The John Marshall Journal of Information Technology & Privacy Law

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

Article 11

Fall 2003

Wireless Spam This Way Comes: An Analysis of the Spread of Wireless Spam and the Present and Proposed Measures Taken to Stop It, 22 J. Marshall J. Computer & Info. L. 229 (2003)

Bridget O'Neill

COMMENT

WIRELESS SPAM THIS WAY COMES: AN ANALYSIS OF THE SPREAD OF WIRELESS SPAM AND THE PRESENT AND PROPOSED MEASURES TAKEN TO STOP IT

I. INTRODUCTION

Advancements in telecommunications have improved peoples' ability to communicate quickly and easily. Electronic mail ("e-mail"), mobile phones, personal digital assistants ("PDAs"), and pagers can facilitate instantaneous communication between individuals. As most individuals with an e-mail address have experienced, these devices can also facilitate unwanted communication from spammers, people or companies that send out unsolicited, unwanted e-mail.[1] While many individuals with an e-mail address have learned to deal with e-mail spam as a daily part of life, now wireless spam, once only a major problem in Japan, is making its presence known in the United States. Even though some individuals may have built up a tolerance for dealing with copious amounts of unwanted e-mail, and filtering technology has improved such that it prevents the delivery of most spam, wireless spam introduces an entirely different level of intrusiveness. Wireless spam is making its way here, and methods should be put into place now to prevent its proliferation.

The background of this paper discusses where wireless spam first had a major impact, the effects it has had in various countries during its travel westward, and the attempted solutions that have been put into place along the way, including legislation, self-regulation, and technological measures. The background also briefly introduces the proposed legislative solutions to wireless spam in the United States. The analysis

1. Throughout this paper, the writer defines "spam" as unsolicited, unwanted marketing via electronic messages, whether in the form of mobile text messages or e-mail. The writer also defines spam in such a way that it is different from the use of the term "mobile marketing." Mobile marketing is a tool that can be used to benefit both the consumer as well as the marketer and exists where there is already a relationship between the marketer and the consumer.

further explores each of the current proposed legislative solutions to wireless spam in the United States, including the recently passed *CAN-SPAM Act*, explains how each proposal could be modified to apply to wireless spam, makes the case for the best legislative alternative, and ultimately comes to the conclusion that the most effective approach to the minimization of spam is an integrated one.

II. BACKGROUND

A. THE EVOLUTION OF WIRELESS SPAM

1. *How Do Spammers Get the Numbers?*

An important basic question to answer is how spammers receive access to mobile phone numbers. One method is to simply spam blocks of numbers.[2] Another method is harvesting phone numbers from Web sites. For example, spammers can harvest numbers from Web sites that allow individuals to download customized ring tones for their mobile phones[3] or from Web sites that act as virtual "white pages," containing telephone numbers including mobile phone numbers.[4] A third way that spammers acquire mobile phone numbers is through methods where an individual will submit his or her phone number to be in the running to win a prize in a contest.[5] And yet another method includes automatic dialing systems, which dial thousands of numbers on a random basis.[6]

Spammers also use a variety of tricks to get individuals to call them. For instance, a person might get a message that reads "I've always liked U. It's time to come clean."[7] Another trick is called "wangiri-style" (or

---

2. Patrick Ross, CNetNews.com, *Taking Aim at Wireless Spam*, ¶ 9 <http://news.com.com/2100-1033-254799.html> (Mar. 27, 2001).

3. Will Sturgeon, CNet, *Spam War Settles into Mobile Phones*, ¶ 8 <http://news.com.com/2100-1041-1015595.html> (June 11, 2003).

4. Sue Lowe, *Now Phone Firms Spam Your SMS):*, Sydney Morn. Herald ¶¶ 1-4 (April 3, 3002) (available at <http://www.smh.com.au/articles/2003/04/02/1048962814945.html>).

5. IT AsiaOne, *Specials, Be Careful Who You Give Your Number to*, ¶¶ 6-7 <http://it.asia1.com.sg/specials/ spotlights20030611_002.html> (June 11, 2003). In Singapore, they have what are called "lucky draws," wherein an individual submits his or her phone number to receive a prize. *Id.*

6. The Japan Times Online, *Before Telecom Abuse Goes Too Far: Laws Urged to Curb Mobile Phone Scams, Spam*, ¶ 5 <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20021226b6.htm> (Dec. 26, 2002). This form of spamming paralyzed a wireless network in Japan. *Id.* at ¶ 9. Eventually, the telecommunications company NTT West turned off services to the companies engaging in these activities. *Id.* Additionally, the police issued them warnings. *Id.* at ¶ 14.

7. BBC News, *Science/Nature, Mobile Spam on the Rise*, ¶ 9 <http://news.bbc.co.uk/1/hi/sci/tech/2116070.stm> (July 8, 2002).

