CANNING SPAM: CONSUMER PROTECTION OR A LID ON FREE SPEECH?

GRANT C. YANG[1]

ABSTRACT

The United States Congress recently passed the first federal legislation to curb the influx of spam. However, the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act") left some measures to be enacted by the Federal Trade Commission ("FTC"), and some consumers are calling for the Act to have a broader reach and for the creation of a Do-Not-E-Mail registry. Conversely, the FTC decided to delay the creation of a registry and opted to assist in the development of a new technological authentication system. This iBrief looks at the current state of spam and explains that it is too early to tell whether the effects of the CAN-SPAM Act warrant new anti-spam measures. In addition, it points out that it is questionable whether the FTC's current authentication approach will be effective, and, thus, considers the possible First Amendment challenges to a Do-Not-Call registry as well as other possible anti-spam solutions. In the end, this iBrief postulates that the most effective option might be for the FTC to implement both a Do-Not-Email registry and an authentication system.

INTRODUCTION

¶1 E-mail has become an integral part of life on the Internet, but like many great communication media it has been tainted by unsolicited commercial communications; unsolicited commercial e-mail is commonly referred to as "spam." Spammers recognize the convenience and efficiency of e-mail, and make significant profits while interfering with consumer usage. The economics of spam are fairly simple. A retailer's goal is to maximize profits by minimizing costs,[2] and advertising is a cost.[3] To

---

[1] B.S. in Computer Science, Stanford University, 2001; Candidate for J.D., Duke University School of Law, 2005; Candidate for LL.M. in International and Comparative Law, Duke University School of Law, 2005. The author would like to thank Professor Erwin Chemerinsky for his comments.

[2] Eric Allman, *The Economics of Spam*, DISTRIBUTED DEVELOPMENT, Dec./Jan. 2003-2004, *available at* http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=108 (last visited Mar. 7, 2004).

[3] *Id.*

maximize the effective use of advertising, the retailer casts as wide a net as possible in a direct marketing scheme.[4] Since the cost of spam is almost negligible, it often makes sense to use e-mail as the primary advertising medium.[5]

¶2 However, society bears a great cost as a result of spam. Recipients of spam suffer because they, or their employers, must shoulder the substantial cost of setting up complex mail servers, maintaining hard drives to store the e-mail, and implementing spam filters.[6] In addition, in the workplace, spam can result in a significant loss of productivity.[7] For example, because spam is already estimated to constitute over half of all e-mail traffic,[8] there is a concern that if spam increases at its expected exponential rate, companies will not be able to support the increased costs of bandwidth and hard drive space.[9] One study estimates that spam costs a business $847 per employee per year in lost productivity alone.[10] Furthermore, society will bear the cost of spam if e-mail becomes a less useful form of communication.[11]

---

[4] *Id.*

[5] A spammer can get an Internet connection, buy spam addresses or harvest them on his own, buy spamming software, and easily start churning out millions of spam messages. *See* Peter Griffin, *Spammers Remain Unrepentant As They Make Money*, THE NEW ZEALAND HERALD, Mar. 21, 2003, *available at* http://www.nzherald.co.nz/storydisplay.cfm?storyID=3251095&thesection=technology&thesubsection=generalhttp://www.nzherald.co.nz/storydisplay.cfm?storyID=3251095&thesection=technology&thesubsection=general (last visited Nov. 17, 2004).

[6] Allman, *supra* note 2; Marguerite Reardon, *Finding A Way to Fry Spam*, NEWS.COM, Feb. 24, 2004, *at* http://news.com.com/2008-1032-5164246.html?tag=nefd_gutspro (last visited Nov. 30, 2004).

[7] *See* Reardon, *supra* note 6.

[8] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2 (a)(2), 117 Stat. 2699, 2699 (2004).

[9] *See* David Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 338-39 (2001).

[10] Paul Roberts, *Report: Spam costs $874 per employee per year*, INFOWORLD, July 1, 2003, *available at* http://www.infoworld.com/article/03/07/01/HNspamcost_1.html (last visited Nov. 11, 2004).

[11] Spam filters may decrease e-mail's usefulness as a form of communication because spam filters may filter out e-mail that is desired or users may stop using e-mail as an integral part of communication. Reardon, *supra* note 6. A 2003 e-mail study also found that employees spend an average of one hour and 47 minutes using e-mail, and 86% of respondents found that e-mail made them more efficient. Lisa M. Bowman, *E-mail's up—is the boss watching?*, ZDNet, June 18, 2003, *available at* http://zdnet.com.com/2100-1104_2-1018562.html (last visited Nov. 17, 2004).

¶3 This iBrief looks at the effects of current and proposed federal anti-spam legislation. In particular, it considers the possible implementation of a Do-Not-Email registry or a new technological authentication process, including possible constitutional and logistical challenges. In the end, this iBrief postulates, the most effective option might be for the federal government to implement both a Do-Not-Email registry and an authentication system.

