NOTES

ATTACKING A WINDMILL: WHY THE CAN SPAM ACT IS A FUTILE WASTE OF TIME AND MONEY

*Daniel L. Mayer**

I. INTRODUCTION

Aside from Al Qaeda, the single most unifying target of Americans' hatred in the twenty-first century seems to be unsolicited commercial electronic mail, or spam. An internet search on the topic reveals a heavily one-sided battle raging over spam's virtues or lack thereof. Informal personal websites, newspaper articles, and legal journal articles all concur that spam is a major problem that must be dealt with. Just as the federal government responded quickly to the widespread fear of terrorism by launching the USA PATRIOT Act,[1] it has attempted to appease the angry demands of the general population by enacting the CAN SPAM Act.

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[2] represents the first major attempt by the federal government to restrict spam. However, I argue that it is about as successful as was Don Quixote at attacking the windmill.[3] Because the most serious problems with spam can be addressed effectively through laws that already exist and current technology, the CAN SPAM Act is simply a superfluous, ineffective law.[4]

In the first part of this note, I will examine the problems that spam creates, namely, the perpetration of fraudulent schemes and the imposition of high costs on the public. Next, I will concentrate on the efforts to battle spam prior to the CAN SPAM Act, both in terms of legislation and of technology. Finally, I will evaluate the CAN SPAM Act itself and argue that it will prove entirely ineffective at slowing the growth of spam.

---

* J.D. Candidate, Notre Dame Law School, 2005; B.A., Arizona State University, 2001. The author wishes to express thanks to his wife, Suzy, for her love and support in the completion of this Note. Special thanks also to Mom, Dad, and Mark for their constant encouragement. Thanks also to Fiona, Ana, and Nel for inspiring in the author a deeper understanding of the law.

1. USA PATRIOT Act, Pub. L. No. 107-56 (2001).

2. 15 U.S.C. § 7701 (2004) [hereinafter CAN SPAM Act].

3. *See* MIGUEL DE CERVANTES SAAVEDRA, DON QUIXOTE DE LA MANCHA (Tobias Smollett trans., Farrar Straus Giroux 1986). In the story of Don Quixote, the hero lives in an imagined utopian world of knights and chivalry. He thus mistakes a windmill for a living giant threatening his ladylove, Dulcinea. He attacks the windmill on horseback and fails miserably, thereby destroying his lance and collapsing into a deep coma.

4. Like any ineffective or repetitious law, I argue that the CAN SPAM Act wastes valuable taxpayer money.

II. WHY STOP SPAM?

Aside from irritating large numbers of average e-mail users, spam has admittedly raised a number of other significant concerns. Consumers are annoyed by the waves of false advertisements washing up on the shores of their inboxes on a daily basis.[5] Parents are repulsed that pornographers indiscriminately send spam to their minor children.[6] Businesses complain that they are losing money due to the vast amounts of time spent sifting through the deluge of spam sent to employees' inboxes.[7] These are the primary frustrations driving the battle to stop spam. However, before we can find solutions to the spam problem, the nature of spam must first be explored and understood in detail.

A. Conned.com: Deceptive Advertising

Perhaps the most abhorrent aspect of spam in the eyes of legislators, scholars, and the general public alike is the fact that so much of it is misleading, deceptive and untraceable.[8] The Federal Trade Commission ("FTC") recently estimated that approximately 66 percent of all e-mails transmitted include false information.[9] In fact, a full 90 percent of spam messages regarding investment opportunities make false claims.[10] Integrity is obviously not a high priority for spammers[11] desperate to project their message to millions.

A key danger of spam is that these false advertisements can appear anywhere. The misrepresentations may be in the e-mail's header, the sender's address, or the body of the e-mail itself. For example, spammers will often leave the subject line blank, attempt to connote some business or personal relationship between the sender and receiver, or replace the true sender's e-mail address with that of the receiver.[12] They will also often list as their e-mail's subject a term that seems inviting or enticing regardless of whether it relates in any way to the topic of the e-mail, in the hopes that the recipient will open the message and read it.[13]

In what is perhaps a more sophisticated manner of conning recipients into opening their e-mail, spammers will often list an innocent third-party's e-mail address in the "from" or "reply to" field, thus making it appear to be from a private party rather than an advertiser.[14] This practice is known as "spoofing."[15] The first benefit of spoofing

---

5. Jonathan Krim, *Spam's Cost to Business Escalates: Bulk E-Mail Threatens Communication Arteries*, WASH. POST, Mar. 13, 2003, at A01.