"one-ring" calls),[8] where the spammer rings a mobile phone just once, leaving the spammer's number on the screen. In both tricks, the person receiving the message will call back out of curiosity. But when the person calls back, the number goes into a tape recorded phone sex message or dating service advertisement.[9] Later, the person receives a large bill for the call.[10]

2. *Wireless Spam's Movement Westward: The Concerns and Costs Along the Way*

By most reports, Japan has the longest running problem with wireless spam. Several facts emerging from November 2001 demonstrate the extent of this problem. That month, Japan's wireless carrier NTT DoCoMo invested one billion yen (US $8.22 million) in systems to block unwanted e-mail.[11] Also during that month, DoCoMo obtained an injunction against a dating service that, in one hour, sent out 900,000 unsolicited messages to users of their I-mode wireless service.[12] Additionally, of the 950 million e-mails sent out in November 2001, about 800 million were returned because of invalid addresses.[13] Thus, wireless spam has had a major impact in Japan.[14]

Moving westward to Korea, where seventy percent of the population uses mobile phones, the country has great concerns about the problems potentially caused by wireless spam. The concerns are so great that last December Korea's Ministry of Information and Communication delayed

---

8. DoCoMo Information, *Advisory Concerning Malicious (One-Ring) Phone Calls* <http://www.nttdocomo.co.jp/english/info/akushitsu/index.html> (Dec. 4, 2001). DoCoMo recommends that its customers not call back a number they do not recognize. The company has a system in place whereby customers who are victims of the one-ring callers can block any future calls from the registered landline number. *Id.*

9. *Id.*

10. Japan Times Online, *supra* n. 6, at ¶ 5.

11. Jay Wrolstad, Wireless NewsFactor, *Japanese Giant Mounts New Wireless Spam Offensive,* ¶ 3 <http://www.wirelessnewsfactor.com/perl/story/14612.html> (Nov. 6, 2001).

12. The Japan Times Online, *Court Issues Injunction on DoCoMo Spammer* (Oct. 31, 2001) (available at <http://www.japantimes.co.jp/cgibin/getarticle.pl5?nn20011031a4.htm>).

13. Wrolstad, *supra* n. 11, at ¶ 3. A July 2002 estimation stated that out of the 950 million e-mails sent out daily, about eighty-four percent are sent out randomly. Evan Cramer, *The Future of Wireless Spam*, 2002 Duke L. & Tech. Rev. 21, ¶ 2 (Oct. 2002) (available at <http://www.law.duke.edu/journals/ dltr/articles/2002dltr0021.html>).

14. Also, a recent estimation (by Mobile Marketing Association's Executive Director Peter Fuller) found forty to fifty percent of all text messages sent in Japan are sent by marketers. Emily Motsay, RCR Wireless News, *Trash or Treasure?; Industry Takes on Wireless Spam,* ¶ 7 (July 7, 2003).

the opening of wireless networks until July 2003.[15] Further, the Korean government plans to spend seventeen billion won (US $13 million) by 2007 researching and developing ways to limit the growth of wireless spam.[16]

Wireless spam is also a problem in Europe, so much so that the European Union passed a law in 2002 addressing it.[17] It is difficult to find the exact cost or even an estimate of the cost of wireless spam in Europe; currently most available financial figures are supplied in terms of traditional e-mail spam and do not factor out the cost of wireless spam. However the yearly cost of spam to European business is estimated at $2.5 billion dollars, the result of a approximately ten billion spam messages sent out every day.

The United States has not seen the same proliferation of wireless spam as other countries, but wireless spam is beginning to make its presence known. Recently, the Federal Trade Commission held a forum on spam, which included a session that addressed the issue of wireless spam.[18] According to panelists at the forum, and others in the telecommunications industry already dealing with the wireless spam, there appears to be no doubt that wireless spam will soon become a major problem in the United States.[19]

B. The Problems of Wireless Spam

Wireless spam can be more invasive than e-mail spam, mainly due to the kind of devices that wireless spam targets by definition. First, with mobile devices, there is a more limited amount of storage available for messages compared to that available for e-mail storage.[20] Therefore, spammers can quickly fill up what storage is available, preventing legitimate messages from being delivered to an individual. Second, it takes more time to go through and remove unwanted messages from a mobile device than it does to go through and delete unwanted messages in e-mail. A major reason for this is due to the fact that often one cannot tell who the sender of a text message is and therefore has to go through the lengthy process of opening each message before deleting it.[21] Addition-

15. Kim Deok-hyun, Hankooki.com, Korea Times, *Technology, Spam Mail Frustrates Mobile Users, Delays Opening of Wireless Network*, ¶¶ 1-3 <http://times.hankooki.com/lpage/tech/200306/ kt2003061218044611790.htm> (June 12, 2003).

16. *Id.* at ¶ 10.

17. Cramer, *supra* n. 13, at ¶ 5.

18. Grant Gross, PCWorld, *Watch Out for Wireless* Spam, ¶¶ 1-2 <http://www.pcworld.com/news/article/0,aid,110553,00.asp> (May 1, 2003).

19. *Id.* at ¶¶ 1-2, 16-17.

20. Sturgeon, *supra* n. 3, at ¶ 3.

21. Michelle Megna, *You've Got Spam Sell Phone Madness Pounded By Marketers And Junk Mail, Mobile Users Pay The Price*, Daily News (N.Y.) § Now, 42, ¶ 11 (July 10, 2003).

ally, wireless spam can render a wireless device useless. For individuals that use mobile phones, PDAs, and pagers for business purposes, when their mobile devices continually signal they have a message and it turns out to be spam, the mobile device "stops being a critical warning," and the user will turn off the device and check messages at a later time.[22] Finally, wireless spam feels like a greater invasion of privacy. Whereas e-mail spam occurs within the confines of an individual's e-mail program and thus an individual is only exposed to it when he or she logs into the e-mail program, wireless spam travels with the individual and is virtually inescapable.[23]

But as with any debate, there are those arguing the other side of the coin: wireless spam will not be the same problem that traditional e-mail spam has proven to be. Supporters of this idea point to the greatest limitation of wireless spam: the cost.[24] But, when one looks at the major problems Japan has had with wireless spam, wireless spam's continuing movement and momentum westward, and the fact that there are sixty million phones in the United States capable of receiving text messages,[25] and also takes into consideration the more invasive, debilitating nature of wireless spam, to refuse to take steps to combat the growth of spam on the theory that it is more costly would be a gross mistake in ignorance of reality. This is why it is important to look at the solutions various countries have taken or proposed in order to inhibit the growth of wireless spam.