I. THE CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003

¶4 Though many states had already enacted anti-spam laws, the United States Congress' first anti-spam action did not come until 2003, when it passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act");[12] the CAN-SPAM Act was signed into law by President Bush on December 16, 2003 and went into effect on January 1, 2004.[13] The CAN-SPAM Act largely delineates certain requirements for sending commercial e-mail and proscribes ancillary methods used by fraudulent spammers to harass consumers.[14] Specifically, it prohibits the use of false-header information[15] and deceptive subject headings,[16] while requiring that the e-mail contain certain content, such as a mechanism to opt-out of receiving future commercial e-mail from that sender,[17] a warning label if the commercial e-mail contains sexually oriented material,[18] and the sender's physical postal address.[19] The CAN-SPAM Act also prohibits many other fraudulent activities associated with spam, such as utilizing open relays,[20] hacking into computers to facilitate

---

[12] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 2 (a)(2), 117 Stat. 2699, 2699 (2004) [hereinafter CAN-SPAM Act].
[13] *Id*. at § 16.
[14] *Id.* §§ 4 & 5. For a concise summary of the requirements and penalties of the CAN-SPAM Act, visit http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm (last visited Nov. 17, 2004).
[15] CAN-SPAM Act §§ 4(a)(3) & 5(a)(1).
[16] *Id.* § 5(a)(2).
[17] *Id.* § 5(a)(3).
[18] *Id.* § 5(d).
[19] *Id.* § 5(a)(5)(A)(iii).
[20] *Id.* §§ 4(a)(2) & 5(b)(3). An open relay is an insecure computer used by third parties to retransmit e-mail messages. *See Open Relay*, WHATIS.COM, *at* http://whatis.techtarget.com/definition/0,,sid9_gci782509,00.html (last updated July 19, 2004).

the transmission of spam,[21] registering for false e-mails or domain names,[22] address-harvesting, and dictionary attacks.[23]

¶5 The CAN-SPAM Act was one of many proposed federal legislations, and has been highly criticized for not being harsh enough in its requirements and limitations.[24] For example, California State Senator Bowen (D-Redondo Beach) criticized the CAN-SPAM Act's adoption of an opt-out mechanism, which she found to be weaker than her opt-in proposal.[25] The CAN-SPAM Act has also been criticized for not recognizing a private cause of action.[26] Rather, actions must be brought by state Attorneys General,[27] Internet Service Providers,[28] or primarily, the Federal Trade Commission ("FTC").[29] Despite these criticisms, it is too early to tell whether additional measures must be taken by either the FTC or by Congress.

---

[21] CAN-SPAM Act § 4(a)(1). Hacking into a computer is gaining accesses to a computer without authorization to use to send multiple transmissions using that computer.

[22] *Id.* § 4(a)(3). Registering for a false e-mail or domain name is to use a false name to represent oneself when registering for an IP address or e-mail.

[23] *Id.* § 5(b). Harvesting addresses is using some type of automated method to parse web pages or other online forums to gather e-mail addresses. Dictionary attacks are an automated method of creating random e-mail addresses using letter combinations that are sent to an e-mail server and then determining which addresses are valid, based on responses from the e-mail server. *See* Grant Yang, *CAN-SPAM: The First Step to No-Spam*, 4 CHI-K. J. INTEL. PROP. 1, 5 (2004), *at* http://jip.kentlaw.edu/art/volume%204/4-1-2.htm (last visited Nov. 23, 2004).

[24] For a listing of proposed legislation from the past three years, *see* http://www.spamlaws.com/federal/index.html (last visited Nov. 17, 2004).

[25] Susan Kuchinskas, *California Senator Slams 'Can Spam'*, CLICKZ NEWS, Nov. 14, 2003, *at* http://www.clickz.com/news/article.php/3109531 (last visited Nov. 17, 2004). An opt-in system requires recipients to explicitly request to receive the e-mail; whereas, in an opt-out system, spammers may send e-mails to all but those who explicitly opt-out. Sorkin, *supra* note 9, at 374. Many commentators have argued that an opt-in approach is better for consumers partly because opting-out takes too much time and also confirms the e-mail address to the spammer. *See* Richard C. Balough, *The Do-Not-Call Registry Model is not the Answer to Spam*, 22 J. MARSHALL J. COMPUTER & INFO. L. 79, 86–87 (2003).

[26] *CANNING SPAM: Federal Government Preempts State Legislation Regarding Unsolicited Commercial E-mail Messages*, GORDON & GLICKSON LAW FORUM, at http://www.imakenews.com/ggalert/e_article000222696.cfm?x=a2JKslM,a18jwlg9 (last visited Sept. 27, 2004).

[27] CAN-SPAM Act § 7(f)(1).

[28] *Id.* § 7(g)(1).

[29] *Id.* § 7(a).