6. *Id.*

7. *Id.*

8. FED. TRADE COMM'N., FALSE CLAIMS IN SPAM 3 (2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf.

9. *Id.*

10. *Id.*

11. Throughout this article, I will refer to those who send spam as "spammers."

12. *See* FED. TRADE COMM'N, *supra* note 8.

13. *Id.*

14. *See* Fed. Trade Comm'n, *FTC Announces First Can-Spam Act Cases* (April 29, 2004), *available at* http://www.ftc.gov/opa/2004/04/040429canspam.htm (last accessed Oct. 10, 2004).

15. *Id.*

for spammers is that recipients are generally more likely to open and read e-mails that do not appear to be spam. Another benefit is that those e-mails that are undeliverable, and thus returned to the sender, are received by third-parties, thereby assuring that the spam will be received by some consumer in the end.[16] A collateral effect of spoofing is that these innocent third-parties are often mislabeled as spammers themselves by spam-blocking software and watchdog groups, which can then lead to their e-mail being blocked by large numbers of recipients.[17]

Perhaps more troubling is the fact that the actual content of the e-mails themselves is also frequently fraudulent.[18] The e-mails are often used to launch such schemes as offers of miracle cures, easy weight loss, and the overnight improvement of reproductive organs.[19] The FTC's report on spam found that 60 percent of spam messages make false claims in the body of the message itself.[20] Why do spammers go through the trouble of sending such ridiculous messages? The answer, quite simply, is money. Spam is a very inexpensive manner for a con artist to reach large numbers of people, thereby making it an attractive means for achieving the ultimate scam. Twenty-first century con artists can reach vast numbers of innocent investors for little or no cost.

B. I Insist, You Pay: Cost-Shifting

The most harmful aspect of spam may lie in the fact that it shifts the costs of advertising away from the advertiser. As pointed out above, the cost to spammers for gathering e-mail addresses and sending spam to thousands or even millions of recipients is extremely low. But the cost to internet service providers ("ISPs") and recipients can be quite high. In fact, nearly the entire cost of the spammer's advertising is generally carried by the ISPs and recipients.[21] "Internet service providers . . . bear the primary cost of spam and do the bulk of the work of filtering spam and prosecuting spammers."[22]

Costs forced upon the ISPs by spam include: providing the server space both to send and receive massive amounts of e-mail; repairing servers that crash under the load of messages being transmitted; paying employees to handle subscriber complaints generated by spam; and developing and implementing means to screen and/or block spam.[23]

The costs forced on the innocent recipient can be no less dramatic and burdensome. Recipients bear the cost of time spent reading, responding to, and discarding spam messages. In fact, it has been estimated that the total annual cost to businesses for the time their employees spend sorting through and discarding spam is approximately $10

16. *See* FED. TRADE COMM'N, *supra* note 8, at X.

17. *Id.*

18. *Id.* at 8.

19. *Id.* at 2.

20. *Id.* at 8.

21. Bruce E. H. Johnson, *Is There a Constitutional Right to Bombard the Public With Penis Enlargement Proposals?*, 21-SUM COMM. LAW. 3 (2003).

22. *Id.*

23. Credence E. Fogo, *The Postman Always Rings 4,000 Times: New Approaches to Curb Spam*, 18 J. MARSHALL J. COMPUTER & INFO. L. 915, 919 (2000).

billion.[24] In total, the annual estimated amount that the economy expends dealing with spam is as high as $87 billion.[25]

For these reasons, spam has earned the boundless ire of America. It seems that most Americans would love to "can spam." However, as with most difficult issues, there are two sides to spam.

E-mail has not only created a nearly costless way for spammers to reach the public, but has also provided a low-cost means of legitimate advertising for smaller businesses around the country and the world. It provides a simple and inexpensive means for the exercise of free speech, whether commercial or private. Therefore, a total ban on spam would not only create obvious First Amendment problems, but would also harm those businesses who use e-mail for legitimate advertising purposes, many of which are small businesses that would otherwise be unable to reach such a wide audience.

