CONGRESS OPTS OUT OF CANNING SPAM

Matthew E. Shames[*]

I. INTRODUCTION

And in the beginning, there was e-mail! At least, that may be the perception of the millions of people who use electronic mail ("e-mail") every day.[1] In fact, the pervasiveness of the Internet in general, and the World Wide Web and e-mail in particular, has made it difficult for many people to remember the world before these technologies changed the face of communications forever. But it was only a decade ago that e-mail was a novelty outside of academic and scientific settings, the Web was not yet viable as a commercial mechanism, and the promise and exuberance surrounding the developing technologies masked the dangers of the road that would lie ahead.[2]

The emergence of the World Wide Web as a commercial tool in the mid-1990's signaled a change in the landscape.[3] No longer was the Internet the sole haven of academia, where open standards and exchange of information were of paramount importance.[4] As the business world jumped on the Web bandwagon, e-mail became a vital means of communication. Entrepreneurs soon recognized that while a web site provided a means for an actively interested audience to gain information, e-mail provided a means to access a relatively passive audience.[5] The best part about e-mail solicitation was the cost. For a fraction of the cost of sending traditional advertisements through

---

* The author would like to thank Professor Bernard Hibbitts for helpful comments on an early draft of this paper, and Professor Teresa Brostoff for all of her assistance and support throughout law school. Special thanks to Jennifer, Ma and Pa for their love and patience.

1. 15 U.S.C.A. § 7701(a)(1) (West Supp. 2004).

2. As a personal aside, I began working at a graphic design company in Austin, Texas, in July 1994. This particular company was moving into the very new area of designing commercial websites to augment the print design work provided to clients. At the time, many of our clients did not even have e-mail addresses, and none yet had websites. In 1995, we helped launch the initial sites for both Whole Foods Markets and the City of Austin.

3. *See* Philip Elmer-Dewitt, *Battle for the Soul of the Internet*, TIME, July 25, 1994, at 50.

4. *Id.*

5. Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation To Control Junk E-mail*, 4 VA. J.L. & TECH. 4, ¶ 6 (1999), *at* http://www.vjolt.net/vol4/issue/home_art4.html.

the U.S. Postal Service, businesses could reach exponentially more potential customers.[6]

Over the next several years, the use of e-mail as a means of commercial solicitation mushroomed,[7] but not without consequences. While commercial e-mail has proven invaluable in providing needed information (both on a business to business level, and a business to consumer level), both businesses and consumers soon began to complain about the volume and nature of unsolicited e-mail that they were receiving.[8] By 2003, experts estimated that over half of the e-mails transmitted on any given day represented unsolicited commercial messages,[9] commonly referred to as "spam."[10] Not only has spam put a strain on existing technological infrastructures, but it has become a massive time sink for businesses and consumers alike, who must cope with the increased volume of mail.[11] Largely based on this background, in December 2003, Congress passed the CAN-SPAM Act of 2003.[12] The Act looked to control the growth of unsolicited commercial e-mail in an effort to preserve the usefulness of e-mail as a communications device.[13]

This Comment will examine the rise of unsolicited commercial e-mail, the associated problems, and the attempts to control these problems via state legislative initiatives. The difficulties of state-by-state enforcement will be briefly discussed, demonstrating the need for federal legislation. Next, this Comment will turn to the CAN-SPAM Act of 2003, highlighting the most important provisions. In particular, this Comment will examine the opt-out provisions of the Act, along with the proposed "Do Not E-mail" registry, and will suggest that Congress failed to adequately address their own findings in crafting solutions that would not directly address the problems raised. Lastly, this Comment will offer suggestions for future legislation to further protect business and consumer interests, and maintain the viability of e-mail as a means of communication in a modern society.

---

6. *See id.*

7. *See* Scot M. Graydon, *Much Ado About Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 81-83 (2000).

8. *Id.* at 82-84.

9. 15 U.S.C.A. § 7701(a)(2) (West Supp. 2004).

10. Elmer-Dewitt, *supra* note 3, at 51. The term "spam" is meant to evoke the image of "dropping a can of Spam into a fan and filling the surrounding space with meat." *Id.*

11. 15 U.S.C.A. § 7701(a) (West Supp. 2004).

12. CAN-SPAM Act of 2003, 108 Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 (2004)).

13. 15 U.S.C.A. § 7701(a) (West Supp. 2004).

II. A BRIEF HISTORY OF SPAM[14]

The roots of the Internet, and specifically e-mail, lay in the belief that communications should be open and easy. Because of this, the structural systems that developed to support e-mail were relatively devoid of security devices. Although it may sound quaint today, the need for security was of relative unimportance to academicians and scientists, who saw the ability to easily share information as most significant.[15] Subsequently, the system that developed was more concerned with open access than possible abuses.

A brief primer on how e-mail works is useful in understanding the problem of unsolicited commercial e-mail. Certain computers, known as mail servers, have software installed that allows them to receive and send electronic messages.[16] These mail servers may be analogized to electronic post offices. Mail servers also store e-mail for users who have authorized accounts on that particular server.[17] In this sense, the mail server from which people retrieve their e-mail is like their local post office. When a person sends a message to someone else, the message contains certain header information that identifies the destination mail server.[18] Generally, the message first goes to the sender's mail server (their "local" post office), and is then forwarded to the recipient's mail server, where the recipient can download the message.[19]

It is important to recognize that for various reasons, a message may not go directly from the sender's mail server to the recipient's mail server.[20] The system is designed to distribute loads among many servers.[21] For example, if

---

14. While the use of the term "spam" is meant to evoke an image of something less than desirable, it should not be confused with the famous canned meat produced by Hormel. In fact, Hormel initially pursued copyright infringement claims in an attempt to prevent the use of the term to describe unsolicited commercial electronic mail. Eventually, Hormel decided not to pursue such claims, under conditions that may still be viewed at their web site. *See* Joanna Glasner, *A Brief History of SPAM, and Spam*, WIRED NEWS, *at* http://www.wired.com/news/business/0,1367,44111,00.html (last visited Oct. 18, 2004); Hormel Foods Corporation, *Spam and the Internet*, *at* http://www.spam.com/ci/ci_in.htm (last visited Oct. 18, 2004).

15. *See* Charles Arthur, *Science and Technology: The Key to Spam Free-Inboxes; Efforts To Cut Junk E-Mail Aren't Working*, THE INDEPENDENT (LONDON), Mar. 3, 2004, at 10 ("The problem is that it was invented by scientists on a network who all trusted each other."); Elmer-DeWitt, *supra* note 3, at 52 (discussing the evolution of the internet).