¶6 The FTC has some flexibility to enact and administer additional spam regulations,[30] such as creating a Do-Not-E-Mail registry[31] or requiring additional labeling.[32] Such additional regulations may be warranted, as the success of the CAN-SPAM Act in its first year has been much-debated. Already, AOL cites a 27% decline in spam and an almost 50% decrease in daily spam-related complaints from customers over a period from February 20 to March 17 of 2004.[33] On the other hand, some reports have indicated that spam volume has risen since 2002.[34] It may take some time to accurately measure the effect that the CAN-SPAM Act will have on the quantity of spam. Furthermore, there are mixed reviews from the industry regarding whether the CAN-SPAM Act will ever be effective.[35]

II. DO-NOT-E-MAIL REGISTRY

¶7 One potential expansion of the CAN-SPAM Act, which may implicate First Amendment issues, is to implement a Do-Not-E-Mail registry. The CAN-SPAM Act gave the FTC six months from its date of

---

[30] *Id.* § 13.
[31] *Id.* § 16.
[32] *Id.* § 11(2).
[33] *AOL Chew Fat on Sliced Spam*, REUTERS, Mar. 19, 2004, *available at* http://news.com.com/2100-1024-5176278.html?tag=nefd_hed (last visited Nov. 17, 2004).
[34] *Spam Volume Keeps Rising*, NEWS.COM, Sept. 1, 2004, *at* http://news.com.com/Spam+volume+keeps+rising/2100-1032_3-5339257.html?tag=nefd.top (last visited Nov. 17, 2004).
[35] *Compare CAN-SPAM Act*: *Full Committee Hearing*, 108th Cong. (2004) (statement of Ronald Scelson, Scelson Online Marketing) (stating that "CAN SPAM Act is working and working well"), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1199&wit_id=2094 (last visited Nov. 17, 2004), *with CAN-SPAM Act*: *Full Committee Hearing*, 108th Cong. (2004) (statement of Peter Brondmo, Senior Vice President, Digital Impact, Inc.) (asserting that "the CAN Spam Act is unlikely to eliminate the hard core spammers, especially those sending viruses and perpetrating 'phishing' attacks – the most dangerous form of spam"), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1199&wit_id=3438 (last visited Nov. 17, 2004). In other words, some think the CAN-SPAM Act can act as a deterrent, whereas others view that the difficulty of finding and catching spammers will not deter the particularly hard-core spammers. Therefore, even with a cause of action, it is argued that spammers may not be deterred. However, this begs the question of whether harsher penalties are needed to deter spammers from flagrantly violating CAN-SPAM; the current sentencing guidelines for CAN-SPAM are already being criticized as too harsh by the National Association of Criminal Defense Lawyers. Paul Festa, *Stiff Spam Penalties Urged*, NEWS.COM, Apr. 14, 2004, *at* http://news.zdnet.com/2100-1009_22-5191651.html (last visited Nov. 17, 2004).

enactment to study the feasibility and effectiveness of establishing a Do-Not-E-Mail registry.[36] In June 2004, the FTC released a report delineating its findings, and advised against implementing a Do-Not-E-Mail registry at that time.[37] The FTC considered three potential types of Do-Not-E-Mail registries: "a registry of individual email addresses, a registry of domains, and a registry combined with a certified third-party email forwarding service."[38] The first two types of registries are intuitive: that is, a user can register an e-mail address or a domain name and spammers would not be allowed to send to those addresses or domain names.[39] The third type of registry considered allows a spammer to submit his distribution list to an FTC-approved third party forwarding service, which then matches the e-mails on the distribution list with those on the Do-Not-E-Mail registry and forwards the spam to those users not on the registry.[40] After considering all three registry types, the FTC determined that there were significant security and privacy concerns,[41] general technical concerns,[42] and obstacles to enforcement.[43]

¶8 The proposal of a Do-Not-E-Mail registry has received popular support from the general public.[44] Some have even said that the registry is integral to the CAN-SPAM Act's success.[45] Many spam opponents feel that spam legislation should employ an opt-in mechanism,[46] and the registry

---

[36] CAN-SPAM Act § 9.
[37] FEDERAL TRADE COMMISSION, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS ii (2004) [hereinafter "REPORT TO CONGRESS"], *available at* http://www.ftc.gov/reports/dneregistry/report.pdf (last visited Nov. 17, 2004).
[38] *Id.* at 13.
[39] *Id.* at 14-15.
[40] *Id.* at 15.
[41] *Id.* at 15-23.
[42] *Id.* at 26.
[43] *Id.* at 23-26 (stemming largely from the difficulty of tracking spammers and forcing them to obey the law).
[44] Pamela Parker, *Do-Not-Spam Proves Popular Concept*, CLICKZNEWS, Dec. 23, 2003 (study showed that 84% of Americans were extremely or very likely to register on a Do-Not-Spam registry), *at* http://www.clickz.com/news/article.php/3292361 (last visited Nov. 17, 2004),
[45] *Do-Not-Spam List Is Crucial to Make Current Law Work*, THE MERCURY NEWS, Feb. 20, 2004, *available at* http://www.mercurynews.com/mld/mercurynews/news/opinion/7998096.htm. (last visited Nov. 17, 2004).
[46] Stefanie Olsen, *California 'Disempowered' By Federal Spam Law*, NEWS.COM, Jan. 22, 2004 (stating that the Federal Spam law preempted the stronger California anti-spam law which was opt-in and gave individuals more power against spam),

would make the CAN-SPAM Act a de facto opt-in law.[47] Meanwhile, others, like FTC Chairman Tim Muris, have expressed serious doubt about the registry's effectiveness.[48] In addition, some opponents are concerned that it would just give spammers millions of valid e-mail addresses to spam.[49]