There is no conflict among the general public or even among academics over the fact that the problem of spam is a real one that must be seriously addressed. There is widespread disagreement, however, over the best possible solution to the problem. I argue that the CAN SPAM Act is both ineffective and unenforceable, making it perhaps the worst of the options available. It adds little to the statutory tools already available for battling spam.

C. Pre-Quixote: Fighting Spam Before the CAN SPAM Act

ISPs and businesses had been battling spam for years before the CAN SPAM Act was even proposed.[26] In the past, the most popular weapons used included legal actions based on fraud and trespass to chattels,[27] as well as technological solutions such as spam blocking software.[28] Yet, these tools were largely ineffective. In fact, the amount of spam sent in 2003 is estimated to have been as much as 2,000 percent greater than that sent in 2002.[29] Part of the debate over the CAN SPAM Act, therefore, involves questions about why these measures failed and whether CAN SPAM adds anything to the mix that will make the law more effective at slowing the influx of spam to e-mail boxes nationwide.

a. Florida Land for Sale!: Fraud Actions

The first of the common actions used to battle spammers was created by the Computer Fraud and Abuse Act.[30] In short, this Act provides a cause of action for those who sustain damage due to an unauthorized party intentionally accessing their

24. *See* Johnson, *supra* note 21, at 3 (citation omitted).

25. *The True Cost of Spam*, MICROTIMES, *at* http://www.microtimes.com/165/internet.html (last modified Aug. 14, 1997).

26. Joseph D'Ambrosio, *Should "Junk" E-Mail Be Legally Protected?* 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 231, 235–236 (2001). D'Ambrosio discusses a number of efforts made using common law principles to battle spam.

27. *Id.* at 236–37.

28. *See* Symantec Brightmail Antispam, *available at* http:/ /enterprisesecurity.symantec.com /content/ displaypdf. cfm?pdfid=1022&EID=0(last accessed Oct. 10, 2004).

29. Johnson, *supra* note 21, at 3 (citing Chris Taylor, Spam's Big Bang, TIME, June 16, 2003, at 52).

30. 18 U.S.C. § 1030 (2004).

computers. Plaintiffs have used the Act to attack spammers who obtain e-mail addresses from protected computers without authorization and those who send large amounts of e-mail to members of an ISP despite that ISP's express disallowance of such spamming.[31] The Act also forbids members of an ISP from exceeding the access for which they are authorized. In the end, the Act creates a cause of action for any ISP that specifically forbids its users from harvesting e-mail addresses or sending spam.[32]

Thus, the Computer Fraud and Abuse Act provides a powerful weapon with which to battle spammers. Rather than placing the onus on the government to prosecute spammers, it gives private ISPs the tools to protect their members if they so desire. In fact, the world's largest ISP, America Online ("AOL"), has used this tool effectively a number of times to prevent its subscribers from sending spam using AOL's services.[33]

Despite the apparently effective options created by the Computer Fraud and Abuse Act, those who argue in favor of the CAN SPAM Act point out that all civil actions currently being used to sue spammers have done nothing to stem the tide of unauthorized commercial e-mail.[34] Their point is accurate in that the continued proliferation of spam has not slowed even with the victories that the Computer Fraud and Abuse Act and other civil actions have provided. However, this does not mean that another federal law will be more successful. The failure of the Computer Fraud and Abuse Act to stem the rising tide of spam may, in fact, be used as evidence in support of the argument that the nature of the internet is such that *any* federal law will be ineffective. I argue here that the rising number of spam messages sent every year has not increased due simply to the lack of a properly tailored federal law. A number of other factors drive the growth of spam, factors which seem simply beyond the effect of *any* federal law.

First, the sheer number of internet users makes finding spammers similar to seeking the proverbial needle in a haystack.[35] Second, technology develops so rapidly that by the time sluggish legislators and courts come up with a manner in which to deal with an internet crime, technology has often already created a new way to evade the law. Finally, federal laws have no impact whatsoever on spammers located outside of the United States. Illustrative of this point is the fact that the only attempts by the FTC to date to enforce the CAN SPAM Act have involved a Detroit-based corporation and a foreign corporation that ships all its products from within the United States.[36] The FTC relied on each of these corporations' substantial United States contacts in order to exercise jurisdiction. It is difficult to see how the Act could be used to stop a spammer with no United States contacts from continuing its fraudulent operation from a computer anywhere else in the world.