16. Marshall Brain, *How Email Works*, *at* http://computer.howstuffworks.com/email.htm (last visited Oct. 18, 2004).

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

the recipient's mail server is not available, the message may be sent to a secondary mail server, which may hold the message until it is able to be delivered.[22] This secondary mail server is said to "relay" the electronic message to the destination mail server.[23] By distributing loads in this manner, the system allows e-mail to be routed around problem points, allowing for more reliable delivery.[24] In the early 1990's, most mail servers were open relays, in the sense that anyone could send e-mail to be relayed through any server. Security concerns eventually led to the closing of many of these open relays, often restricting relaying to specific authorized users. Even today, senders of unsolicited commercial e-mail often attempt to relay messages through multiple mail servers in an attempt to disguise the origin point of the message.[25]

It was into this relatively open and decentralized system that commercial enterprises began to enter in the early to mid-1990's. Ironically, one of the earliest controversies over unsolicited commercial e-mail involved a small law firm in Arizona.[26] In April of 1995, the husband and wife team that ran the firm sent out a message to approximately 5,500 electronic bulletin boards to solicit new business.[27] They utilized a program they had developed that would send the message to several destinations simultaneously, thus avoiding the time constraints of sending out one message at a time.[28] Although the incident provoked an overwhelming negative response from experienced Internet "citizens," the couple claimed that the advertisement resulted in over $100,000 in new business.[29]

Since those "early days," the use of unsolicited e-mail to gain customers has exploded. At first, administrators of mail servers attempted to combat the onslaught through technological means.[30] What resulted was a back and forth between the "spammers," as the senders of such messages came to be known, and the server administrators.[31] For every measure that was instituted to protect recipients from unwanted messages, the spammers would develop

---

22. *Id.*
23. *Id.*
24. *Id.*
25. *See* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 380-81 (2001) (discussing open relays in general).
26. Elmer-Dewitt, *supra* note 3, at 51.
27. *Id.*
28. *Id.*
29. *Id.*
30. Amaditz, *supra* note 5, at ¶ 15; Sorkin *supra* note 25, at 344-50.
31. Amaditz, *supra* note 5, at ¶ 15; Sorkin *supra* note 25, at 344-50.

either a new way to work around, or a new means to exploit the system.[32] Although technical responses to the rise of spam continue to this day, increasingly businesses and consumers have turned to legislatures to control the electronic communications landscape.[33]

Several states responded by passing laws that levied varying levels of restrictions on the practice of unsolicited commercial e-mail.[34] While some of these laws were, and are, quite strict, they suffer from three major problems. First, many states have trouble establishing jurisdiction over senders that reside elsewhere, either in other states, or even in other countries.[35] Because of the distributed nature of the e-mail system, it is virtually impossible to determine the location of a recipient simply from their e-mail address.[36] Plaintiffs and prosecutors therefore face difficulties establishing jurisdiction over spammers simply on the basis of sending messages to recipients within the state borders.[37] Spammers can often avoid state court by either operating in a state that does not have strong anti-spam laws, or outside of the United States entirely.[38]

The second major problem with the state legislative approach is a lack of uniformity. This results from different states enacting different types of legislation.[39] Spammers make a convincing argument that it is unrealistic to force them to adhere to the laws of the most restrictive state because at the time of sending, they really have no way to know where the messages would end up.[40]

---

32. Amaditz, *supra* note 5, at ¶ 15; Sorkin *supra* note 25, at 344-50.

33. Many experts believe that any successful attempts to curb unsolicited commercial e-mail will need to be based on technological advances rather than legislation. The most promising suggestions include rebuilding the basic structure of e-mail from the ground up to be more secure. This would be no easy undertaking, would take years to accomplish, and would require e-mail administrators from around the world to change behaviors. *See* Arthur, *supra* note 15 (mentioning various technical options for changing the structure of e-mail systems). Several members of Congress have expressed the view that legislation will only be effective in conjunction with new technical solutions. *See*, *e.g.*, 149 CONG. REC. S13029 (daily ed. Oct. 22, 2003) (statement of Sen. Hatch).

34. In particular, Virginia and California have passed very strong anti-spam statutes. The California statute, for example, forbids all unsolicited commercial electronic mail unless a person has previously indicated a willingness to receive messages from that particular sender. Bill Husted et al., *Spam Wars: Can Deluge Be Stopped*, ATLANTA JOURNAL-CONST., Dec. 16, 2003, at 1F.

35. *See* Sorkin, *supra* note 25, at 380-81 (discussing jurisdictional problems that arise in state regulation of unsolicited e-mail).

36. *Id.*

37. *Id. See also AOL Spam Lawsuit Dismissed, Firm Says*, L.A. TIMES, Dec. 31, 2003, at C3.

38. Sorkin, *supra* note 25, at 380-81.

39. *Id.* at 381-82.

40. *Id.*

The third major issue with reliance on state legislation is that state-by-state prosecution makes it more difficult to combat the oftentimes fraudulent practices of spammers. The senders of unsolicited commercial e-mail often disguise their identities by relaying messages through several mail servers, manipulating the header information of the message, and including false or misleading subject information with the message.[41] The lack of standards and resources across states makes it easier for fraudulent spammers to evade detection and prosecution.[42]

Because of these shortcomings, by the late 1990s advocacy groups began to push for legislation on a federal level. Federal legislation would clearly address the first two problems with a state-by-state approach. No matter where the senders were located in the United States, the courts would be able to establish jurisdiction.[43] Additionally, even spammers located outside the country would likely be subject to the courts, as it would be much easier to establish that they "purposefully availed" themselves to recipients in the United States in general as opposed to specific locations within the borders. With uniform laws, spammers would be on fair warning of what is allowed and what is prohibited. Lastly, although fraud would still be an issue, the resources of the federal government would allow for a more comprehensive approach to combating unsolicited commercial e-mail.

III. THE CAN-SPAM ACT OF 2003

Responding to the need for federal legislation, Congress passed the CAN-SPAM Act of 2003 in December 2003.[44] For the first time, Congress outlined a federal policy that addressed unsolicited commercial e-mail.[45] The Act also recognized the major problems of such e-mail, and offered a means to regulate it through criminal and civil penalties.[46]

---

41. *Id.* at 339-40.

42. *See id.* at 381-82 (discussing the consequences of a lack of uniformity in state laws).

43. *See* 15 U.S.C.A. § 7706(f)(7) (West Supp. 2004).

44. CAN-SPAM Act of 2003, 108 Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 (2004)).

45. 15 U.S.C.A. § 7701 (West Supp. 2004).

46. *Id.* §§ 7707-7713.

A. Findings of Fact

The Congressional findings provide a framework from which to analyze the Act. Congress acknowledged that e-mail has become an essential element of communication, both on a personal and commercial level.[47] Additionally, e-mail has become a powerful force in the development of commerce.[48] Congress estimated that as of 2003, unsolicited commercial e-mail accounted for over fifty percent of all e-mail traffic.[49] This represented a seven percent increase from 2001, and the volume continues to grow.[50]

Congress also outlined the various problems that unsolicited commercial e-mail now poses.[51] At the most individual level, the amount of e-mail costs recipients in terms of the time needed to review, delete, or otherwise deal with these unwanted messages.[52] Additionally, the increased volume forces recipients to incur costs for increased storage of e-mail.[53] The massive amount of "junk" mail also increases the risk that necessary messages will be overlooked or lost in the shuffle, thereby reducing the reliability of e-mail.[54]

In addition, Internet Service Providers ("ISPs") also suffer significant cost increases because of the proliferation of unsolicited commercial e-mail.[55] Providers of Internet service, whether or not of a commercial nature, must invest in networking infrastructure to handle the increased traffic.[56] As the amount of e-mail increases, so do the costs for all organizations involved in providing Internet service.[57]