¶9 Most importantly, an effective registry must be robust in order to counteract the weaknesses mentioned in the report. For example, use of third-party intermediaries would provide the most security; however, the FTC found that doing so would "deprive legitimate bulk e-mailers of key marketing data."[50] The FTC further argued that the use of such a system would increase the cost to legitimate marketers and take away "key components to any marketing strategy – measuring the success of the campaign and understanding the customer."[51] Thus, although a registry would further protect consumer privacy, it also has the potential to impinge on legitimate marketers' First Amendment rights. To determine whether an expanded Do-Not-E-Mail registry could withstand constitutional scrutiny, it is helpful to examine the legal precedent provided by the recent judicial challenge to the Do-Not-Call registry.

¶10 The Do-Not-Call registry is "a list containing the personal telephone numbers of telephone subscribers who have voluntarily indicated that they do not wish to receive unsolicited calls from commercial

---

at http://news.com.com/2100-1028_3-5145849.html?tag=st_rn (last visited Nov. 17, 2004).

[47] A registry would require a one-time opt-out and thereafter the user would need to opt-in to receive commercial e-mail.

[48] *FTC Chief's Doubts On Do-Not-Spam List Remain*, ASSOCIATED PRESS, Mar. 12, 2004, (Chairman Muris had expressed doubt about the registry even before the passage of the CAN-SPAM Act), *available at* http://www.wral.com/technology/2919192/detail.html (last visited Mar. 20, 2004); David Ho, *FTC Chair: Do-Not-Spam List Won't Help*, ASSOCIATED PRESS, Aug. 19, 2003, *available at* http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=44014 (last visited Nov. 17, 2004).

[49] Janis Mara, *FTC Requests Vendor Input on Do-Not-Spam List*, CLICKZNEWS, Feb. 24, 2004, *at* http://www.clickz.com/news/article.php/3316911 (last visited Nov. 17, 2004). In fact, one scam website tried to set itself up as a registry in order to fool people into providing their e-mail addresses. *"Do-Not E-mail" Site a Scam, U.S. Officials Say*, REUTERS, Feb. 13, 2004, *available at* http://www.usatoday.com/news/nation/2004-02-13-no-spam-list-scam_x.htm (last visited Nov. 17, 2004). *See also* Marc Simon, *The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional?*, 4 J. HIGH TECH. L. 85, 93-94 (2004), *available at* http://www.jhtl.org/V4N1/JHTL_Simon_Note.pdf (last visited Nov. 23, 2004)

[50] REPORT TO CONGRESS, *supra* note 37, at 28.

[51] *Id.* at 30-31.

telemarketers."[52] The Do-Not-Call registry, originally established under the Telephone Consumer Protection Act of 1991,[53] is a joint effort between the FTC and the Federal Communications Commission ("FCC") under the Do-Not-Call Implementation Act,[54] and both agencies have promulgated the rules governing the Do-Not-Call registry.[55] Under the Do-Not-Call registry regulations, telemarketers have up to three months to remove phone numbers listed on the registry from their call lists; however, only personal phone numbers may be listed[56] and the list does not apply to non-telemarketers, such as political organizations, charities, telephone surveyors, or companies with which consumers have an existing relationship.[57]

¶11 In *Mainstream Marketing Services Inc. v. FTC*,[58] the Court of Appeals for the Tenth Circuit recently upheld the constitutionality of the Do-Not-Call registry, holding that it did not violate the limited First Amendment protection provided to commercial speech.[59] The Supreme Court uses a form of intermediate scrutiny in evaluating commercial speech.[60] In *Central Hudson Gas v. Public Service Commission*,[61] the Supreme Court articulated a four-part intermediate scrutiny analysis used to determine whether a government regulation violates commercial expression under the First Amendment: (1) the speech must concern lawful activity and not be misleading; (2) the government interest must be substantial; (3) the regulation must directly advance that government interest; and (4) the regulation must not be more extensive than necessary to serve that