C. Suggested Solutions to Wireless Spam

1. *Self-Regulation*

The marketing industries in various countries affected by wireless spam have taken measures to curb spam. Such measures are important to the marketing industry because spam damages the reputation of legitimate marketers. Therefore, it is in marketers' best interests to establish marketing principles and adhere to them. Many of these principles, though produced in different countries, are quite similar.

---

22. Grant Gross, Network World Fusion, *Wireless Spam: Some Fighting it Successfully*, ¶ 6 <http://www.nwfusion.com/news/2003/0509wirelspam.html> (May 9, 2003).

23. Neil McCartney, *Getting the Message Across: Mobile Advertising*, Fin. Times § FT REPORT- FT-IT, 3, ¶ 8 (Jan. 15, 2003); *see also* Sturgeon, *supra* n. 3, at ¶ 5.

24. Mike Grenville, chief executive of 160 Characters, a mobile messaging company, stated that while it is not expensive to send a million e-mails across the Atlantic, sending a million text messages across the Atlantic would be expensive, thus suggesting that the greater cost of wireless spam inhibits it from reaching the same level of growth as traditional e-mail spam. Sturgeon, *supra* n. 3, at ¶ 6.

25. Michael Thuresson, *Phone Spam Emerges as Costly Annoyance*, 25 L.A. Bus. J. No. 21, 1, ¶ 9 (May 26, 2003). The estimation comes from the Mobile Marketing Association, based out of Mountain View, California. *Id.*

The Direct Marketing Association of Singapore ("DMAS") has been working on a code of practice to which it recommends its members adhere.[26] One of the main principles recommended by the DMAS is that its members be "upfront and not pushy."[27] Also, members should utilize an opt-in system that asks the consumer if he or she would like to receive marketing materials before sending them.[28] According to the DMAS, "opt-out" is the minimum acceptable standard, where the consumer has a viable way of discontinuing the reception of unwanted marketing materials.[29] And in the cases where there is e-mail sign-up, double opt-in is a requirement, where the DMAS member confirms with the consumer that he or she has signed up to receive the marketing materials.[30]

In the United Kingdom, the Independent Committee for the Supervision of Standards of Telephone Information Services ("ICSTIS"), a non-profit making, industry-funded regulatory body, investigates complaints and has the power to fine telecommunication companies.[31] The ICSTIS regulates marketing through its Code of Practice, which promotes principles of legality, decency, honesty and integrity.[32] Applicable to efforts to curb spam, the Code specifies that one cannot engage in marketing that would be an "unreasonable invasion of privacy."[33] It also requires that marketing cannot be misleading.[34] Additionally, any promotion must clearly provide the identity and contact details of the sender,[35] and service providers must make every effort to ensure that promotional material is not inappropriate.[36]

In the United States a couple of organizations, the Wireless Advertising Association ("WAA")[37] and the Network Advertising Initiative ("NAI")[38] have developed anti-spam principles and recommendations for self-regulation in the marketing industry. WAA's Guidelines on Privacy

26. IT AsiaOne, *Do You Have Permission. . .*, Computer Times <http://it.asia1.com.sg/specials/ spotlights20030611_004.html> ¶ 3, 10 (accessed June 11, 2003).

27. *Id.* at ¶ 16.

28. *Id.*

29. *Id.*

30. *Id.*

31. *See generally* ICSTIS, *Home* <http://www.icstis.org.uk/icstis2002/default.asp> (accessed July 23, 2003).

32. *Id.* ICSTIS, *ICSTIS The Code of Practice* <http://www.icstis.org.uk/icstis2002/pdf/9TH_CODE_FINAL_AMENDED_DEC_2002.PDF> (accessed Aug. 4, 2003) [hereinafter *ICSTIS Code of Practice*].

33. *Id.* at 3.2.2a.

34. *Id.* at 3.3.1a.

35. *Id.* at 3.5.

36. *Id.* at 3.9.

37. Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services*, 10 CommLaw Conspectus 133, 154 (2001).

38. Allison S. Brantley et al., *The Legal Web of Wireless Transactions*, 29 Rutgers Computer & Tech. L.J. 53, 62 (2003).

and SPAM are voluntary.[39] The guidelines include: (1) customers should approve or give confirmed opt-in to members before the members send wireless push advertising; (2) members should not transfer subscriber data to third parties without authorization; and (3) members should not forge the identity of message originators, send chain letters, make "fake" voice calls, or mislead subscribers about content.[40] The NAI has introduced the Self-Regulatory Principles for Online Marketing for Network Advertisers.[41] These principles, similar to those of the WAA, were endorsed in 2000 by both the Federal Trade Commission and the Department of Commerce, and protect three kinds of user data: (1) information that is non-personally identifiable, (2) information gleaned from the combination of a "Web user's name, e-mail address, or other personal information with information about her Internet usage across web-sites;" and (3) statistics produced from taking personally identifiable information offline and combining it with information collected online.[42]