Congress also recognized that most unsolicited commercial e-mail is "fraudulent or deceptive in one or more respects."[58] Purveyors of such e-mail oftentimes disguise the header information in messages by utilizing such tactics as changing the "From:" address that usually identifies the sender of a message.[59] Additionally, the subject lines of messages are often falsified to

---

47. *Id.* § 7701(a)(1).
48. *Id.*
49. *Id.* § 7701(a)(2).
50. *Id.*
51. *Id.* §§ 7701(a)(3)-(6).
52. *Id.* § 7701(a)(3).
53. *Id.*
54. *Id.* § 7701(a)(4).
55. *Id.* § 7701(a)(6).
56. *Id.*
57. *Id.*
58. *Id.* § 7701(a)(2).
59. *Id.* § 7701(a)(7).

induce the recipient into viewing the message.[60] Most important, in terms of analysis of the Act, Congress explicitly recognized that many senders of unsolicited commercial e-mail do not provide a means for recipients to request exclusion from future messages, and that even those who seem to provide such an opt-out mechanism refuse to honor such requests.[61] What Congress did not acknowledge is that many of these senders may utilize an opt-out feature to verify addresses as opposed to identifying addresses that should be removed.[62] Because many recipients have become aware of this behavior, ISPs have consistently cautioned recipients to not reply to these opt-out requests.[63]

Congress also made a strong statement of public policy. First, it unequivocally stated that there is a substantial government interest in federal regulation of commercial e-mail.[64] Secondly, Congress stated that senders of commercial e-mail should not be deceptive or fraudulent in the design or delivery of messages.[65] Lastly, Congress declared that recipients have a right to opt-out of receiving additional commercial messages from a source that has already delivered such a message to them.[66]

B. Prohibitions and Protections

The Act contains two main prohibitions. The first of these prohibits knowingly transmitting or relaying commercial e-mail messages through a "protected computer" with the intent to deceive or mislead recipients.[67] The Act defines a protected computer as any computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[68] This definition would include any computer that acts as an e-mail server. The prohibition addresses

---

60. *Id.* § 7701(a)(8).

61. *Id.* § 7701(a)(9).

62. See Mike Himowitz, *Congress Needs To Put Teeth in Laws To Can E-mail Spam*, BALT. SUN, July 10, 2003, at 1D; Husted et al., *supra* note 34; Cindy Richards, *Lawmakers Are Hearing Us*, CHI. SUN-TIMES, Jan. 7, 2004, at 35; Christine Winter, *Few Expect National Anti-Spam Law To Have Much Effect*, FORT LAUDERDALE SUN-SENTINEL, Dec. 10, 2003, at 1A.

63. *See* Husted et al., *supra* note 34; Dwight Silverman, *New Law Takes Effect, but It Seems To Can Little Spam*, HOUSTON CHRON., Jan. 3, 2004, at Business 1.

64. 15 U.S.C.A. § 7701(b)(1) (West Supp. 2004).

65. *Id.* § 7701(b)(2).

66. *Id.* § 7701(b)(3).

67. 18 U.S.C. §§ 1037(a)(1)-(2) (2004).

68. 15 U.S.C.A. § 7702(13) (West Supp. 2004). The Act adopts the definition from 18 U.S.C. § 1030(e)(2)(B) (2003).

the common practice of relaying messages through multiple computers to disguise information about the sender.[69] This practice can make it more difficult to track the origin of the message.[70]

The second major prohibition makes it illegal to materially falsify the header information contained in e-mail messages.[71] Again, this prohibition addresses the practice of falsely stating such information as the message sender or subject.[72] Unscrupulous commercial e-mailers may do this in an attempt to both deceive the recipient about the nature of the message, and to make it more difficult to ascertain the identity of the sender.[73]

In addition to these general prohibitions, the Act contains several other provisions meant to protect recipients. Most important, the Act requires that all commercial e-mail messages contain a valid "opt-out" mechanism by which recipients can request not to receive future electronic messages from that particular sender.[74] Additionally, the Act specifies that senders must honor any opt-out requests, and sets up required timetables for complying with such requests.[75] Lastly, any sender who has received such a request is prohibited from sharing the e-mail address of the recipient with any other commercial entity.[76]

C. The "Do Not E-mail" Registry

One of the more interesting proposals in the Act is the creation of a "Do Not E-mail" registry.[77] Such a registry appears to be based on the recent "Do Not Call" registries that have become a popular means to combat unsolicited phone calls from telemarketers.[78] The "Do Not Call" initiatives have been re-written to survive First Amendment attacks.[79] While any similar initiatives regarding e-mail will likely face constitutional challenges as well, there is

---

69. 149 CONG. REC. S13012, S13024 (daily ed. Oct. 22, 2003) (statement of Sen. Wyden).
70. *Id.*
71. 18 U.S.C. § 1037(a)(3).
72. *Id.*
73. 149 CONG. REC. S13029 (daily ed. Oct. 22, 2003) (statement of Sen. Hatch).
74. 15 U.S.C. §§ 7704(a)(3)-(5) (West Supp. 2004).
75. *Id.*
76. *Id.*
77. *Id.* § 7708.
78. *Id. See also* S. REP. NO. 108-102, at 14 (2003).
79. *See* Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228, 1250-51 (10th Cir. 2004).

little reason to believe that well-crafted regulations would not survive First Amendment scrutiny.[80]

The Act instructed the Federal Trade Commission (FTC) to submit a report to the Senate by June 16, 2004.[81] The report was to set a timetable and plan for implementing a nationwide "Do Not E-mail" registry.[82] The report was to include analysis of all concerns regarding the technical, practical, security, and enforceability aspects of the registry.[83] The FTC submitted the report to Congress on June 15, 2004, and concluded that the proposed registry would not decrease the amount of spam, but might actually increase the volume of unwanted e-mail.[84] The FTC concluded that a national "Do-Not-E-mail" registry was neither feasible nor advisable at the present time.[85]

IV. BENEFITS OF THE ACT

The symbolic aspects of the Act should not be overlooked. For the first time, the problem of unsolicited commercial e-mail has been recognized as a national problem.[86] Whatever the strengths and shortcomings of the Act might be, this Act marks an acknowledgment of the federal interest at stake, sets forth a broad policy statement with regard to the importance of e-mail to the economy of the country, and suggests a belief that people should not be forced to receive unsolicited e-mail of a commercial nature.[87] This treading into new waters is one that the federal government is not likely to retreat from any time soon. By making a strong statement of public policy, reinforced by detailed findings of fact, Congress has finally staked out a federal position on this issue.[88]

Another major benefit of the Act is the establishment of a federal basis of jurisdiction.[89] Any spammers in the United States, and many outside of its

---

80. *See* Credence E. Fogo, *The Postman Always Rings 4000 Times: New Approaches To Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 930 (2000) (postulating that a narrowly crafted anti-spam statute would survive constitutional challenges).

81. 15 U.S.C.A. § 7708 (West Supp. 2004).

82. *Id.*

83. *Id.*

84. 2004 FTC NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS 32, *at* http://www.ftc.gov/opa/2004/06/canspam2.htm (June 2004).

85. *Id.* at 37.

86. 15 U.S.C.A. § 7701 (West Supp. 2004).

87. *Id.*

88. *Id.*

89. *Id.* § 7706.

borders, will be subject to the terms of the Act. This will address one of the main shortcomings of state-by-state adjudication.