---

[52] Mainstream Mktg Servs., Inc. v. F.T.C., 358 F.3d 1228 (10th Cir. 2004).
[53] Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991) (codified as amended at 47 U.S.C. §227 (1994)).
[54] Do-Not-Call Implementation Act, Pub. L. No. 108-10, § 3, 117 Stat. 557, 557 (2003).
[55] 16 C.F.R. §310.4 (FTC rule); 47 C.F.R. § 64.1200. Both agencies also maintain their own websites regarding the Do-Not-Call registry. The FTC has a website at http://www.ftc.gov/donotcall/, and the FCC has a website at http://www.fcc.gov/cgb/donotcall/. Registration is available at http://www.ftc.gov/donotcall/.
[56] Business-to-business calls are not covered by the Do-Not-Call registry. *Q&A: The National Do Not Call Registry*, National Do Not Call Registry, *at* https://www.donotcall.gov/FAQ/FAQConsumersNew.aspx (last visited Oct. 4, 2004).
[57] *Information for Consumers*, National Do Not Call Registry, *at* https://www.donotcall.gov/FAQ/FAQConsumers.aspx (last visited Sept. 29, 2004).
[58] Mainstream Mktg Servs., Inc. v. F.T.C., 358 F.3d 1228 (10th Cir. 2004).
[59] *Id.* at 1233.
[60] ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 1047 (2d ed. 2002).
[61] 447 U.S. 557 (1980).

interest.[62] The Tenth Circuit applied the *Central Hudson* test and provided four reasons why the Do-Not-Call registry is consistent with the First Amendment's requirements.[63] The court's reasoning readily applies to a potential Do-Not-E-Mail implementation.

¶12 First, the *Mainstream Marketing* court emphasized that only core commercial speech is restricted by the Do-Not-Call registry.[64] The law clearly defined the scope of content to include only commercial speech, and as such, it fell within the constitutional purview of the *Central Hudson* test. Similarly, the CAN-SPAM Act only targets commercial speech.[65] However, the FTC could make this analysis more difficult if it pushes the limit of its discretion concerning the implementation of a Do-Not-E-Mail registry.[66] For example, if the FTC expanded the registry to reach non-commercial political speech, the registry would not be protected by the *Mainstream Marketing* precedent.[67]

¶13 Second, the court acknowledged that the government had two justifiable interests, thus passing the second prong of the *Central Hudson* test. The Do-Not-Call registry was meant to protect individual privacy in the home and protect consumers against "fraudulent and abusive solicitation."[68] The court stated that the home is a "personal sanctuary that enjoys a unique status in our constitutional jurisprudence."[69] These interests would also apply to consumers using personal e-mail. However, while the Do-Not-Call registry only applies to personal phone numbers,[70] an effective Do-Not-E-Mail registry would also need to include business e-mail addresses. Many of the costs of spam are incurred by businesses through lost productivity and technology costs, and businesses generally invest more in costly anti-spam programs than individuals do.[71] Thus, under a potentially expanded Do-Not-E-Mail registry, a court would have to also determine whether decreasing the burden on businesses is a justifiable government interest.

---

[62] *Id.* at 566.
[63] *Mainstream Mktg. Servs.*, 358 F.3d at 1233, 1236.
[64] *Id*.
[65] CAN-SPAM Act § 4.
[66] *Id.* § 9(a).
[67] The Tenth Circuit explicitly stated that their opinion did not serve as precedent for political and charitable callers. *Mainstream Mktg. Servs.*, 358 F.3d at 1233 n.2.
[68] *Id.* at 1237.
[69] *Id.* at 1233 (citing Frisby v. Schultz, 487 U.S. 474, 484 (1988)).
[70] 47 C.F.R. § 64.1200(c)(2) (2003).
[71] Deborah Fallows, *Spam: How It Is Hurting Email and Degrading Life on the Internet*, PEW INTERNET & AMERICAN LIFE PROJECT, Oct. 22, 2003, at 19, *at* http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf (last visited Nov. 23, 2004).

¶14 Third, the *Mainstream Marketing* court addressed the issue of choice, as the Do-Not-Call registry acts as an opt-in program that leaves choice in the hands of the consumers.[72] It found that the Do-Not-Call registry materially furthers the government's interests of combating the danger of abusive telemarketing and preventing the invasion of consumer privacy, thus fulfilling the third prong of the *Central Hudson* test.[73] In this same manner, a Do-Not-E-Mail registry would put the power to receive or prevent spam in the hands of consumers. The CAN-SPAM Act states that it forwards a substantial government interest in that it protects consumers from the fraudulent aspect of spam and provides them the right to decline commercial e-mails.[74] Thus, a Do-Not-E-Mail registry would further the government interest of protecting consumers by putting the power in the hands of the consumer to determine whether or not to receive unsolicited commercial e-mails.

