue of contention in State of Washington v. Heckel, 143 Wn.2d 824 (2001). *See*, *supra*, note 46 and accompanying text.

of the license would be limited to regulation of UCE only. The proposed system is not meant to supplant any of the current mechanisms in place to regulate spam. Rather, it is merely a proposal to legitimize the UCE industry and could potentially put the reigns on illegitimate spammers while preserving the right of legitimate businesses to market their products through UCEs.

B. System in Action

Before being able to operate, an ISP would be required to file for a license with the FCC. The license would require that the ISP use the FCC's mandatory National Registry of Businesses ("NRB") to screen voluminous e-mail messages. Additionally, the ISPs would be required to disclose to their new customers the availability of an FCC optional National Registry for Opt-out UCE ("NROU) for users only.

The National Registry of Businesses would serve as a single tracking source for businesses/individuals sending out mass commercial e-mail mailings.[58] The object is to legitimize UCE by providing a check and balance before it is delivered to recipients who do not want it. Any business or any individual wishing to send unsolicited commercial[59] bulk e-mail would be required to register with the National Registry of Businesses and pay a small fee. A law requiring the e-mail marketers to register would provide the incentive for businesses or individuals to register. By law, businesses are already required to register as corporations, an LLC, an LLP, or record their fictitious business names in locations accessible by the public, for example. Mandatory registration with the NRB would be but another requirement for those businesses or individuals who wish to take

[58] The system articulated in this Comment does not contemplate unsolicited bulk e-mail (UBE) for political, religious, or non-profit purposes. That class of e-mail may have heightened constitutional considerations in relation to federal regulation not relevant to commercial e-mail.

advantage of low cost marketing e-mail tools. By charging a small fee, egregious spam purveyors will be less likely to register multiple times with the NRB since they will have to pay for each registration.

Currently, spammers use the deceptive practice of sending out relays of spam from different addresses so as to avoid cancellation of their ISP accounts for their fraudulent practices.[60] This is frequently done from websites issuing free e-mail addresses.[61] Part of the attraction for spammers is that they accrue little cost in sending mass volumes of spam, while the servers, ISPs, and individual users of e-mail absorb the costs (cost-shifting).[62] The business would have to provide identifying information to the FCC, including a valid contact e-mail response address. The FCC would oversee identification verification.[63]

The National Registry for Opt-out UCE would function as a master check list for those e-mail users who never wish to receive UCE. Upon opening an account with an ISP, the user would be informed of their opportunity to opt-out of UCE by registering with the NROU. If the user chooses to opt-out, his e-mail address will be automatically forwarded to the NROU. If the user later changes his mind, he will be able to register at the NROU directly through the FCC website. If the user does not choose to opt-out, he will receive UCE. If the user wishes to receive some UCE, but not all UCE, he can still

---

[59] For the purposes of this proposal, "commercial" means an advertisement that promotes the commercial availability of a product or service for profit.

[60] *See* Heckel*,* 143 Wash. 2d 824 (2001). Defendant-Heckel registered multiple free accounts with juno.com in order to prevent discontinued access by Juno's cancellation of his accounts used for practices in violation of their User Agreement. "[W]hen Juno canceled one e-mail account, [Heckel] would simply open a new one and send out another bulk mailing." *Id.* at 830.

[61] For example, hotmail.com, yahoo.com, and juno.com all issue free e-mail addresses.

[62] *See generally*, CAUCE, *supra* note 53. (discussing the cost-shifting effects of spam on ISPs, including the costs of filtering, bandwidth purchases, outages, while pointing out the spammer accrues virtually no cost); *see also,* SCHWARTZ & GARFINKEL, *supra*, note 3, 50.

customize his own e-mail account with personal filters and take advantage of the current ISP filtering mechanisms in place. Electronic newsletters from businesses with which the individual or business has had an existing relationship will not be subjected to the requirements of the registry since this form of communication is not considered unsolicited in nature.

Upon receipt of a volume of e-mails that are detected by the ISP as being substantially similar or upon detection of an emerging pattern of bulk e-mails, the receiving ISP would automatically hold the mail while checking the senders e-mail address against the NRB. If the check comes back okay (i.e., the business/individual has registered), the mail will then automatically be checked against the NROU. If the e-mail recipient's address is not on the list, the mail will then be delivered.