---

31. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001) [hereinafter Nat'l Health Care Disc.].

32. *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) [hereinafter LCGM].

33. *See, e.g.*, Nat'l Health Care Disc., *supra* note 31; *LCGM*, 46 F. Supp.2d 444.

34. *See* Fogo, *supra* note 23, at 922.

35. *See* Cindy M. Rice, Comment, *The TCPA: A Justification for the Prohibition of Spam in 2002?*, 3 N.C. J. L. & TECH. 375, 375–376 (2002) (discussing the vast number of people who use the internet and the rapid growth of such users).

36. Fed. Trade Comm'n, *supra* note 14.

In short, the fact that the Computer Fraud and Abuse Act has not effectively hampered the efforts of spammers is not an indication that new federal laws regarding spam are needed, but that federal laws attempting to regulate spammers are futile. The CAN SPAM Act will thus most likely emulate the Computer Fraud and Abuse Act in its failure to slow spammers, leading one to question why taxpayers' money should be spent to create and enforce such an act in the first place.

b. Keep Off the Server: Trespass to Chattels

Another common action used by plaintiffs when suing spammers is the old common law tort of trespass to chattels. Perhaps the best case illustrating this strategy is *Intel Corporation v. Hamidi,*[37] in which Intel, a major computer microchip manufacturer, sued under a trespass to chattels theory when a former employee, Kourosh Hamidi, repeatedly sent extremely large amounts of e-mail to Intel employees via their Intel e-mail accounts.[38] The trial court entered a judgment for Intel to which Hamidi appealed.[39] The California Court of Appeals upheld the trial court's decision, explaining that since Intel owned the network to which Hamidi was transmitting his e-mails they could choose to exclude certain messages from that network.[40] California's Supreme Court overturned this decision, however, pointing to the fact that a trespass to chattels action has always required a showing of damage to the chattel.[41] The court decided that Intel had not shown any damage to any of its property but had only proved that Hamidi had used their network.[42] This leads to the possible conclusion that had Intel argued under a trespass to real property theory, which does not require any showing of damage but only of unauthorized use of the property in question, it would' have been successful. Ultimately the court found that indirect financial loss due to its employees taking time to access and read Hamidi's messages did not constitute a violation of Intel's interest in its computers or its network.[43] Further, the court found that temporary use of Intel's servers and storage space did not constitute an injury for the purpose of a trespass to chattels action either.[44]

Hamidi recognized that a trespass to chattels action would be successful where a plaintiff is able to show that the defendant's use of its network had a "functional impact" on the plaintiff's efficient use of the system.[45] Thus, while Intel was ultimately unsuccessful in its claim, the court made it clear that an ISP *can* successfully sue a spammer for trespass to chattels upon a showing that the volume of spam has some sort of negative impact on the functionality of the network. Intel lost only because it had failed to plead such an impact.[46]

37. Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32 (2003).

38. *Id.* The e-mails aired complaints of Hamidi's about business practices at Intel. They generally attempted to attack employees' loyalty to the company.

39. *Id.* at 38.

40. *Id.* at 39.

41. *Id.* at 47.

42. *Id.* at 48.

43. *Hamidi*, 1 Cal. Rptr. 3d at 46.

44. *Id.* at 41–44.

45. *Id.* at 44.

46. *Id.* at 32.

The drawback to using trespass to chattels actions against spam is that the responsibility falls on the individual plaintiff to stop the spammer. The benefit, however, is that the plaintiff may recover costs if they are successful. It is the spammer that ultimately pays for the damages and the cost of litigation as opposed to these costs being levied upon the government and, ultimately, taxpayers. Further, large ISPs have the resources to take spammers to court and are responsible for so many e-mail accounts that even one court victory results in far less spam being sent to millions of e-mail account holders.