2. *Legislation*

Just as marketing principles in various parts of the world have similarities, the laws promulgated and proposed in different countries to combat spam have similarities. The Japanese Parliament and the European Parliament have both passed laws regarding wireless spam, and the United States has several proposed bills in Congress focused on combating traditional e-mail spam. All of these are discussed in turn.

a) Japan

In April 2002, the Japanese Parliament enacted two anti-spam bills regulating wireless commercial solicitations, which came into effect July 1, 2002.[43] The first law is the *Law for Appropriate Transmission of Specified Emails* (Law No. 26 of 2002).[44] The main requirements specify that the receiver of unsolicited mail must be informed of who the sender is, the sender's contact information, and the fact that the e-mail is an unsolicited advertisement.[45] All of this information must be in the subject line so that the receiver knows the information before downloading the e-mail.[46] Additionally, the law prevents the sending of e-mails to randomly generated addresses.[47] As a deterrent, the law imposes a fine for

39. *Id.*
40. Traupman, *supra* n. 37, at 154.
41. Brantley et al., *supra* n. 38, at 63.
42. *Id.*
43. Cramer, *supra* n. 13, at ¶ 3.
44. *Id.* at ¶ 4.
45. *Id.*
46. *Id.*
47. *Id.*

non-compliance.[48] The second law, passed one day after the previous law, is an amendment updating the *1976 Specific Commercial Transactions Law* (Law No. 28 of 2002).[49] The attributes of this law include the following: (1) it only applies to products and services, (2) it is narrowly tailored, (3) it provides cellular users with the ability to opt-out, and (4) it gives individuals the ability to report spam they have received to the Public Management Ministry, who in turn will send out cease and desist letters to the spammers.[50] Violations of this law are much more severe than Law No. 26 as it imposes a maximum two year prison term or fines up to three million yen (U.S. $ 24,000) for violations.[51]

b) European Union

In 2002, the European Union's Parliament May approved the *Directive for the Protection of Personal Data and Privacy in the E-communications Sector*.[52] The Directive, which applies to unsolicited commercial e-mail, faxes, and automated calling systems, takes an opt-in approach to spam.[53] It also addresses the issue of location-based technology and requires the consent of mobile phone users before marketers can utilize location information to provide area and interest specific advertisements.[54] EU member states are expected to finish the implementation of the Directive in 2003.[55]

c) United States

The only federal legislation introduced specifically to combat wireless spam is H.R. 113 the *Wireless Telephone Spam Protection Act*, which was introduced in 2001 by Representative Holt (D-N.J).[56] The legislation makes it illegal to transmit unsolicited commercial messages via wireless telephone text, graphic, and image messaging systems.[57] While this is the only legislation currently targeted solely at unsolicited wireless advertisements, there are several other proposed laws aimed at traditional notions of wireline spam. These laws could be modified in order to accommodate the growing concern of wireless spam, as discussed in much greater detail below.

48. *Id.* The fine imposed for non-compliance is 500,000 yen (U.S. $4,180). *Id.*
49. Cramer, *supra* n. 13, at ¶ 4.
50. *Id.*
51. *Id.*
52. *Id.* at ¶ 5.
53. *Id.* Members of the European Parliament debated the issue for a year before agreeing on the opt-in approach. *Id.*
54. *Id.*
55. *Id.*
56. Motsay, *supra* n. 14, at ¶ 22.
57. H.R. 113 (2001). The legislation was reintroduced in 2003 as H.R. 122.

3. *Anti-Spam Technology*

On an individual level, the proliferation of spam has spawned anti-spam technology, which puts some power into the hands of the individual to deal with those who will neither abide by self-regulation principles nor comply with the law. Wireless carriers state that they have implemented measures that will protect their customers from wireless spam.[58] The carriers utilize filters that can block out mass amounts of messages coming from one source, and also offer their customers the ability to personalize their filters based on keywords, which will block out messages that contain certain words, for example, Viagra.[59] The unavoidable weakness in anti-spam technology, however, is that the technology does not always work the way it is intended to work,[60] and spammers are constantly able to adjust to the technology and find a way in, despite the use of filters.[61]

III. ANALYSIS

A. MODIFY CURRENT LEGISLATION

1. *Current Legislation*

a) H.R. 122, Wireless Telephone Spam Protection Act

As stated earlier, the only legislation to specifically address the issue of wireless spam is the *Wireless Telephone Spam Protection Act*, originally introduced in 2001, and reintroduced in January 2003.[62] The proposed law, which is brief and prohibits unsolicited commercial messages on wireless telephone text, graphic, and image messaging systems, would allow individuals to sue spammers for $500 per unsolicited message.[63] If a judge permits, an individual may receive up to $1,500

58. Thuresson, *supra* n. 25, at ¶ 15.

59. *Id.* at ¶ 15–16. T-mobile and Verizon are two companies implementing the filtering technology. *Id.*

60. *Am. Lib. Assn. v. United States*, 201 F. Supp. 2d 401 (E.D. Pa. 2003) (striking down the *Children's Internet Protection Act*, Pub. L. No. 106-554, as unconstitutionally abridging freedom of speech). Internet filters, meant to block out certain Web sites containing obscenity and pornography, often fail to work as intended: they overblock thousands of Web sites that should not be blocked, and they underblock, allowing in Web sites that should be blocked. *Id.* Although the Supreme Court, in *United States v. Am. Lib. Assn.* subsequently overturned the final holding of the District Court, the Supreme Court did not overturn the District Court's specific findings of fact with regard to the weaknesses in filtering technology. *See generally id.*