If the NRB check comes back negative, the mail will be transferred to a hold server while the sender is notified by an auto-responder. If no response is received within 3 business days, the mail would be permanently deleted. If the sender did not have a validly registered address on the NRB and the auto-response remains unanswered by the sender, these two factors will serve as a complete defense for any liability on the part of the ISP.

C. Policy Considerations

Although it may at first glance seem unfair to put the weight of stopping spam on the ISPs, they are in the best practical position to do so. Already they are at the forefront of stopping spam by suing abusive spammers; [64] employing filtering mechanisms to

---

[63] For a discussion on identification verification, see LYNN M. LOPUCKI, INFORMATION LAW: A SYSTEMS APPROACH 459-469 (2001).
[64] *See supra*, note 8.

control spam;[65] utilizing personnel to manage spam and responding to customer complaints of spam;[66] and increasing their bandwidth to deal with voluminous amounts of spam.[67] The ISPs have both the technology and know-how to fight spam, and have the best economic incentive.[68]

A useful analogy to understand why ISPs are ideally suited to regulate spam is the model of the credit reporting system. The ISPs are private entities like the credit reporting agencies, both in a good position to function as a control mechanism. The proposed licensing requirement would provide the incentive for the ISPs to regulate spam.

The agency most capable of managing and maintaining a national registry is the Federal Communications Commission.[69] Not too long ago, the FCC took a "hands-off" stance to regulation of the Internet.[70] In a 1997 document, however, the U.S. government

---

[65] *See supra*, notes 25-43 and accompanying text.
[66] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 7; *see also supra* text accompanying note 30.
[67] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 4-6; *see also supra* text accompanying note 53; Rik Farrow, *Putting a Stop to Spam*, NETWORK MAGAZINE, Nov. 1, 2001, at 80 (stating that spammers "steal server time and network bandwidth"), *available at* http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703232&classroom= (last visited Aug. 14, 2003).
[68] *See* James Niccolai, *Users look to ISPs to fight spam, survey finds*, IDG NEWS SERVICE, June 14, 1999 (stating that "[m]ost users think their Internet service provider (ISP) should help protect them from spam mail, and a significant number will switch to another ISP if it doesn't [according to a survey]") *at* http://www.idg.net/idgns/1999/06/14/UsersLooktoIspsToFight.shtml (last visited Aug. 14, 2003). The article also reported that "7 percent of respondents cited spam as their primary reason for switching to another service provider…[which] translates into about US$7 million a year in lost revenues."
[69] *See* About the FCC at http://www.fcc.gov/aboutus.html (last visited Aug. 14, 2003) (the FCC is "charged with regulating interstate and international communications by radio, television, wire, satellite and cable"); *but see* the proposed legislation Unsolicited Commercial Electronic Mail Act of 2001§ 3, 6(H.R. 95) *available at* http://www.spamlaws.com/federal/107hr95_this_bill_was_not_enacted.html (last visited Aug. 14, 2003) (defining "Commission" as the Federal Trade Commission in section 3 and designating the Commission as the enforcement agency in section 6). The FTC, charged with regulating "unfair and deceptive practices" is a natural candidate for the pending legislation since their provisions mostly deal with truthfulness. The FCC in my proposed system, on the other hand, would act prophylactically to prevent dissemination of spam in the first place and issues related to unfair and deceptive practices would still fall under the jurisdiction of the FTC.
[70] *See* William E. Kennard, *Connecting the Globe: A Regulator's Guide to Building a Global Information Community*, June 16, 1999, FCC document *available at* http://www.fcc.gov/connectglobe (last visited Aug. 14, 2003) (stipulating that the absence of regulation has allowed the Internet to flourish and that "[a] 'hands-off' approach [of the FCC] allows the Internet to develop free from the burdens of traditional regulatory mechanisms.").