In contrast to the practical advantages of civil actions, the CAN SPAM Act allows injunctions only where the spammer has used some form of dishonesty in their messages or where they have sent e-mail to someone who has specifically opted-out.[47] But even in these situations, it is at the taxpayers' expense that such injunctions are implemented. Further, even where someone is listed on the no-spam list and has specifically requested not to be contacted by a particular spammer, spammers have shown ingenuity over the years at using false return addresses or switching their sender accounts quickly, thereby making it nearly impossible and very expensive to track down spammers who violate the Act. An action for trespass to chattels obviously does not make the process of finding violators any easier, but it is senseless to pour money into a new law that makes no headway in solving this problem. Further, another extant statute, the Lanham Act,[48] which prohibits the use of a false designation of origin, may also be used to attack those spammers that use a false return address.[49] Therefore, since both the flooding of a network with spam and the false designation of origin are already prohibited by the common law and by statute, it seems that the CAN SPAM Act is simply a superfluous addition to the Code.

c. Fire with Fire: Technology and the Private Regulation of Spam

Another tool that exists independent of the CAN SPAM Act is technology itself. Technology drives both the advances of spam as well as the battle against it. Spammers are constantly developing new ways of avoiding efforts to block their messages or detect their messages' origins. Private entities are always devising new technology intended to block spam altogether or make it more difficult for spammers to reach them.[50] Given the fact that it was private technology that created the spam problem, many argue that private technology is the only practical means for slowing spam's advance. It is commonly argued, in fact, that "[t]he most successful battle against spam is being waged through technology by large companies and ISPs."[51] For those who

47. CAN SPAM Act, Pub. L. No. 108-187, §§ 5, 7 (2003). The Act allows members of the public to opt-out of receiving spam by registering their e-mail address with a government created list. The Act forbids spammers from sending spam to any addresses on that list.

48. 15 U.S.C. § 1125(a).

49. For an example of a case involving spam and the Lanham Act, see Am. Online v. Prime Data, 1998 WL 34016692 (E.D. Va. Nov. 20, 1998) (finding defendant in violation of the Lanham Act for sending millions of e-mails falsely designating AOL as the source).

50. Jane Black, *The Guardian Angels of E-Mail*, BUS. WK. ONLINE (Sept. 2003), *available at* http://www.businessweek.com/technology/content/sep2003/tc20030892_7253_tc024.htm (last accessed Oct. 10, 2004).

51. Johnson, *supra* note 21, at 4.

wish to fight spam by technological means, a number of options are available.

The leading innovator in spam-blocking technology is Brightmail, Inc.[52] Its software programs are available to both businesses and ISPs and promise to block nearly all spam.[53] Brightmail has set up one million e-mail accounts by which it seeks to attract spam.[54] Its staff reads through all the spam that comes in, categorizes it, and then adds new spam senders to the list of addresses that the software will block.[55] The success of Brightmail's software lies in the fact that it employs actual people to read e-mail rather than using a machine or software program. This ensures that Brightmail will find spam sent using randomization software.[56] Brightmail's website boasts that only one message in a million is falsely designated as spam and thus wrongly blocked.[57] The availability of such software appears to render the debate over such measures as the CAN SPAM Act entirely meaningless. Using such software, those who do not want to receive spam can simply sign up with Brightmail or a similar service, thereby blocking all spam. Without the need for opting out or prosecuting a claim, spam sent from throughout the world, whether or not in violation of the CAN SPAM Act, will be barred from ever reaching a user's inbox.

One common argument against leaving the spam battle in the hands of such technology is that the effective spam blocking software is too expensive for the average individual to afford.[58] Brightmail's website itself seems to effectively answer this concern, however. The company admits that its software is too expensive for most individual users to afford and, in fact, it does not even sell its product to individuals.[59] However, some of its largest clients are ISPs such as AT&T and MSN.[60] Thus, Brightmail suggests that individuals who desire to block spam from their inboxes simply set up their e-mail accounts through an ISP that subscribes to Brightmail.[61] If users take this advice, it seems that the technology is available and affordable for any internet user to block nearly 100 percent of spam from ever reaching their inboxes. It is up to individual users: if they do not want spam, they can sign up with a spam-blocking ISP.

Another technical option used by a number of ISPs is to allow users to simply report spam to the ISP and request that it be blocked from their specific account.[62] Thus, if a user no longer wishes to receive e-mail from a specific sender, they can simply ask the ISP to stop accepting mail from that sender. While this system is not as effective against stopping spammers who are using randomization software, it does provide users with another powerful weapon in blocking a significant amount of spam.