61. Thuresson, *supra* n. 25, at ¶ 17.

62. In 2001, the bill was introduced as H.R. 113. In 2003, the bill was introduced as H.R. 122.

63. *Live From the Headlines 19:00,* "Congress is considering legislation to allow cell phone users to sue text message spammers" ¶ 3 (CNN June 16, 2003) (tv broadcast, transcript # 061603CN.V94 available in LEXIS, News & Business).

per unsolicited message.[64] While this law is simple and straightforward, and as Congressman Holt states, "would put the power in the hands of the cell phone owner,"[65] a more efficient alternative would be to incorporate the prohibition on wireless spam into legislation that prohibits traditional e-mail spam.[66] Until recently, there were four bills introduced in Congress that could envelop the ban on wireless spam. In December 2003, one of those bills passed both Houses of Congress and was signed into law by the President: the *CAN-SPAM Act of 2003.*

b) S. 877, CAN-SPAM Act of 2003

The first bill introduced to Congress with the purpose of banning e-mail spam was the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, or the *"CAN-SPAM Act of 2003".*[67] The bill addresses "unsolicited commercial electronic mail messages," recognizing that while such messages can attract customers, they also can have great costs to the consumers who do not wish to receive them.[68] The proposed law finds that individuals should not be misled by advertisements and should have the right to decline future advertisements.[69] Some of the requirements set forth in the bill include: (1) senders of commercial electronic mail must not intentionally provide false or misleading header information;[70] (2) senders of commercial electronic mail must not mislead recipients as to the content of the message;[71] and (3) recipients must be able to opt-out, thus senders must supply information so that recipients are able to opt-out of receiving any further unsolicited commercial e-mail.[72] While these requirements are similar to the self-regulation principles set forth by the WAA and the NAI, the major difference is that the Act provides damages for violations of the Act. The statutory damages vary depending on who seeks enforcement of the Act.[73]

64. *Id.*

65. *Id.* at ¶ 19.

66. Traupman, *supra* n. 37, at 154. A potential weakness of this bill is the argument that it would face First Amendment challenges, as companies fight to communicate with customers. *Id.* Ms. Traumpan argues in her article that H.R. 113 "does nothing that competent self-regulation and enforcement cannot also do." *Id.*

67. 108 S. 877 (2003). The bill was introduced April 2003 by Mr. Burns and is sponsored by Mr. Burns, Mr. Wyden, Mr. Stevens, Mr. Breaux, Mr. Thomas, Ms. Landrieu, and Mr. Schumer. It is a bill "[t]o regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet." *Id.* The CAN SPAM Act can be found at <http://www.spamlaws.com/federal/108s877.html> (accessed Dec. 28, 2003).

68. *Id.* at § 2(a) Congressional Findings.

69. *Id.*

70. *Id.* at § 4.

71. *Id.* at § 5(a)(2).

72. *Id.* at § 5(a)(3).

73. *Id.* at § 7.

Where States and Internet Service Providers (ISPs) seek enforcement, the *CAN-SPAM Act* permits penalties for violations of the Act to reach $2,000,000.[74]

The final version of the *CAN-SPAM Act* addresses the issue of wireless spam.[75] In its previous version, the CAN-SPAN Act would not have applied to wireless spam: there was no mention of wireless spam in the original version, and the definitions of electronic mail address and electronic mail message could not be reasonably stretched to apply to wireless spam.[76] Now, however, the Act requires the Federal Communication Commission ("FCC") and the Federal Trade Commission ("FTC") to promulgate rules to protect consumers from "unwanted mobile service commercial messages."[77] Additionally, the *CAN-SPAM Act* requires the FTC to report to Congress a report on implementation of a Do Not E-Mail Registry, for which consumers can sign up if they do not wish to receive spam.[78]

Although the *CAN-SPAM Act* is now the law, the previously proposed legislative solutions to spam deserve review. A review of those proposals demonstrates the variety of congressional foci in the war on spam, as well as whether these proposals could have addressed the issue of wireless spam.

c) H. R. 1933, REDUCE SPAM Act of 2003

Not long after the *CAN-SPAM* was introduced in the Senate, the *Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or SPAM Act of 2003*, or *"REDUCE SPAM Act"*, was introduced in the House of Representatives.[79] The bill's twin purposes were protecting children from sexually oriented advertisements and reducing spam. In order to affect its purposes, the *REDUCE SPAM Act* prohibited and required similar actions as found in the *CAN-SPAM Act*, including a prohibition against fraudulent header information[80] and valid return addresses.[81] It also included a labeling requirement.[82] The FTC would

74. *Id.* at § 7(f)(3) and § 7(g).

75. *Id.* at § 14.

76. *Id.* at § 3(5). "Electronic mail address" is defined as a "destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as the 'domain part'), to which an electronic mail message can be sent or delivered." *Id.* Also, "electronic mail message" is a "message sent to an electronic mail address." *Id.* at § 3(6).

77. *Id.* at § 14.

78. *Id.* at § 9.

79. Introduced May 1, 2003 by Ms. Lofgren, sponsored by Ms. Lofgren, Mrs. Tauscher, Mr. Defazio, Mr. Frank, and Ms. Harman.