¶15 Fourth, the Do-Not-Call registry was challenged under the last factor of the *Central Hudson* test which requires that the commercial speech regulation be "narrowly tailored," but not necessarily the least restrictive means.[75] The Tenth Circuit found that the Do-Not-Call regulation is narrowly tailored because it is a proportional response to the government interest.[76] The appellees in *Mainstream Marketing*, who were telemarketing companies, contended that there were alternative approaches that could be taken to fulfill the government's interests; however, the court struck each of them down. For example, telemarketers suggested that consumers could make company-specific opt-out requests,[77] but the court found that only having a company-specific approach is "seriously inadequate to protect consumers' privacy from an abusive pattern of calls."[78] Telemarketers also argued that the government could employ less restrictive technological alternatives to stop unsolicited phone calls; however, the court recognized that such alternatives would not only place the cost of unwanted calls on

---

[72] *Mainstream Mktg. Servs.*, 358 F.3d at 1233, 1238.
[73] *Id.* at 1233, 1241-42.
[74] CAN-SPAM Act § (2)(b); *see also Mainstream Mktg. Servs.*, 358 F.3d at 1237 (finding that the government's justifications of protecting individuals' privacy and fraudulent and abusive solicitation are "undisputedly substantial governmental interests").
[75] *Id.* at 1237.
[76] *Id.* at 1238. The Tenth Circuit found that "do-not-call prohibits not only a significant *number* of commercial sales calls, but also a significant *percentage* of all calls" and that commercial sales calls are exactly the type that Congress is seeking to redress. *Id.* at 1242–42.
[77] *Id.* at 1244.
[78] *Id.*

recipients, but would also be ineffective as technological advances have been made to circumvent blocking techniques.[79]

¶16 In the same manner, spam advertisers may argue that there are ample alternatives to implementing a Do-Not-E-Mail registry; however, because spam and telemarketing have many of the same characteristics and alternatives, the *Mainstream Marketing* arguments may also apply to a Do-Not-E-Mail challenge.[80] Under the current CAN-SPAM Act scheme a consumer only has a company-specific opt-out option.[81] It is questionable how effective this option will be in stopping spammers, and it shifts the burden to the consumer to opt-out of each company's mailing list. This is in contrast to the Do-Not-Call registry, by which telemarketers are charged with removal of the phone numbers listed on the registry from their call lists; however, only personal phone numbers may be listed[82] and the list does not apply to non-telemarketers, such as political organizations, charities, telephone surveyors, or companies with which consumers have an existing relationship.[83]

¶17 An effective Do-Not-E-mail registry would not only be narrowly tailored, but welcomed by consumers because it would allow them to opt-out only once, similar to the Do-Not-Call registry.[84] As with telemarketing, there are many spam blocking technologies; however, they have proven to be both costly and ineffective.[85] The Tenth Circuit found a registry to be the most efficient for consumers, and unlike the current scheme of the CAN-SPAM Act, where an e-mail user can only opt-out from each individual solicitation, a registry provides one easy means to "erect a wall . . . that no advertiser may penetrate without [the registered party's] acquiescence."[86]

---

[79] *Id.* at 1245.
[80] *Id.* at 1244–46.
[81] CAN-SPAM Act § 5(a)(5)(ii).
[82] Business-to-business calls are not covered by the Do-Not-Call registry. *Q&A: The National Do Not Call Registry*, National Do Not Call Registry, *at* https://www.donotcall.gov/FAQ/FAQConsumersNew.aspx (last visited Oct. 4, 2004).
[83] *Information for Consumers*, National Do Not Call Registry, *at* https://www.donotcall.gov/FAQ/FAQConsumers.aspx (last visited Sept. 29, 2004).
[84] Whether or not this would be effective is also questionable, as suggested by the FTC report; however, this minimally puts a law-abiding company on notice and gives the enforcing agencies statutory means to protect the consumer.
[85] *See* Yang, *supra* note 23, at 30–35.
[86] *Mainstream Mktg. Servs.*, 358 F.3d at 1243 (quoting Rowan v. Post Office, 397 U.S. 728, 738 (1970)).

¶18 The Tenth Circuit correctly found that the Do-Not-Call registry was constitutional, and a constitutional challenge against a Do-Not-E-Mail registry would face many of the same issues. However, a successful Do-Not-E-Mail registry would inevitably need to be a more encompassing registry than a Do-Not-Call registry, given that a large amount of spam is sent to both consumers and businesses[87] and also because the general nature of e-mail is such that users can check their personal or business e-mail wherever they are. If only personal e-mails could be registered, the nuisance aspect of spam could still occur in the home because the nature of e-mail allows many users to frequently check their business e-mail from home and vice versa.

¶19 While the Direct Marketing Association ("DMA"), one of the appellees in *Mainstream Marketing*, decided not to appeal the Tenth Circuit's decision, the American Teleservices Association announced that it would appeal the case to the Supreme Court[88] and did so in May 2004.[89] However, the Supreme Court recently denied certiorari.[90] The Tenth Circuit's holding thus stands, and is not only instrumental in protecting consumers but also serves as significant precedent for the Do-Not-E-Mail registry.[91]

¶20 If created, a Do-Not-E-Mail registry would be more difficult to administer than a Do-Not-Call registry,[92] and it is possible that the FTC may be "emboldened enough to create a do-not-email registry broader than the

---

[87] REPORT TO CONGRESS, *supra* note 37, at 1.