did reserve the right to some forms of future regulation of the Internet.[71] The U.S. government may not have fathomed the Internet's significant role in future commerce and personal transactions and, thus, may have been hesitant to regulate the burgeoning Internet during its "growth-spurt." Regardless of its past "hands-off" stance, the Internet's graduation from infancy to adolescence has clearly shown that the problem of spam is ripe for regulation. Evidence of the need for regulation can be seen in both the state enacted anti-spam laws during the past four years and the pending federal anti-spam bills of the 107th Congress.[72]

D. How the System Addresses the Problem of Spam

There is a general sentiment that all UCE is unscrupulous in nature,[73] which is very unfortunate since responsible e-mail advertising had significant marketing potential before its abuse by spammers.[74] It is well established, however, that UCE has lost its attractiveness for legitimate businesses that do not wish to be categorized with spammers and thus lose their reputation and business opportunities with present and future

---

[71] *See id*. (reciting the principle that "[w]here government involvement is needed [for regulation of the Internet], it should support a predictable, minimalist, consistent, and simple legal environment for commerce").

[72] The bills introduced in the 107th Congress were the Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001), the Wireless Telephone Spam Protection Act, H.R. 113, 107th Cong. (2001), the Anti-Spamming Act of 2001, H.R. 718, 107th Cong. (2001), Anti-Spamming Act of 2001, H.R. 1017, 107th Cong. (2001), the Netizens Protection Act of 2001, H.R. 3146, 107th Cong. (2001), and the "CAN SPAM" Act of 2001, S. 630, 107th Cong. (2001). Most of the laws reflect similar provisions of the state laws. *See*, Brett Arquette, *supra*, note 50.

[73] *See About the Problem* by CAUCE *at* http://www.cauce.org/about/problem.shtml (asserting that "very few reputable marketers us[e] UCE to advertise goods and service" and listing the most commonly seen UCE advertisements as "chain letters, pyramid schemes, 'get rich quick' schemes…, offers of phone sex lines and ads for pornographic web sites, offers of software for collecting e-mail addresses and sending UCE, offers of bulk e-mailing services for sending UCE, stock offerings for unknown start-up corporations, quack health products and remedies, illegally pirated software").

[74] *See* Eric Schlachter, *The Intellectual Property Renaissance In Cyberspace: Why Copyright Law Could Be Unimportant On The Internet*, 12 BERK. TECH. L.J. 15, (1997) *available at* http://www.law.berkeley.edu/journals/btlj/articles/vol12/Schlachter/html/reader.html (last visited Aug. 15, 2003) (asserting that "other media industries [besides the Internet] indicate that multi-billion industries can be built primarily on advertising").

customers.[75] The proposed system will help to legitimize UCE as a useful tool for those willing to receive it. Accountability through registration at the NRB is the first step towards legitimization. By registering, a business or individual is saying "Yes, we use UCE as a marketing tool, we use it responsibly, and we will remain definitively identifiable to sort out any problems that arise from our advertisements."

Spammers, on the other hand, will not be legitimized through this system. Spammers use deceptive practices[76] to purvey their spam. With the registry system, voluminous spam will be stopped from being delivered at the ISP level unless it passes through the two-tiered registry system (and is therefore, arguably legitimate). Although it is unrealistic to expect to stop all spam from ever reaching all unwilling recipients, the system will at least present some significant hurdles for spammers that currently take advantage of the virtual non-regulatory status of the Internet today. Additionally, it will give legitimate businesses and individuals the opportunity to seek valuable business opportunities by using UCE as a marketing tool for those willing to receive it.

Although NROU registration requires an affirmative act on the part of the user, the opt-out solution is more reasonable than an opt-in solution. Presently, the hardliner anti-spam organizations[77] support opt-in only for UCE. Their complaints regarding opt-out lists are based on the principle that they never asked to receive spam in the first place; that spammers include opt-out provisions in their mailings but do not honor them; and on the principle that opting out of one list will not cover all mailing lists and thus the proliferation of spam will continue. The two-tiered registry, however, addresses these

[75] *See supra*, notes 56-58 and accompanying text.
[76] *See infra*, notes 104-8 and accompanying text.

concerns. First, there is only one global opt-out list, which means that the user only has to take action one time. Second, there will be a certain level of legitimacy of the UCE because of the identification mechanism inherent in the registry. Senders of UCE will be required to include a valid e-mail address or they will suffer criminal penalties. Finally, their complaint that they did not ask to receive the advertisements in the first place ignore the economic value of advertising.