80. H.R. 1933 at § 3.

81. *Id.* at § 4(b).

have had the power of enforcement,[83] and individuals and Internet access providers were permitted to bring civil actions in the event of violations of the *REDUCE SPAM Act*.[84]

Definitions play a crucial role in determining whether the *REDUCE SPAM Act* could have applied to wireless spam. Unlike the *CAN-SPAM Act*, this bill did not define electronic mail message. It did, however, define "commercial electronic mail message," the crux of which was that the message's primary purpose must be the "commercial advertisement or promotion of a commercial product or service."[85] If the message merely made reference to a commercial entity or link to an Internet Web site operated for a commercial purpose, that would not be enough to qualify it as a "commercial electronic mail message."[86] An e-mail message was also not commercial if the sender has a personal relationship established with the recipient.[87] Because there was no specific definition of electronic mail message, it is possible that the Act could have applied to wireless messages.

d) H. R. 2214, RID SPAM Act

Approximately three weeks after legislators introduced the *REDUCE SPAM Act*, legislators in the House of Representatives introduced another new anti-spam bill, the *Reduction in Distribution of SPAM Act of 2003*, or the *"RID SPAM Act"*.[88] The bill was introduced with the single purpose of preventing unsolicited commercial e-mail and was the most detailed of all the anti-spam bills. The bill required that any commercial

82. The subject line of commercial e-mail messages must contain identification that the message is an advertisement. *Id.* at § 4(a)(1). With regard to this specification, the subject line must contain either (A) an identification that the message complies with standards adopted by the Internet Engineering Task Force for identification of unsolicited commercial e-mail messages, or (B) contain the letters "ADV" as the first four characters. *Id.* Also, commercial e-mail messages that have adult content must be identified as such. *Id.* at § 4(a)(2). Similar to § 4(1), the adult identification in the subject line must comply with standards adopted by the Internet Engineering Task Force, or contain "ADV:ADLT" as the first eight characters. *Id.*

83. *Id.* at § 5.

84. *Id.* at § 6. The individuals or Internet Access providers would have been able to request an injunction and damages either in the amount of actual monetary loss or statutory damages in the amount of ten dollars per violation. *Id.* at § 7(b).

85. *Id.* at § 2(1).

86. *Id.*

87. *Id.* Also of note, this is the only anti-spam legislation that defines, let alone mentions, "opt-in". § 2(9)(B). It is defined as "the recipient has given the sender permission to initiate commercial electronic mail messages to the electronic mail address of the recipient and has not subsequently revoked such permission." *Id.*

88. This bill was introduced on May 22, 2002 by Mr. Burr and sponsored by Mr. Burr, Mr. Sensenbrenner, Mr. Tauzin, Mr. Goodlatte, Mr. Upton, Ms. Hart, Mr. Stearns, and Mr. Cannon.

electronic message sent out must contain clear and conspicuous identification that the message is an advertisement or solicitation, and there must also be clear and conspicuous notice of how to opt-out, and that mechanism must be functioning properly.[89] As with other bills, any transmission of commercial e-mail with fraudulent header information was prohibited.[90] It also prevented sending commercial e-mail to addresses obtained through automated means.[91]

Initially, this bill had more teeth to it than the other bills, for it provided a private right of action to ISPs.[92] An ISP could have recovered up to $500,000, or have the damages tripled in the case of intentional violations,[93] an amount now lower than the *CAN-SPAM Act*'s $2,000,000 statutory damages cap for ISPs.[94] States, on behalf of their residents, could have brought a cause of action with even higher statutory damages allowed than the ISPs; the States would have been capped at $3,000,000 in cases of intentional violations,[95] one million dollars greater than the statutory damages allowed pursuant to the *CAN-SPAM Act*.

e) S. 1231, The SPAM Act

The bill most recently introduced to Congress was the *Stop Pornography and Abusive Marketing Act* or *SPAM Act*. [96] The main purpose of the *SPAM Act*, and the one major characteristic that set it apart from the other anti-spam legislation, was the establishment of the National No-Spam Registry.[97] Any person that did not wish to receive unsolicited commercial e-mail was permitted to register.[98] The Act then prohibited individuals from sending unsolicited commercial e-mail to anyone on the registry.[99] Pursuant to the *SPAM Act* the FTC could have imposed a civil penalty no greater than $5,000 for each violation of sending unsolicited commercial e-mail to an individual on the registry.[100] The Act also established a penalty of up to $100,000 for unauthorized use of the regis-

89. *Id.* at § 101(a)(1).

90. *Id.* at § 101(c).

91. *Id.* at § 101(d).

92. *Id.* at § 102(a). ISPs could obtain an injunction or monetary damages. *Id.* at § 102(b). The statutory damages provided in the Act are $10 for each separate e-mail address that a message is sent to in violation of the Act over the ISP's line. *Id.* at § 102(c).

93. *Id.* at § 102(c)(1)(C).

94. S. 877 at § 7(g).

95. H.R. 2214 at § 103.

96. Introduced by Mr. Schumer on June 11, 2003.

97. *Id.* at § 101. The original CAN-SPAM Act did not contain a Do Not E-Mail Registry.

98. *Id.* The FTC would be responsible for maintaining the registry. *Id.*

99. *Id.* at § 101(d).