The Act also provides relatively clear guidelines for businesses that engage in legitimate use of commercial e-mail.[90] Assuming that commercial e-mail will play an important role in the development of robust economic systems, such guidelines are essential to reduce enforcement costs, both by encouraging voluntary compliance and making it easier to identify illegitimate spammers. While the effectiveness of the guidelines as currently constructed may be questioned, this first attempt at marking clear rules should be applauded.

Lastly, the "Do Not E-mail" registry is an intriguing idea, which may have long-term implications in the fight against spam. While it remains to be seen how such a system will be implemented, and to be sure, there are several technical and conceptual stumbling points,[91] the commissioning of what amounts to a feasibility report along with the granting of authority to the FTC for implementation should, at the very least, further educate government officials about the workings of the technology and has the potential to be a proverbial "good thing."

V. SHORTCOMINGS OF THE ACT

Unfortunately, because of several shortcomings, the Act as passed may not have a large immediate effect on unsolicited commercial e-mail, and, in some cases, may even increase the volume. The most glaring weakness is the reliance on an opt-out mechanism in place of a more prohibitive opt-in requirement.[92] Additionally, it is not clear how the Act will deal with fraudulent spammers, including those who attempt to conceal the origin or subject matter of unsolicited messages.[93] Thirdly, the Act preempts most state laws that regulate unsolicited commercial e-mail.[94] Many of these state laws provide stronger restrictions and punishments than the Act. Lastly, while the "Do Not E-mail" registry is an interesting idea, there are potentially huge technical hurdles to overcome in implementing such a system, and it is not

90. *Id.* § 7704(a).

91. *See infra* Part V.D.

92. *See* Himowitz, *supra* note 62; Husted et al., *supra* note 34.

93. *See generally* 15 U.S.C. § 7704. While the Act clearly prohibits fraudulent electronic mail practices, it is not clear what additional enforcement mechanisms, if any, will come into existence.

94. *Id.* § 7707(b).

clear that the fundamental differences between telephone solicitation and e-mail solicitation have been taken into account.[95]

A. The Act Allows Unsolicited Commercial E-mail Until a Recipient Opts Out of Messages from a Particular Sender

Congress's most egregious error in drafting the Act is the dependence on an opt-out mechanism for recipients to notify senders that they wish to be removed from future mailings.[96] While such a mechanism is surely useful and necessary, it allows companies to send messages up until the point when a user declines to receive them.[97] It requires an active effort on the part of the recipient to initiate action.[98] A stricter option would have been to require senders to affirmatively gain permission from recipients before sending commercial solicitations.

1. Advantages of Opt-In Methodology

There are several advantages to requiring recipients to opt-in to receiving messages. The first of these is the ease of enforcement and identification of violating messages. By only allowing solicitations to those people who have affirmatively stated that they wish to receive messages, both individuals and regulatory authorities will be able to determine more easily whether a message is in violation of the Act. Senders of messages will not be able to claim a negative defense, something such as "we never received a request to opt-out," because they would be required to retain affirmative proof of a recipient's desire to receive messages. Because it is much easier to disprove a positive than a negative, enforcement would be aided by an opt-in requirement.

More important, perhaps, an opt-in requirement would stand closer to the findings and purposes enumerated by Congress. The sheer volume of unsolicited commercial e-mail places stress on the infrastructure of the Internet, and shifts costs away from advertisers and towards service providers and recipients.[99] By requiring commercial mailers to gain permission before soliciting, the volume of spam, at least legitimate spam, would immediately

---

95. *Id.* § 7708.
96. *See* Himowitz, *supra* note 62; Husted et al., *supra* note 34.
97. 149 CONG. REC. S13043 (daily ed. Oct. 22, 2003) (statement of Sen. Leahy).
98. *Id.*
99. *See* 15 U.S.C. § 7701(a).

decrease more drastically.[100] By only requiring an opt-out device, Congress has implicitly given its stamp of approval to commercial mailers who already have large databases of addresses. Even though these addresses may have been obtained through fraudulent or even illegal means, these companies will be allowed to continue to send unsolicited e-mail up until the point where a recipient affirmatively says "no more."[101] This process will almost certainly result in a less immediate reduction in the volume of unsolicited commercial e-mail, and thus allow the cost-shifting from these advertisers to the service providers and recipients to continue.[102]

Along these lines, there is also concern that by only including an opt-out device, Congress may inadvertently *increase* the amount of unsolicited commercial e-mail, at least in the short run.[103] Because senders are permitted to send virtually unlimited amounts of commercial e-mail until a recipient takes affirmative action, legitimate companies that previously were wary about soliciting customers may throw caution to the wind.[104] The Act legitimizes these "early" messages, and may function as an incentive to send more messages.[105] Also, because the terms for legitimate commercial mailers are so favorable towards the senders, some fraudulent providers—those that use deceptive practices, such as relaying or masking of identity—may start providing "legitimate" service as well. While some may argue that such a move is exactly what the legislation should strive for (moving illegitimate businesses into a legitimate business model), one concern is that these spammers will not give up their fraudulent means, but merely augment them with an increased flow of "legitimate" spam.[106] And again, because of the

---

100. *Cf.* Himowitz, *supra* note 62 (suggesting that an opt-in model would better serve consumers); Husted et al., *supra* note 34 (suggesting that an anti-spam law should explicitly state that senders should not send spam); Henry Norr, *Bill Seeks To Stem Spam*, S.F. CHRON., Feb. 24, 2003, at E1 (discussing the ineffectiveness of California's opt-out law as the primary reason for passage of a new opt-in law).

101. *See* 15 U.S.C. § 7704(a) (West Supp. 2004); 149 CONG. REC. S13043 (daily ed. Oct. 22, 2003) (statement of Sen. Leahy).

102. *Cf. supra* note 100.

103. See Charles Arthur, *US Law To Cut Junk E-Mail Will Give Big Boost to Spammers, Warns UK Expert*, THE INDEPENDENT (LONDON), July 2, 2003, at 2; Jim Landers, *Turning Up Heat on Spam; Congress Sends Bill to Bush, but Some Say It Could Backfire*, DALLAS MORNING NEWS, Dec. 9, 2003, at 1A.

104. *See* Doug Bedell, *Spammers Given a Lift, Experts Say; Many Argue Newly Signed Act Is Too Soft, Legitimizes Methods*, DALLAS MORNING NEWS, Dec. 20, 2003, at 1D; Stanley A. Miller II, *Getting Spam Under Control; Experts Say New Law Opens Door for More Abuse*, MILWAUKEE J. SENTINEL, Mar. 2, 2004, at E4 (quoting David Sorkin, professor at John Marshall Law School).

105. Bedell, *supra* note 104.

106. *Cf.* Arthur, *supra* note 103 (proposing that illegitimate spammers would increase their output after passage of the Act).

difficulty of proving a negative, it will become harder to distinguish between the two forms.