To be sure, the proposed system does not completely remedy the cost-shifting effect of spam on the ISPs. They are still going to be the first line of defense. Some of the costs, however, would be shifted upon the UCE senders in the form of registration fees.[78] Additionally, there will be other costs to implement the two-tiered registry system. The most obvious repercussion is that the cost will be passed on to the consumer. This should not destroy the idea, however. Everyday we pay for many regulatory activities – public utilities, financial institutions, aviation to name a few – in the form of taxes because the simple truth is, some people refuse to obey the law. For an unregulated system such as the Internet, the potential for abuse is high because anonymity is easy to obtain and borders are seemingly invisible.

Part III: PROBLEMS WITH THE SYSTEM

A. Topology of the Internet

---

[77] *See generally*, the organizations of CAUCE (Coalition Against Unsolicited Commercial E-mail) *at* http://www.cauce.org; MAPS (Mail Abuse Prevention Program) *at* http://mail-abuse.org; and the spam prevention discussion group SPAM-L *at* http://www.claws-and-paws.com/spam-l.

[78] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 5 (comparing the high costs of traditional paper advertising with the extremely low costs of e-mail advertising and asserting that the low costs of e-mail advertising do not give the spammer any incentive to target his message).

Given the current configuration of the Internet, the logistics of the proposed two-tiered registry system will be difficult to implement. This is partly due to the topology of the Internet.[79] No one actually "owns" the Internet. The Internet is simply a system of interconnected networked computers that receive and relay information. The idea of a networked communication system (later to become the Internet) was conceived by information technologists and researchers who worked for a government agency called ARPA[80] during the 1960's.[81] Their goal was to interconnect computers at different geographical locations in order to share data processing amongst the connected computers and ultimately to save money.[82] At the time, private industry did not have a say in the development of the Internet (they arguably did not know it existed either) and therefore, a commercial application for it was not contemplated by its designers.[83] Consequently, the developers of the Internet did not foresee any reason for regulating it at that time. The Internet is now effectively in the public domain.[84]

The various networks[85] that compose the Internet are connected by the same cable and wireless system used by the telecommunications industry. In fact, the major ISPs,

---

[79] *See* Chase, *supra* note 15 (stating the "the problem [with controlling spam] is inherent in the design of the Internet.").
[80] ARPA stands for the Advanced Research Projects Agency.
[81] *See* STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET 39 (2000) (stating that the "Information Processing Techniques Office…of ARPA …buil[t] the foundations of the networked information economy which surrounds us today").
[82] *See id.* at 59 . Vint Cerf, one of the original designers of the pre-Internet technology, commented:

> The trouble was that ARPA was asked repeatedly to buy the best computing equipment for each one of the universities on the grounds that you couldn't do…quality computer science without the best computers…[but ARPA] couldn't afford to keep doing that every year for every place…so the question was, how do I hook them together to do resource sharing, which was the original motivation for the ARPAnet.

Id. The ARPAnet was the predecessor of the Internet. *Id*.
[83] *But see id.* at 73 (relating the reluctance of AT&T, the long-distance telephone monopoly, to become involved in the development of ARPAnet during 1967-1969).
[84] *See* Am. Libraries Ass'n v. Pataki, 969 F.Supp. 160, 164 (S.D.N.Y. 1997) (stating that "The Internet is [now] a decentralized, global communications medium.").

also called backbone providers, are the telecommunication giants.[86] Some backbone providers are interconnected with other backbone providers at independent Network Access Points in addition to their own dedicated access points called Metropolitan Access Exchanges.[87] Smaller ISPs are connected to backbone ISPs, while even smaller ISPs are connected to the ISPs connected to backbone providers. The more connectiveness there is amongst the various systems, the more efficiently and quicker information travels. Connectivity and efficiency, however, come with the price of trackability. The interconnected computers communicating with each other will deliver any given e-mail message through the path of least resistance. This means that a computer will not discriminate between routers to which a given e-mail will pass, making the travel pattern of the e-mail random. Ultimately, this means that spam can travel through many networks to reach its final destination and, therefore, it may be more difficult to track.