100. *Id.* at § 102. Each day of violation constitutes a separate offense. *Id.*

try, a penalty not included in the current *CAN-SPAM Act*.[101] Just as found in the *REDUCE SPAM Act*, the *SPAM Act* contained the labeling requirement for all commercial e-mail.[102] The bill was similar to the *CAN-SPAM Act* in its prohibition of misleading information in the return address, and in taking an opt-out approach to spam.[103]

The *SPAM Act*'s definition of "electronic mail address" is identical to the definition found in the *REDUCE SPAM Act*,[104] and thus could have been applicable to wireless spam. The *SPAM Act* also included the broader definition of "commercial electronic message" as seen in the *CAN-SPAM Act*, where a message, in order to be considered commercial, must have as its primary purpose the advertisement or promotion of a commercial product or service.[105] Unique to the *SPAM Act* was its specific exemption from the definition of unsolicited commercial message any e-mail sent for the purpose of notifying an individual that he or she is violating someone else's protected intellectual property rights.[106]

1. *The Anti-Spam Law*

Prior to the passage of the *CAN-SPAM Act*, Congress had all of what it needed to create what will be referred to going forward as "the Anti-Spam Law", an ideal law that would apply to wireless spam as well as the traditional notion of e-mail spam. Although the *CAN-SPAM Act* provides for the prohibition of both wireless spam and traditional e-mail spam, Congress could have made the *CAN-SPAM Act* better by "cutting and pasting" more of the best elements of each bill, tweaking a few parts here and there, and adding one crucial dimension to fulfill its role in the fight against spam. Following are ideas as to what elements of all the bills to include, what elements to exclude, and what elements should be added to a more Anti-Spam Law.

---

101. *Id.* Additionally, the bill requires that there are certain categories to which recipients who are minors can receive protection from, including products or services that a minor child is prohibited by law from purchasing, and e-mail that advertising or contains adult content, or has links to such content. *Id.* at § 103.

102. *Id.* at § 201(a). The labeling requirement would not apply to a self-regulatory organization approved by the FTC if the organization meets the specified requirements of § 201(b). Another specific difference from the REDUCE SPAM Act is that the SPAM Act states nothing about the Internet Engineering Task Force; the only labeling requirement is to place "ADV:" as the first characters the subject line. *Id.*

103. *Id.* at § 204. The bill also specified statutory damages in the amount of ten dollars per violation. *Id.* at § 303.

104. *Id.* at § 4(5).

105. *Id.* at § 4(2).

106. *Id.* at § 4(18)(B). The drafters of the Anti-SPAM Act may have included this exemption for situations analogous to the record industry's attempt to prosecute individuals who engage in music file sharing. *See* Elec. Frontier Found., *File Sharers, See if the Recording Industry is After You* <http://www.eff.org/IP/P2P/20030725_eff_pr.php> (accessed July 25, 2003).

a) Elements to Include

Before the passage of the *CAN-SPAM Act*, the strongest and most comprehensive bill was the *RID SPAM Act*. Congress should have started with this bill as a foundation for the Anti-Spam Law. The *RID SPAM Act* provided the stiffest penalties and allowed the federal government, state governments, and ISPs to bring causes of action against those who violated the Act. The *RID SPAM Act* also has the same basic provisions of the other three proposed laws: (1) the prohibition of fraudulent or misleading headers and subject lines, (2) the requirement of the sender to provide accurate and working contact information to the receiver, (3) specified damages for each individual violation (despite the difference in the maximum penalties), and (4) prohibiting the acquisition of e-mail address through harvesting or sending unsolicited electronic message via automated systems.[107] Furthermore, the *RID SPAM Act* included a labeling requirement for all e-mails that were advertisements; this is important to include as it would create uniformity among current anti-spam laws in the individual states. Unique to the *RID SPAM Act* was the prohibition on class action suits.[108] This prohibition should have been maintained in the Anti-Spam Law because it is practical; it would be difficult procedurally to engage in an anti-spam class action lawsuit, and the *RID SPAM Act* provided ample avenues to prosecute those who would break the law.

The *REDUCE SPAM Act* provided the best definition of commercial electronic mail message. The definition, in addition to stating that the "primary purpose" of the commercial electronic message had to be the promotion of a commercial product or service, also made important exceptions to clarify what would not be considered a commercial electronic mail message. For First Amendment purposes, the more specific the definition for understanding what is prohibited, the better. Further, the exceptions put forth in the *REDUCE SPAM Act* for what did not constitute a commercial e-mail message were reasonable and logical, excluding messages that merely reference a commercial entity for identification purposes, or that merely reference or include a link to a commercial Internet site operated for a commercial purpose. The ideal Anti-Spam Law would have started with the *RID* SPAM as a foundation, but would have utilized the definition of commercial electronic mail message as found in the *REDUCE SPAM Act*.

107. The REDUCE SPAM Act was the only bill which does not prohibit harvesting or using automated systems for sending out e-mails.

108. 108 H.R. 2214 § 104.

b) Elements to Exclude

While it would be great to cure all the ills of spam in one perfect Anti-Spam Law, the reality is that including too many requirements could be too burdensome to achieve the main desired result: eliminate spam. For example, the *REDUCE SPAM Act* includes a requirement for commercial e-mails with adult content to be labeled as such. This requirement is somewhat ambiguous, as those trying to comply with the law might claim uncertainty as to what is considered "adult". Rather than deal with potential First Amendment problems, it would be better to exclude this requirement altogether from the Anti-Spam Law.