Early measurements regarding the effect of the Act seem to verify this fear. Many surveys report that levels of unsolicited commercial e-mail actually increased in January and February 2004.[107] Overall, in the twelve months following enactment, the percentage of e-mail identified as spam has steadily increased.[108] Additionally, at least one known sender of unsolicited commercial e-mail has publicly stated that he will change his operations to comply with the standards set forth in the law, indicating that there is still "too much money involved" to walk away from the business.[109] Such realizations have led to the Act being nicknamed the "I CAN SPAM ACT," because it provides an outline for how to legally send unsolicited commercial e-mail.[110] A Federal Trade Commission official admitted as much in February 2004 by stating, "[t]his law provides some tools that we hope will be helpful, but it's not going to make a major difference."[111]

Additionally, over the past several years, savvy Internet users have become distrustful of opt-out procedures.[112] Many spammers have reportedly used such procedures as a means to verify the existence of a valid e-mail address.[113] Once a recipient responds to an opt-out mechanism, the spammer knows that the address is valid, and may send even more unsolicited mail.[114]

---

107. *See* Hiawatha Bray, *Survey Finds Do-Not-Call List Effective but Effort To Control Unwanted E-Mail Gets a Failing Grade*, BOSTON GLOBE, Feb. 21, 2004, at D1; Carrie Kirby, *Spam Keeps Coming Despite the New Law; You Can Complain to the FTC or State Attorney General, but It Might Not Resolve the Problem*, S.F. CHRON., Jan. 19, 2004, at E1. For more recent statistics on the volume of spam, see Spam Links, *Spam Statistics*, *at* http://spamlinks.net/stats.htm (last visited Mar. 12, 2005) (providing links to several organizations that provide spam statistics).

108. Spam Links, *supra* note 107. For example, MessageLabs estimates that the percentage of email identified as spam has increased from 63% to 83% from January 2004 to January 2005. *See* MessageLabs, *Email Threats*, *at* http://www.messagelabs.com/emailthreats/default.asp (last visited Mar. 12, 2005).

109. Saul Hansell, *An Unrepentant Spammer Vows To Carry On, Within the Law,* N.Y. TIMES, Dec. 30, 2003, at C1; *see also* Landers, *supra* note 103 (quoting the CEO of an e-mail advertising delivery company that orders have increased in anticipation of the new law).

110. Husted et al., *supra* note 34. As one advocate commented, "[a]s it stands, it fails the most basic test for any anti-spam law, which is telling people not to spam. . . . It doesn't say don't spam. It just regulates how to spam." *Id.*

111. Bray, *supra* note 107. *But see* Hiawatha Bray, *Tech Experts Say Spammers Are on the Run*, BOSTON GLOBE, Jan. 26, 2004, at C3 (arguing that a combination of new laws and new technology will result in a reduction of spam in the near future).

112. *See* Himowitz, *supra* note 62; Husted et al., *supra* note 34; Richards, *supra* note 62; Winter, *supra* note 62. Additionally, some security experts have warned that responding to fraudulent opt-out instructions could leave recipients vulnerable to viruses depending upon the methodology utilized. *Id.*

113. *See* Himowitz, *supra* note 62; Husted et al., *supra* note 34.

114. *See* Husted et al., *supra* note 34. *But see* Kirby, *supra* note 107 (quoting an FTC official that

Many recipients have fallen victim to this trap, and many more have been warned about it.[115] Because of this, recipients will face a tough choice—either trust the system and hope it works, or face the threat of even more unwanted messages.[116] While the overall effect of the opt-out system implemented in the Act is not yet clear, fears such as these will surely lead to a less than optimal system.

It would be difficult to believe that the omission of an opt-in requirement was an accident. In fact, interest groups voiced concerns about this missing feature. In a letter to Senator John McCain, an attorney from Consumer's Union wrote, "[W]e still have significant reservations about the . . . bill, because we believe that consumers will not see a significant reduction in spam without a guarantee that spam is disallowed unless the consumer opts to receive such materials."[117] Additionally, Senator Patrick Leahy expressed a "concern . . . that this approach permits spammers to send at least one piece of spam to each [e-mail] address in their database, while placing the burden on . . . recipients to respond."[118]

Furthermore, the Act provides an opt-in requirement for e-mail sent to wireless devices, such as mobile phones.[119] The rationale behind the more stringent requirement for wireless devices was twofold. First, there was a belief that unsolicited messages to a wireless device such as a phone were more intrusive than those sent to regular e-mail accounts, which are usually accessed from a computer.[120] Second, the provision was justified because some providers of wireless services charge based on the number of text messages received.[121] This produces an even greater shifting of costs to recipients because they must directly pay for the privilege of retrieving an unsolicited message. Still, the inclusion of the wireless provision indicates an awareness by at least some members of Congress of the existence of the more effective opt-in requirement.

It would appear that Congress engaged in a balancing act in crafting the dominant opt-out mechanism that applies to e-mail outside of the wireless frame of reference. Representative Heather Wilson of New Mexico has talked about offering legislation featuring an opt-in requirement, although the

---

the agency has never actually seen a case where opting out resulted in more unwanted e-mail).

115. *See* Silverman, *supra* note 63.

116. Husted et al., *supra* note 34; Silverman, *supra* note 63.

117. 149 CONG. REC. S13021 (daily ed. Oct. 22, 2003) (statement of Sen. McCain).

118. *Id.* at S13043 (statement of Sen. Leahy).

119. 15 U.S.C.A. § 7712 (West Supp. 2004).

120. 149 CONG. REC. H12195 (daily ed. Nov. 21, 2003) (statement of Rep. Markey).

121. *Id.*

competing bill she put forth in 2003 merely attempted to include stronger opt-out methods.[122] Although Congressional debates shed surprisingly little light on the reasons behind the rejection of an opt-in requirement, there appear to be two dominant concerns with such an approach. The first of these surrounds the constitutionality of an opt-in requirement; the second deals with its effect on the development of electronic commerce.

2. Constitutionality of Opt-In Methodologies

Constitutional challenges to strong anti-spam laws have centered primarily on the First Amendment and the Dormant Commerce Clause. For example, a trial court held that a Washington State anti-spam law violated the Dormant Commerce Clause because it was unduly restrictive and burdensome on interstate commerce.[123] Subsequently, the Washington Supreme Court reversed, holding that the benefits of the law outweighed any burdens on interstate commerce, and that the law was narrowly tailored to only affect Washington residents.[124] It should be noted that federal legislation would not implicate this concern, no matter how burdensome to interstate commerce. Congress clearly has the power to regulate commerce, and the CAN-SPAM Act was passed under this authority.[125]

Because unsolicited commercial e-mail would probably be regarded as commercial speech, any regulations would need to satisfy the constitutional requirements of the First Amendment.[126] Regulations of commercial speech are subject to the four-part test laid out in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[127] The first part of this test asks whether the speech in question concerns lawful activity and is not misleading.[128] While Congress recognized that a good amount of unsolicited

---

122. Jeff Nelson, *Competing Anti-Spam Bills Locked Up in Congress*, MILWAUKEE J. SENTINEL, Oct. 27, 2003, at 1D. Rep. Wilson's initial attempt at competing legislation stressed more inclusive definitions of what constitutes spam, but retained the opt-out methodology. *Id.*

123. State v. Heckel, 24 P.3d 404, 408 (Wash. 2001). *See also* Sabra-Anne Kelin, *State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435, 446-47 (2001).

124. *Heckel*, 24 P.3d at 413.