B. What is an ISP?

Since the proposed system uses the ISP as the stop-gap for controlling spam, understanding the function of the ISP and defining the ISP is relevant. An ISP is a private entity that provides an access point for individuals to enter the public global Internet. The ISPs have the equipment and point of access needed to enter the domain of the Internet. Individual and businesses users generally use local ISPs[88] to access the Internet.

---

[85] A network is a series of points or nodes interconnected by communication paths. For purposes of this Comment, a network will be defined as the series of points maintained by an ISP, whether it is a private or public entity maintaining the server.

[86] *See* KEITH SUTHERLAND, UNDERSTANDING THE INTERNET: A CLEAR GUIDE TO INTERNET TECHNOLOGIES 138 (2000). The larger ISPs are referred to as backbone providers and include AT&T WorldNet, Cable & Wireless, UUNet, BT to name a few. Other backbone providers include IBM Global Network, MCI, Netcom PSINet, to name the most popular.

[87] *Id.* at 138-39.

[88] By local ISP I mean any ISP other than the telecommunication giants which are considered backbone ISPs.

Backbone ISPs, however, can also serve as an individual or business direct point of access.

The Online Copyright Infringement Liability Limitation Act also provides a useful definition. The Act defines "service provider" as both "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing" and as "a provider of online services or network access, or the operator of facilities therefor."[89] This broad definition seems to encompass almost any network. For practicality's sake, however, the ISP should be defined as the first network server to encounter the mass mailing – the usual case being the spammer's ISP. Even if an illegitimate UCE purveyor "spoofs"[90] the header, the first network server to receive the mailing would still have an obligation to check the NRB to make sure that the purveyor was registered.

A spammer may be interested in bypassing his local ISP for risk of termination of his account for violation of the ISP User Agreement prohibiting using the network for spam-related activities. If a user wishes to access the Internet by bypassing a local ISP, he needs to obtain his own dedicated T1 line, [91] an inconvenience to those spammers who rely on the virtual cost-free, hassle-free nature of the Internet to deliver their unscrupulous marketing ploys. Additionally, even if one obtained a dedicated, high-speed connection bypassing a local ISP, a backbone ISP has the ability to terminate this

[89] *See* the Online Copyright Infringement Liability Limitation Act, 17 U.S.C.S. § 512(k)(1)(A)-(B) (1998).
[90] Spoofing means that an e-mail sender deliberately changes the From: line of the header information in order to disguise its origins.
[91] *See* SCHWARTZ & GARFINKEL, *supra* note 3 at 25. In order to bypass ISPs and gain independent access to the Internet, Cyber Promotions, Inc.'s Sanford Wallace "obtained his own high-speed T1 connection to the Internet's backbone."

connection.[92] Since two big attractions for spammers are the low cost and the hassle-free nature of the spamming, purchasing a dedicated line for most spammers is impractical. Also, in light of the perception that spam is dubious in nature, spammers probably do not want to attract attention to themselves by purchasing a dedicated line that would give them a permanent IP address that would be easily traceable. It is assumed for the purposes of the proposed two-tiered registry system, therefore, that principle access to the Internet is via an ISP.[93]

C. Registry Problems

A principle problem with the registry system is that a spammer could obtain a legitimate address registered on the NRB to legitimize their spam and force it to come through. If the spammer forges a header and the mail looks like it is from a legitimate business or individual, the system will have been circumvented and the spam will be delivered. Thus, a legitimate business name could be "hijacked" and cause the expenditure of financial resources and discredit to the reputation of the legitimate business. This problem may be solved by criminalizing the use of a business or individual's registered business name without authorization to send bulk e-mail. Alternatively, the NRB could be made to be secure and confidential with the use of SSL and encryption.[94] It would be easy for a spammer, however, to obtain the legitimately registered address once the first bulk mailing was sent by the business. The mailing would make the address public and therefore, free to use by fraudulent spammers.

---

[92] *See id.* at 28. Cyber Promotions' Sanford Wallace's "high-speed Internet connection…was [eventually] terminated by Sprint, his upstream ISP."