[88] Caroline E. Mayor, *Telemarketers Split on Appeal of Do-Not-Call*, THE WASHINGTON POST, Mar. 4, 2004, *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A28821-2004Mar3&notFound=true (last visited Nov. 17, 2004).

[89] Mainstream Mktg. Servs., Inc. v. F.T.C., 358 F.3d 1228 (10th Cir. 2004), *petition for cert. filed*, (U.S. May 14, 2004) (No. 03-1552).

[90] Mainstream Mktg. Servs v. F.T.C.., 358 F.3d 1228 (10th Cir. 2004), *cert. denied*, 2004 WL 2050134 (2004).

[91] In fact, both the DMA and the American Association of Advertising Agencies oppose the creation of a Do-Not-E-mail registry. Declan McCullagh, *Court Upholds Do Not Call List*, NEWS.COM, Feb. 17, 2004, *at* http://news.com.com/2100-1028-5160690.html (last modified Feb. 17, 2004). Furthermore, some experts believe that a Do-Not-E-mail challenge would track a Do-Not-Call precedent. *Id.*

[92] REPORT TO CONGRESS, *supra* note 37, at 16. Some administrative problems are: security/privacy concerns, difficulty in enforcement because of spammers' abilities to hide their identities, difficulty in tracking spammers, difficulty obtaining subpoenas to obtain the information necessary to file cases against spammers, and the vast number of e-mail addresses. *Id.* at 15-26.

telephone registry [and] . . . go for noncommercial e-mail."[93] If the FTC created a registry outside the bounds of the Tenth Circuit's holding, such as one allowing the registration of business e-mails or the restriction of non-commercial e-mail, this could possibly incite marketing trade groups to make First Amendment challenges. However, the costs of spam and telemarketing are different and there are other significant justifications, such as the nuisance of pornographic spam,[94] which could justify farther reaching provisions of a Do-Not-E-Mail registry.

III. OTHER SOLUTIONS SUBJECT TO CHALLENGE

¶21 Given the time necessary to study the effects of the CAN-SPAM Act and the potential First Amendment challenges, Congress is not likely to amend the Act to give it any more force. Therefore, the FTC is left to either implement a registry or look to alternative non-statutory solutions, most of which are not susceptible to attack under the First Amendment. For example, an e-mail tax would severely hinder the cost-efficiency of spam, and though it would have to pass intermediate scrutiny,[95] such a measure would likely pass a First Amendment challenge because it would apply to all e-mail.[96] In addition, various Internet Service Providers (ISPs) have proposed technical solutions to verify the validity of an e-mail and its origin.[97]

---

[93] *Id.*

[94] Unlike annoying telemarketing, pornographic spam affects individual consumers; that may justify an argument for "privacy" equal to that of personal e-mail. A Pew Research study showed that pornographic spam causes the same embarrassment and emotional reaction that would be manifested in personal e-mail, and in some situations may cause employees to lose their jobs. *See* Fallows, *supra* note 71, at 29-31.

[95] CHEMERINSKY, *supra* note 60, at 903

[96] *Id.* at 903 (stating that "A law regulating speech is content-neutral if it applies to all speech regardless of the message . . . . For example, a sales tax, applicable to all purchase including of reading material, might have a significant incidental effect on speech, but it is content-neutral."). Similarly, a tax on all e-mail would be similar to requiring a stamp on all postal mail. A person would have to affix the stamp on regardless of the mail's content. Also, due to the prevalence of e-mail in all businesses with very little differential taxation on the press, it would be unlikely that a tax would be construed as an unconstitutional special taxation. *See id.* at 1123.

[97] *E-mail Identity System Proposed to Combat Spam*, ASSOCIATED PRESS, Feb. 27, 2004, *available at* http://www.cnn.com/2004/TECH/internet/02/27/email.origins.ap/index.html (last visited Nov. 17, 2004).

¶22 Many of the suggested technical solutions require some type of key, authentication, or identification process.[98] In fact, in its June 2004 report, the FTC suggested that it will convene a Federal Advisory Committee to consider an authentication process[99] in lieu of a Do-Not-E-Mail registry.[100] Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC), cautions that while digital certificates requiring identification of a sender are allowable for commercial speech, they would most likely violate First Amendment protections of political or religious speech.[101] However, while the Supreme Court has held that laws that ban anonymity on political literature are unconstitutional, there would be a question if this requirement of anonymity could be applied to technological standards implemented by private ISPs, particularly when the implementations are completely content-neutral.[102] Most likely, unless ISPs are regarded as state actors,[103] those who send unsolicited e-mails would be unable to make First Amendment challenges against ISPs,[104] as the First Amendment only protects against speech regulated by the government.[105] Thus, if private ISPs and other technology companies take the initiative on their own to create an e-mail standard, they would be able to defend against First Amendment challenges.