The Anti-Spam Law also would not include the National No-Spam Registry, as is included in the *CAN-SPAM Act*. Although modeled after the currently popular Do Not Call Registry,[109] a No-Spam Registry would be much more difficult to maintain than the Do Not Call Registry. This is so because, while individuals can presumably change their phone numbers with some speed through their telecommunications carrier, phone numbers remain relatively constant, and numerous e-mail addresses can be created in an instant. This would make maintaining and continually updating a No-Spam registry much more difficult. Also, once spamming becomes illegal, a No-Spam Registry is superfluous.

c) Elements to Tweak and Add

Under the category of an element to "tweak" is the opt-out requirement as used in the proposed legislation. The opt-out requirement gives a marketer or spammer the ability to send an initial e-mail to individuals who then must turn around and notify the marketer that they do wish to receive any more advertisements. Although the opt-out approach might be better for marketers in the United States,[110] the opt-in approach takes the onus off of the consumer. Further supporting this is the fact that the Internet is a global community, and the opt-in approach is

109. *See* Federal Trade Commission, *National Do Not Call Registry* <http://www.ftc.gov/donotcall/> (accessed Aug. 7, 2003).

110. Erin Joyce, Internetnews.com, *DMA's E-mail Guidelines: Better Late than Never* <http://www.internetnews.com/IAR/article.php/12_968671> (accessed Feb. 5, 2002). Additionally, one recent new report stated that the European Parliament is concerned that the United States will take an opt-out approach to spam. Jennifer L. Schenker, *EU Rolls Out Anti-Spam Strategy*, Intl. Herald Trib. ¶ 8 (July 15, 2003) (available at <http://www.iht.com/articles/102770.html>). The concern expressed is that if the United States takes an opt-out approach, and China patterns their practice after the United States on this issue, then Europe will not be able to go after spammers. *Id.* at ¶ 9. A coalition of British Parliament members reportedly are planning a trip to the United States for fall 2003 to address this issue and their concerns regarding the United States adopting an opt-out instead of an opt-in approach to spam. *Id.* at ¶ 14.

the current approach utilized in Japan and in Europe.[111] Without a universal approach to combating spam, efforts to combat it globally will be frustrated. The United States should adopt an opt-in approach to spam.

Last but not least, the Anti-Spam Law should incorporate H.R. 122 in its entirety in order to clearly prohibit wireless spam, an effect not accomplished in the *CAN-SPAM Act*. H.R. 122 is a good model because not only does it define and prohibit wireless spam, it specifically applies to wireless telephones, PDA's, and pagers – the current popular devices most effected by a proliferation of wireless spam.[112] The *CAN-SPAM Act* is weak as it applies to wireless spam for it simply defines commercial wireless spam, and then throws the responsibility for handling issues related to wireless spam on to the shoulders of FTC and the FCC. It does not state anywhere in the Act that wireless spam is prohibited. It supplies no clear direction as to how to handle wireless spam, but nonetheless requires the two commissions to promulgate rules regarding wireless spam. Thus, Congress neither effectively prohibited wireless spam, nor did it provide a sufficient deterrent to wireless spam. This is a gaping hole in the *CAN-SPAM Act* that easily could have been and should have been filled.

IV. CONCLUSION

The law is only one method by which to combat wireless spam, and even with strong laws in place, people still will ignore and break the law. This is especially true when technology grows at such a speed that tracking down individuals responsible for breaking the law can be considerably difficult, and quite possibly not worth the cost. Therefore, the best way to truly diminish the proliferation of spam is to continue to utilize all the methods discussed, beginning with legislation that sets the standard for self-regulation and is consistent on a global level.

In addition to the legislation, it is important for private industry to continue its efforts at self-regulation. By setting its own standards and requirements, private industry can place more pressure on marketers to act in a responsible, respectable, and honest manner. This will give the industry the additional benefit of gaining the trust of consumers who will then be more likely to initiate or continue to do business with companies that follow industry self-regulation principles. Furthermore, private industry has greater resources than the government to investigate what

111. *Id.* at ¶¶ 3, 22.

112. Under H.R. 122, a "'covered messaging system' means a messaging system capable of providing text, graphic, or image messages (including a short message service and systems using the wireless application protocol)" that—"(A) is provided as part of a commercial mobile service. . .and (B) provides access to the text, graphic, or image messages on the same handset used to access voice messages." *Id.* at § 3(b)(2).

approach is most agreeable to the public and thus likely to be the most financially beneficial to the industry.

Finally, legislation and self-regulation will do nothing to stop individuals who do not care about breaking laws or their reputation. For those individuals, it is important that wireless carriers continue to create effective filters and provide customizable filters to their customers. While such filters are currently available, technology is always changing, and when faced with filtering, spammers can find another way in. Therefore, even though legislation and self-regulation may become stronger, the filtering technology also needs to improve and become stronger. Utilizing all three of these methods is the most effective way to eliminate spam.

It is important to reiterate that despite the fact that wireless spam is not a major problem in the United States yet, the federal government should be proactive and take measures now to prevent problems with wireless spam later, and it was proper for Congress to include the prohibition on wireless spam in the *CAN-SPAM Act of 2003*. Although marketers have a right to advertise, individuals have a right to be left alone.[113]

Bridget M. O'Neill†

113. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 193 Harv. L. Rev. (1890).

† January 2004 graduate of The John Marshall Law School, J.D., with an LL.M. in Information Technology & Privacy Law, *cum laude*; B.A. in English, University of Illinois, Urbana-Champaign. The author also extends a special thanks to Professor Leslie Reis, J.D., LL.M., for her constant advice and help for the last three years.