[93] This is a general assumption. There are ways in which spammers can deliver their spam by bypassing the ISP in which they hold an account; *see infra* notes 103-5 and accompanying text.

[94] *See generally*, SUTHERLAND, *supra*, note at 77-98. SSL stands for Secure Socket Layer and is a form of certification exchange for authentication purposes.

Therefore, the best solution is probably to make illegal the unauthorized use of a registered business address.

D. How Does e-mail Work?

The way in which e-mail is ultimately delivered to the recipient has bearing on the proposed system and may present problems. E-mail transmission uses a protocol called Simple Message Transfer Protocol (SMTP)[95] through port 25.[96] Standard protocols are used so that different computers can understand each other - a universal standard language for computers. When a user logs on to the Internet via his ISP, the ISP assigns the user an IP[97] address from a range of IP addresses that the ISP owns. Alternatively, an IP address can be permanently assigned to a user who holds an account with the ISP (this is the best case scenario since the individual or business with a permanently assigned IP address is always traceable). Once logged on, a user can create an e-mail message and send it via SMPT. The ISP is the *first network* to encounter the e-mail message. It recognizes that the message is from its user because the message has a label on it that the ISP recognizes – the IP address that it temporarily or permanently assigned to the user. After recognition, the ISP's network disseminates the e-mail through routers until it reaches its ultimate destination. The ISP cannot predict which router through which the e-mail will travel to reach the addressed to recipient.

---

[95] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 48 (explaining SMTP as the standard protocol by which e-mail is relayed); *also see*, SUTHERLAND, *supra*, note 86 at 55.
[96] *See* SCHWARTZ & GARFINKEL, *supra*, note 3 at 47 (explaining that services such as e-mail, Use net, and web pages are assigned ports to designate that service so that the computers can understand what the user wishes to do).
[97] *See id.* at 43-4 (explaining Internet Protocol (IP) addresses).

ISP's have the capability of knowing who sent an e-mail message if it hits their server.[98] An ISP ("primary ISP") accepts a message either directly from the originator of the message, in which case the ISP will know that the message was sent from someone who has an account with the ISP; or from another ISP ("secondary ISP"), in which case the primary ISP will know the identity of the secondary ISP because the secondary ISP is paying the primary ISP money to carry its Internet traffic. This means that a given e-mail message cannot be sent unless the ISP is willing to take and deliver it. This is, of course, assuming that the ISP's network does not host an open relay, which essentially "launders" the originator's identifying information.[99] So, an ISP could know that it is the first network to receive a bulk spam if it receives it from an originator.

In the proposed system, therefore, since the ISP of the sender would generally be the first network to encounter the spam, they have the most control over its dissemination. Thus, the ISP of the spammer is the stop-gap and would be required to follow the protocol for verification with the registries as per their license. While many ISPs already disallow the dissemination of spam via their networks in accordance with their User Policies, other ISPs do allow dissemination or are considered spam-friendly sites by maintaining open relays.[100] Therefore, a license requiring ISPs to check legitimacy with the registries would force them to stop this practice.

E. Deceptive Practices by Spammers

---

[98] *But see*, *id.* at 85 (stating that "[t]he spammer's ISP may not know that its computers are being used to send spam"). This, however, is most often the case when an ISP is not policing its own system very well. With the licensing requirement, the ISP would be required to police their system or suffer revocation of their license or other penalties.

[99] *See*, *infra*, notes 103-5 and accompanying text for an explanation of open relays.

[100] *See* Farrow, *supra*, note 67 (reporting that open mail relays are still available in 20% of ISPs as of 1999).

To purvey their spam, dubious spammers will use deceptive practices in an attempt to circumvent the registry system by bypassing their Internet Service Provider (who is serving as the stop-gap). The two most popular mechanisms that spammers use are "spoofing" headers and using open relays to deliver their spam to recipients who are unwilling to receive it.