---

[98] *See* REPORT TO CONGRESS, *supra* note 37, at 35-37.
[99] *Id.* at 36.
[100] *Id.* at 34-35. Technological solutions, such as authentication, have received much support from technology companies, such as AOL. *CAN-SPAM Act*: *Full Committee Hearing*, 108th Cong. (2004) (statement of Ted Leonsis, Vice Chairman, America Online, Inc.), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1199&wit_id=3436 (last visited Nov. 17, 2004).
[101] Marc Rotenberg, Executive Director, Electronic Privacy Information Center, *Testimony and Statement of Record Before the Committee on Commerce, Science and Transportation*, May 21, 2003, *available at* http://www.epic.org/privacy/junk_mail/spam/spamtestimony5.21.03.html (last visited Nov. 17, 2004).
[102] *See* Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Talley v. California, 362 U.S. 60 (1960).
[103] CHEMERINSKY, *supra* note 60, at 1103 ("There is not a right to use private property owned by others for speech. Because it is private property, the Constitution does not apply.").
[104] The Supreme Court has concluded that the First Amendment does not create a right to use privately owned shopping centers for speech. Hudgens v. Nat'l Labor Relations Bd., 424 US 507, 520-21 (1976). If ISPs were to be regarded as an entity similar to a shopping center, where the general public has access to the traffic of the privately owned ISPs, then ISPs would not be required to offer network access to spammers.
[105] CHEMERINSKY, *supra* note 60, at 894.

¶23 However, it is problematic to implement these technical solutions.[106] Furthermore, getting the major e-mail providers to agree on a single protocol will be extremely difficult.[107] The FTC, anticipating these hurdles, is considering mandating an authentication protocol.[108] A government-imposed technological standard may not be advisable, but it is beyond the scope of this paper to discuss those issues. Authentication may even work best with a registry, rather than in lieu of a registry.[109] Currently, spammers can exploit the e-mail system because the identity of the e-mailer is unverifiable.[110] In the same way, a major problem with the Do-Not-E-Mail registry is the fear that spammers may illegally use the registry e-mails to continue spamming while avoiding detection because of their inability to be traced.[111] If the FTC implements a Do-Not-E-Mail registry with an authentication system in place, this may very well be more effective than only implementing a registry.

CONCLUSION

¶24 Although many spam scholars are calling for the expansion of the current CAN-SPAM legislation, there is still time to determine whether the current legislation will make an impact on spam. The Spamhaus Project's Register of Known Spam Operations has found that 90% of all spam comes from 200 spam groups.[112] Some on the list, such as Bernard "Merlin" Balan, who Canada.com News dubbed the "King of Spam," have since retired.[113] However, the CAN-SPAM Act provides a Damoclean sword for those spammers who wish to take Balan's place among the spamming elite, and has caused many to be wary of sending spam.[114]

---

[106] Yang, *supra* note 23, at 30-34.
[107] *See* Jim Hu, *AOL Drops Microsoft Antispam Technology*, NEWS.COM, Sept. 16, 2004, *at* http://news.com.com/AOL+drops+Microsoft+antispam+technology/2100-1032_3-5369915.html?tag=nefd.top (last visited Nov. 17, 2004). AOL has already backed out of Microsoft Sender ID, while Yahoo supports Domain Keys. *Id.*
[108] REPORT TO CONGRESS, *supra* note 37, at 36.
[109] *Id.* at 37 (finding that the FTC would consider a registry if "an authentication system is in place, and if other technological developments removed the security and privacy risks associated with a Registry.").
[110] *Id.* at 12.
[111] Simon, *supra* note 49, at 106.
[112] *Register of Known Spam Operations*, THE SPAMHAUS PROJECT, *at* http://www.spamhaus.org/rokso/index.lasso (last visited Mar. 27, 2004).
[113] Gary Dimmock, *The King of Spam*, THE OTTAWA CITIZEN, Mar. 11, 2004 (on file with author).
[114] Saul Hansell, *Unrepentant Spammer to Carry on, Within the Law*, N.Y. TIMES, *at* http://www.nytimes.com/2003/12/30/technology/30spam.html (last

¶25 Hopefully, an authentication implementation will be able to stem the increasing flow of spam. However, if the amount of spam does not decrease, the statutory requirements of the CAN-SPAM Act will need to be expanded and further expansion will undoubtedly test the limits of free speech. Since the Supreme Court denied certiorari, the Tenth Circuit's decision stands as a significant precedent. An emboldened FTC may consider creating an expansive Do-Not-E-Mail registry alongside an effective authentication system, which together would add to the growing arsenal in the war on spam. In fact, this may be necessary to appease the various anti-spam organizations and corporations that are tired of fighting an ever-increasing amount of spam.

---

visited Nov. 17, 2004). Alan Ramsky, one of the top 200 ROKSO spammers, expressed his concern about the CAN-SPAM Act and stated, "You would have to be stupid to try to violate [the CAN-SPAM Act]." *Id*.