125. U.S. CONST. art. I, § 8, cl. 3; 15 U.S.C.A. § 7701 (West Supp. 2004).

126. *See*, *e.g.*, Nelson, *supra* note 122. "The Internet is just as much a space for legitimate commercial advertising as buying an ad in a newspaper or sending a piece of mail." *Id.* (quoting Congressman James Sensenbrenner).

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

128. *Id.*

commercial e-mail is fraudulent in nature, much of it is not, and therefore any regulation should pass this threshold question.[129]

The second part of the *Central Hudson* test asks whether the asserted government interest is substantial.[130] In the Act, Congress explicitly stated the importance of e-mail in the framework of national and international economic policy.[131] Congress also detailed the problems created by unsolicited commercial e-mail, including overloading the infrastructure and reduction of the effectiveness of e-mail as a tool of commerce.[132] Based on courts' historical willingness to recognize legislative determinations of governmental interest, the Act, even with an opt-in requirement, would likely survive this scrutiny.[133]

Next, *Central Hudson* asks whether the regulation directly advances the government interest asserted.[134] Given the interests that Congress has identified, it could be argued that requiring recipients to opt-in to receiving commercial e-mail would more directly advance the governmental interests. Such a requirement would likely reduce the volume of unsolicited e-mail more quickly, would allow for easier and faster identification of violators, and would more immediately shift the costs of unsolicited commercial e-mail from the service providers and recipients back to the senders.

Lastly, *Central Hudson* requires that the regulation must not be more extensive than is necessary to serve the government interest.[135] An opt-in requirement would still allow commercial e-mail, it would just require that businesses obtain affirmative consent from recipients before sending such e-mail. A carefully crafted bill would not interfere with the majority of legitimate messages. For example, it could still allow businesses to contact current customers regarding product information. More important, it would split the cost burden of obtaining consent between the senders of messages and recipients, rather than solely on recipients and service providers. This

---

129. 15 U.S.C.A. §§ 7701(7)-(8) (West Supp. 2004).

130. *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566.

131. 15 U.S.C.A. § 7701 (West Supp. 2004).

132. *Id.*

133. *See e.g.*, 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 504-505 (1996) (accepting the validity of the governmental interest, but holding that the interest is not effectively supported by the regulation); *id.* at 529 (O'Connor, J., concurring) (asserting that both parties agreed that government interest was substantial); Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 416 (1993); *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 568-69.

134. *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566.

135. *Id.*

would more directly advance the very important interests enumerated by Congress.

It should be noted that the ends-means test of *Central Hudson* may not be satisfied when the activities that are allowed contribute to the evil as much as the activities that are not allowed.[136] It would seem that the current version of the CAN-SPAM Act might fall under this description. It might be difficult for a court to strike down an opt-in requirement, if only because the lack of such a requirement admittedly may not reduce the amount of spam.

Constitutional concerns should not stand in the way of an opt-in requirement for the regulation of unsolicited commercial e-mail.[137] Although a problem for state legislative initiatives, the Dormant Commerce Clause poses no obstacle for federal legislation. Additionally, a carefully crafted statute should survive First Amendment challenges regarding commercial speech.[138]

3. Effects of an Opt-In Requirement on Economic Development

It would seem that Congress was more concerned with the effects strong anti-spam legislation would have on the growth of electronic commerce (and the position of American businesses in that growth) than the constitutionality of such regulation.[139] Businesses and groups with an interest in maintaining unsolicited commercial e-mail as a business tactic, including the Direct Marketing Association, backed the development of the current Act.[140] More

---

136. *See Discovery Network*, 507 U.S. at 427. "[T]he burden on commercial speech was imposed by denying the speaker access to one method of distribution . . . without interfering with alternative means of access to the audience." *Id.*

137. *See* David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1022 (1997) (stating Professor Sorkin's belief that a ban on unsolicited commercial e-mail would likely survive constitutional scrutiny).

138. *See* Fogo, *supra* note 80, at 930 (speculating that a complete ban on unsolicited commercial e-mail might pass First Amendment challenges if crafted narrowly). *Cf.* Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 357, 413 (2000) (arguing that a total ban on unsolicited commercial e-mail might survive a First Amendment challenge, but would be weakened by the availability of less restrictive alternatives). Note that the less restrictive alternatives mentioned by Fisher appear to not be very effective alternatives.

139. *See*, *e.g.*, Husted et al., *supra* note 34; *see also infra* notes 140-42 and accompanying text.

140. *See* Arthur, *supra* note 103; Husted et al., *supra* note 34; *see also* Norr, *supra* note 100 (discussing the Direct Marketing Association's opposition to state legislation in California that contains opt-in requirements). The Direct Marketing Association has apparently staked out a claim that unsolicited commercial e-mail is not just a good thing, but is necessary. Patricia Kachura, vice-president for ethics and consumer affairs at the DMA states, "[t]here are so many things in this world that you wouldn't know to ask for . . . . It's about offering things to consumers that they may in fact really need." Anuradha

importantly, members of Congress openly expressed concern about over-regulating the Internet, so as to not "impede or stifle the free flow of information," including commercial messages.[141] The Congressional Record provides examples of legislators indirectly stating their reasons for not passing more stringent requirements. For example, on October 23, 2003, Senator Russ Feingold stated, "Not all unsolicited commercial [e-mail] is bad. [E-mail] is an inexpensive way for businesses to advertise their products and we should not try to stamp out all such communications."[142] Such statements may shed light on a reluctance to regulate unsolicited commercial e-mail for fear of stalling economic development, possibly placing American businesses at a disadvantage to international concerns.

Still, the reasoning behind instituting relatively weak regulations is amazingly circular. The Act clearly states that the volume of unsolicited commercial e-mail threatens the future of e-mail as a viable means of communication, and more directly, the growth of electronic commerce domestically and internationally.[143] The Act then goes on to present regulations which arguably do not go very far in addressing these concerns. Moreover, the Act clearly rejects means which by any measure would more effectively deal with the problems enumerated in the Congressional findings.[144] The irony, of course, is that to justify these weaker measures, Congress seems to implicate an unwillingness to do anything that would harm the development of electronic commerce. In short, Congress has stated that it must do something to save electronic commerce, but cannot do anything because it might hurt electronic commerce.

These are the primary effects of only including an opt-out mechanism in the Act. Unfortunately, many secondary effects exist as well.

B. Fraudulent Spammers Will Still Be Difficult To Identify and Track

Although the Act does provide various mechanisms for enforcement, it does not directly confront the difficulty of identifying and finding illegitimate spammers.[145] This group would include the senders of unsolicited commercial

---

Raghunathan, *No Easy Escape "Opting Out"—Taking Action To Cut Off Credit Card Solicitations, Spam and the Like—Is Easier Said than Done*, DALLAS MORNING NEWS, Feb. 26, 2004, at 1A.

141. 149 CONG. REC. S13042 (daily ed. Oct. 22, 2003) (statement of Sen. Leahy).

142. *Id.* at S13125 (statement of Sen. Feingold).

143. *See* 15 U.S.C.A. § 7701(a) (West Supp. 2004).

144. *Id.* § 7704.