Spoofing involves using someone else's e-mail address or a completely fictitious one[101] in order to trick an ISP who may have a filter blocking all e-mail from the spammer's real address or his spam-friendly domain site. It also involves altering the message header to disguise the spammer's origins. With the registry system, a fake address that the spammer uses will be automatically checked by the ISP against the NRB. Criminalizing the use of a legitimately registered address without authorization and the use of addresses from throw-away accounts will serve as a deterrent to spammers.[102]

Relaying is the practice of using a third party server without authorization to deliver e-mail. A spammer has only to send one message to a third party server with an open relay site instructing it to deliver voluminous amounts of spam. The result is that the recipient believes the spam to have been originated from an ISP other than the spammer's ISP.[103] Spammers use this technique in order to disguise the origin of their e-mail and avoid filters.[104] This is probably the single-most unresolvable problem with the proposed two-tiered registry system. If the spammer can effectively bypass his ISP, then the ISP

---

[101] *See*, Farrow, *supra*, note 67.
[102] Spammers may use throw-away accounts to purvey their spam. This is a common practice since free e-mail addresses are allowed, such as those offered by Hotmail, Yahoo, and Juno. *See*, *supra*, note 61.
[103] *See* MULLIGAN, *supra*, note 45 at 19 (stating that "[s]pammers…use relays to hide their real identities and locations. By sending a message through a relay system, the spammer can make it look like that system was the originator of the message. Therefore, if mail from the spammer's site is blocked, a message from the relay site probably isn't").
[104] *See* Chip Rosenthal, *What is Third-Party Mail Relay*, *available at* http://mail-abuse.org/tsi/ar-what.html (last visited Aug. 27, 2003) for a detailed explanation of third-party relays.

can no longer act as the stop-gap for controlling dissemination of spam or unwanted UCE. This problem, however, may be remedied by designating all network systems[105] as "ISPs," and thus requiring them to check the registries before delivering.

F. Volume of e-mail

Another problem associated with the proposed system is how to define a volume of e-mail that will constitute spam. Would 10 or 100,000 identical or almost identical messages constitute a spam mailing? In theory, the ISP would have to be able to detect identical or substantially similar messages coming from a sender in large quantities in order to determine whether or not is was spam or unwanted UCE. As mail servers are set up now, however, they generally ignore the content of the message.[106] Alternatively, the ISP may detect spam or unwanted UCE by sheer volume. Upon receipt of a specified quantity of email coming from a single e-mail address, regardless of the legitimacy at this point, the ISP would automatically assume that it is spam or unwanted UCE and would go through the registry system to assess legitimacy.

The problem is the quantity of e-mail that would trigger the ISP to perform its licensed duty. If for example, the trigger volume is defined at 100, a spammer would most likely send out packages of 99 spam e-mails at varying time intervals in order to avoid detection. The ISPs, however, already have capabilities for recognizing spam through pattern-matching heuristics and other such filters.[107] The software they employ could conceivably recognize patterns of unwanted e-mail. If, for example, the ISP server

[105] *See, supra*, note 85.
[106] *See*, Farrow, *supra*, note 67 (stating that mail servers generally ignore the content of e-mail).
[107] *See*, *supra,* note 10.

detected 100 e-mails coming from a single user in a half of an hour's time,[108] this volume pattern may be an alternative trigger to causing the ISP to first check the registry before disseminating the messages.

Part IV: CONCLUSION

E-mail has become the most widely used technology on the Internet today. As such, preventing e-mail from becoming a tool of abuse should be a top priority within the Internet community. As the deceptive methods and software technologies used by spammers become more sophisticated, the incentive for spammers to self-regulate themselves by targeting their mail and respecting an individuals right to opt-out from their mailings decreases. At the same time, deceptive practices of spammers have given UCE, in general, dubious undertones.

Arguably, no one quite foresaw the important commercial advantage that the Internet presented in its early stages. UCE could have (and may yet) become an important means for generating revenue from the Internet. As it stands now, however, legitimate businesses do not want to use this tool because of the negative association with spam.

The mechanisms that have arisen to combat spam are important developments in the fight against spam. Legitimate businesses and individuals hoping to take advantage of electronic commercial advertising should have that right as long as a proper mechanism is in place to control it. The proposed two-tiered registry system that could legitimize UCE would provide this proper mechanism.

---

[108] It is not likely that a single human user could compose 100 messages in a half of an hour's time. Therefore, this may trigger the ISP that such a volume of e-mail is being composed and sent by some type

of automation.