145. Winter, *supra* note 62. "The legislation does not address the underlying investigatory problem that all spam cases involve . . . ." *Id.* (quoting a Fort Lauderdale attorney who specializes in cyberlaw). *See*

e-mail who falsify subject information, relay through unsuspecting mail servers, or otherwise attempt to disguise their identities to make tracking difficult and expensive.[146] The Act continues the trend in previous legislation, both state and federal, that condemns these activities as illegal,[147] but it is not clear how enforcement of these provisions will be any more effective under the new legislation.

In fact, Congress rejected one particular approach which might have made enforcement just a little bit easier. While an opt-in requirement would not have made the fraudulent spammers disappear, it would have provided an even clearer guideline for enforcement agencies. Spam messages themselves would be easier to identify, as there would be little evidentiary question as to whether a recipient had initiated the transaction. Additionally, because of the more immediate reduction in traffic in unsolicited commercial messages, more resources could be utilized to track fraudulent senders, as opposed to navigating the evidentiary maze of legitimate spammers that the Act puts into place.

C. Preemption of Strong State Regulations

In an attempt to create a uniform legal landscape, the Act preempts most state regulations of unsolicited commercial e-mail.[148] The Act "supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages . . . ."[149] Because uniformity was a problem with state-by-state regulation, at first blush this would seem to be a useful and necessary provision.[150] However, the fact that uniformity was a problem before federal legislation does not necessarily mean that state laws cannot coexist with federal legislation.[151] Moreover, if the federal legislation were stronger, specifically including an opt-in requirement, preemption would not be so problematic.

---

also Kirby, *supra* note 107 (discussing the difficult process of tracking fraudulent spammers).

146. 15 U.S.C.A. § 7704 (West Supp. 2004).

147. *See* Bray, *supra* note 107 (pointing out that many spamming activities are covered by existing laws).

148. S. REP. NO. 108-102, at 13 (2003).

149. 15 U.S.C.A. § 7707(b)(1) (West Supp. 2004).

150. S. REP. NO. 108-102, at 13.

151. *See*, *e.g.*, Bedell, *supra* note 104 ("[S]tate officials believe they have the right to protect their citizens by whatever methods they choose.").

Several states have enacted laws that are substantively tougher than the federal CAN-SPAM Act.[152] These states have chosen to take a tougher stand against unsolicited commercial e-mail than Congress has chosen. The federal legislation may have the effect of actually weakening statutory controls in these jurisdictions.[153] In the event that plaintiffs and prosecutors are able to obtain jurisdiction, the question remains as to why they should not be able to choose a state court route.

An example of such legislation lies in California. Recently, that state passed a strict anti-spam bill, which requires senders of unsolicited commercial e-mail to obtain affirmed consent of recipients before sending e-mail.[154] California had previously had only an opt-out requirement, similar to the federal CAN-SPAM Act.[155] Officials believed that the weaker requirements did not adequately address the problem, and specifically passed the new legislation to correct that shortcoming.[156]

Some commentators correctly point out that the federal law does not preempt state laws where fraud is alleged.[157] This means that in cases involving fraudulent activity, such as manipulating e-mail header information, state laws may still be used. Additionally, because of the nature of e-mail, which can traverse borders unseen and unknown, federal preemption may be necessary to prevent a single state from setting the policies for the entire country. Still, given the limitations on state legislation regarding jurisdiction and interstate commerce, state officials are fretting over their inability to prosecute even the few cases where these hurdles may be overcome.[158]

D. The "Do Not E-mail" Registry

A key to the passage of the CAN-SPAM Act was the inclusion of a provision requiring the study and creation of a "Do Not E-mail" registry.[159] The idea for the registry came from the perceived success of the recently implemented "Do Not Call" registries utilized to combat unwanted telephone

---

152. Husted et al., *supra* note 34.

153. *Id.*

154. *See* Bedell, *supra* note 104; Husted et al., *supra* note 34.

155. *See* Bedell, *supra* note 104.

156. *Id. See also* Norr, *supra* note 100 (pointing out the ineffectiveness of California's opt-out legislation).

157. 15 U.S.C.A. § 7707(b)(2)(B) (West Supp. 2004).

158. Bedell, *supra* note 104.

159. 15 U.S.C.A. § 7708 (West Supp. 2004).

solicitations.[160] The e-mail version of this registry would theoretically work in a similar fashion to the telemarketing registries; some sort of central database would keep track of e-mail addresses that were not to receive unsolicited commercial e-mail, and senders would be required to check against this database before delivering their messages.[161] The idea received overwhelming support in both houses of Congress, and appears to have been a key addition in securing unanimous passage in the Senate.[162] In fact, some Senators appeared to view this provision as being among the most important of the Act.[163] The importance placed on the inclusion of this provision may indicate that even while praising the Act, at least some members of Congress recognized the overall weakness of the legislation.[164] Inclusion of an opt-in requirement, in fact, might have made the "Do Not E-mail" registry unnecessary.

Unfortunately, it is not clear that the analogy between telephone solicitation and e-mail solicitation is particularly strong. Critical differences exist in the basic structure of the two industries.[165] For example, the centralized nature of telephone service makes it relatively easy to track the source of a call.[166] Phone numbers themselves usually have some sort of geographic marker, such as an area code, and even toll-free numbers are easy to trace. Additionally, because wireless numbers are not publicly available, and businesses are often easily differentiated by name from residential customers, telemarketers can easily target the residential market. Calls generally connect directly from one point to another. Fraud, in terms of concealment of identification, tends not to be an issue.[167] Moreover, because of the expense of international calling, telemarketers are more likely to be domestically based.[168] Lastly, phone numbers tend to be fairly stagnant, with individuals only changing home numbers when absolutely necessary, such as when moving from one area to another.

---

160. Bray, *supra* note 107.

161. *See generally* 149 CONG. REC. S13012, S13024-27 (daily ed. Oct. 22, 2003) (statement regarding Schumer Amendment).

162. *See id.* at S13125 (statement of Sen. Feingold); *id.* at S13024-27 (statement regarding Schumer Amendment).

163. *See id.* at S13125 (statement of Sen. Feingold); *id.* at S13024-27 (statement regarding Schumer Amendment).

164. *See* 149 CONG. REC. S13012, S13043-44 (daily ed. Oct. 22, 2003) (statement of Sen. Leahy that he would support the Act, but had concerns).

165. *See* Himowitz, *supra* note 62.

166. *See id.*

167. *See id.*

168. *See id.*

Comparatively speaking, decentralized e-mail systems can make tracking e-mail much more difficult, particularly when senders purposefully attempt to hide their identities.[169] E-mail addresses themselves generally contain no information regarding the sender's location,[170] and spoofing of addresses is both easy and commonplace.[171] As recognized by Congress, fraud is a prevalent problem in unsolicited commercial e-mail.[172] Also, e-mail addresses tend to be transitory in nature, with people changing service providers and addresses much more frequently than phone numbers, and even having multiple addresses for different purposes.[173]

The success of the "Do Not Call" registries seems to be largely based on both the relative ease of identifying the callers, the legitimate, as opposed to fraudulent, nature of the business, and relatively static phone numbers.[174] These same factors would seem to make a "Do Not E-mail" registry much more difficult to implement. Identifying the senders of solicitous e-mail messages can oftentimes be difficult, and the admitted problems of fraud make it even more difficult.[175] Additionally, any system would have to account for all e-mail addresses (possibly even internationally), because there is no simple way to filter "home" addresses from "work" addresses, or even to filter based on geographic location. The load on such a system would be much greater than the relatively finite number of phone numbers with which the "Do Not Call" registries must cope.[176]

In fact, shortly after the Act passed, the Federal Trade Commission indicated it might recommend against such a plan.[177] FTC officials complained that enforcement would be almost impossible given the difficulty of identifying senders.[178] Additionally, concerns arose about spammers utilizing the database to harvest more potential recipients.[179] Lastly, keeping such a large database current would be extremely difficult given the flux of individual e-mail addresses.[180] Because of the sheer volume of the

169. *See id.*

170. *See* Sorkin, *supra* note 25, at 380.

171. *See id.* at 340.

172. *See* 15 U.S.C.A. § 7701(2) (West Supp. 2004).

173. *See* Husted et al., *supra* note 34.

174. *See* Himowitz, *supra* note 62.

175. *See* Kirby, *supra* note 107.

176. *See*, *e.g.*, Himowitz, *supra* note 62 ("Telemarketers churn out 100 million calls a day—a big number, but nothing compared to billions of spam messages flooding the Net.").

177. *See* Miller, *supra* note 104.

178. *See* Husted et al., *supra* note 34.

179. *See* Landers, *supra* note 103.

180. *See* Husted et al., *supra* note 34.

information that would need to be stored and updated, it is not clear that the FTC would have the resources necessary to effectively carry out such a task.[181] In June 2004, the FTC reported that a national registry would not work under present conditions.[182]

VI. HOW CONGRESS SHOULD APPROACH FUTURE LEGISLATION

In passing the CAN-SPAM Act of 2003, members of Congress recognized that this legislation would likely be only the first step in a federal response to the problem of unsolicited commercial e-mail.[183] Hopefully, this demonstrates a willingness to quickly revisit the statute, and make necessary changes.[184]

The single most important change needs to be the inclusion of an opt-in requirement in addition to the opt-out rules provided for in the Act. This would require senders of unsolicited commercial e-mail to obtain the affirmative permission of recipients before sending them commercial solicitations. Such permission might be gained from websites, from print advertising materials, point of sale locations, and other places where consumers typically interact with businesses. Additionally, unsolicited e-mail should be defined so as not to include correspondence from businesses to current customers, particularly regarding product information needed by the consumer, such as recall notices and safety information.

The inclusion of opt-in requirements should not relegate opt-out provisions obsolete. While the effectiveness of the opt-out provisions in the Act may be questioned, they would seem to work more effectively in conjunction with new opt-in requirements. The combination would lead to a faster reduction in the volume of unsolicited commercial e-mail, and allow for easier regulation of the remaining unsolicited commercial e-mail. This would also permit more resources to be trained on spammers who commit fraudulent practices, including those who refrain from honoring the established opt-out rules. The result is that the opt-in requirements would increase the effectiveness of the opt-out provisions.

---

181. *See* Kirby, *supra* note 107 (discussing the difficult process of tracking fraudulent spammers and the volume of complaints received by the FTC before the Act went into effect).

182. 2004 FTC NATIONAL DO NOT EMAIL REGISTRY, *supra* note 84, at 37. The FTC suggested a basic change in the structure of the e-mail system was needed, allowing better authentication of senders, before any registry could be effective. *Id.*

183. *See* 149 CONG. REC. H12194, H12197 (daily ed. Nov. 21, 2003) (statements of Reps. Dingell and Eshoo); 149 CONG. REC. S13044 (daily ed. Oct. 22, 2003) (statement of Sen. Cantwell).

184. *See* 149 CONG. REC. S13043 (daily ed. Oct. 22, 2003) (statement of Sen. Leahy).

Inclusion of opt-in regulations would also reduce the problems associated with preemption of state laws and the proposed "Do Not E-mail" registry. If the federal laws are as strong or stronger than most state laws, the need to preempt would, for the most part, disappear. Likewise, the need for the "Do Not E-mail" registry would be greatly reduced if the burden for maintaining affirmative consent of recipients is placed directly on the shoulders of the senders of unsolicited commercial e-mail.[185] Not only would the FTC not have to tackle what may amount to an unsolvable problem, but the public would not have to bear the cost of implementing such a system. Instead, the overall cost would be shared with the businesses that choose to participate in unsolicited commercial e-mailing.

VII. CONCLUSION

The CAN-SPAM Act of 2003 sets forth a bold policy statement, recognizing both the importance of e-mail to the global economy, and the severe consequences that the economy will suffer if unsolicited commercial e-mail is left unchecked. Given this recognition, it is somewhat puzzling that Congress chose remedies which may have little or no impact on the problem of spam. In the absence of requiring senders of unsolicited commercial e-mail to obtain affirmative permission from recipients before sending e-mail, the opt-out requirements of the Act will likely be ineffective. In this respect, the Act reads more like a "how-to" guide, establishing a framework for companies to "legitimately" spam. Senders will legally be allowed to send at least one unsolicited e-mail. Organizations that have been reluctant to take advantage of solicitous e-mail are more likely to join the fray. Recipients, after years of being warned not to reply to opt-out messages, are likely to resist trying the new system for fear of confirming their address and receiving even more spam.

While the dependence on opt-out mechanisms is the main shortcoming in the Act, several others abound. Aside from defining certain fraudulent activities as illegal (which other laws already appear to do),[186] enforcement

---

185. The FTC suggested that the need for the "Do Not E-mail" registry might disappear with the development of better authentication schemes for e-mail senders along with better enforcement of the CAN-SPAM Act. While the FTC report to Congress did not directly address the reliance on opt-out provisions, it stands to reason that any revisions to the Act that would make enforcement easier and more effective would diminish the need for the registry. 2004 FTC NATIONAL DO NOT EMAIL REGISTRY, *supra* note 84, at ii, 37.

186. *See* Bray, *supra* note 107.

agencies are not given much in the way of new weapons to deal with fraudulent spammers. In fact, preemption of stronger state laws may actually remove some devices from the legal arsenal. Lastly, the proposed "Do Not E-mail" registry will likely prove technically and practically impossible to implement in a meaningful way.

The unfortunate part is that inclusion of opt-in requirements would have more effectively dealt with most of these problems. The volume of unsolicited commercial e-mail would have been reduced more quickly, which would more closely align with the enumerated policy goals of the Act. With a reduced volume, fraudulent messages would be more easily identified, and more resources would be available to track and punish senders. Preemption of state statutes would not be as controversial because federal legislation would be stricter than almost all states. Additionally, the "Do Not E-mail" registry, which appears unlikely to be implemented in an effective manner, would not be necessary.

Congress had to balance various interests in crafting this legislation. Unfortunately, the balance came out solidly on the side of business interests as opposed to consumers. The result is likely to be legislation that on the surface shows great promise, but in practice has little effect. It did not have to be this way, and perhaps in the future it will not. A strong anti-spam law should require recipients to opt-in before receiving unsolicited commercial e-mail. Constitutional concerns could be overcome. Legitimate business interests would be better served, particularly when the alternative is an e-mail system that chokes economic development as opposed to allowing growth. The CAN-SPAM Act of 2003 represents the federal government's first direct attempt to regulate unsolicited commercial e-mail; hopefully, it won't be its last.