---

52. Black, *supra* note 50.

53. Symantec Brightmail Antispam, *supra* note 28.

54. Black, *supra* note 50.

55. *Id.*

56. *Id.* Randomization software is a program used by spammers that randomly adds meaningless figures to the end of every subject line or text in order to avoid being stopped by software attempting to block the messages.

57. Symantec Brightmail Antispam, *supra* note 28.

58. Johnson, *supra* note 21, at 4.

59. Symantec Brightmail Antispam, *supra* note 28.

60. Johnson, *supra* note 21, at 4.

61. Symantec Brightmail Antispam, *supra* note 28.

62. Johnson, *supra* note 21, at 4.

Blacklists are another strong weapon used to fight spam. A number of independent companies keep lists of spam addresses and sell those lists to companies and ISPs.[63] Those companies and ISPs then simply block their inboxes from accepting e-mail from the addresses on the list.[64]

Some internet users, mostly private companies and ISPs, also choose to utilize a method inverse to that of the blacklist. Rather than receiving mail from all addresses except those on the blacklist, software can be set up to receive mail from only those addresses specifically included on a "whitelist."[65] This solution seems particularly attractive for those entities that know they only need to receive e-mail from specific addresses. Some companies, for example, only need to receive messages from particular clients or vendors and have no interest in allowing messages of any other nature to come in, whether personal or spam. The company can, of course, add new addresses to the whitelist at any time they wish.

The final and perhaps most simple technological solution to the problem of spam has been available and widely used since e-mail was first invented. Any internet user can simply delete all messages from their inbox for which they do not recognize the sender. With the internet moving at increasingly higher speeds, this takes less time than ever. This simple and obvious solution suggests that perhaps those who choose indiscriminately to open and read every e-mail they receive have no one to blame but themselves for the time they waste reading spam.

After considering the technological solutions described above, the CAN SPAM Act again appears to be an unnecessary legislative maneuver. Brightmail and other blocking technologies can block spam sent from anywhere in the world while the CAN SPAM Act will only be enforceable against those within the jurisdiction of the United States. Further, the CAN SPAM Act is implemented only when the FTC or some individual user is willing to bring a complaint against a spammer and pursue it to the end. The First Amendment is protected with such programs because it is the user, not the government, who determines what will and will not be received in any given e-mail box. In this way, e-mail may even be seen as an improvement upon traditional postal service mail, for the recipients can block unwanted advertising from their e-mail boxes but not from their mailboxes. The government does not find it necessary to stop bulk advertising sent to mailboxes; it should also stay away from regulating mail sent to e-mail boxes.

d. Let Me Try!: State Legislation

The majority of states have enacted some form of law that attempts to limit the amounts of spam being sent to its citizens.[66] No discussion of pre-CAN SPAM Act attempts at slowing the spam growth would be complete without mention of these ill-fated efforts by state legislators.

63. *Id.*
64. *Id.*
65. *Id.*
66. *See* Fogo, *supra* note 23, at 923.

The attempts by states at drafting effective laws to deal with the problems of spam have varied widely in their approach. Rules have ranged everywhere from those outlawing specific content in spam[67] to those simply requiring some form of opt-out option within the body of the e-mail.[68] Most of these laws have been completely ineffective due either to the ease with which they are avoided by spammers or to difficulty on the part of the state in prosecuting offenders.

The internet reaches all over the world and, consequently, across state lines. It is therefore very difficult for states to draft laws that do not violate the Dormant Commerce Clause.[69] Thus, no state has the ability under federal law to ban spam completely. Consequently, no state has attempted to do so.[70] Those states that begin with the goal of banning spam end up with some statute falling far short of doing so, often with the result of enacting a completely ineffective statute.[71]

As an example, we should evaluate Nevada's spam law. The Nevada legislature began with the lofty goal of banning all spam. Their final law, however, simply required that spam include a return address and instructions for being removed from the spammer's e-mail list.[72] The result of all the time spent getting the law drafted and passed is that Nevada now has a law that has failed to slow the influx of spam to its residents' inboxes even at a minimum amount. In fact, the law has not slowed spam at all; it simply changed some of the content of some of the spam that still arrives en masse on a daily basis.

Regardless of how strict or lenient various state statutes have been, they have obviously been entirely ineffective at slowing spammers.[73] A federal regulation will certainly solve problems with the Dormant Commerce Clause, but will do nothing about the fact that spammers are constantly developing new manners of circumventing the laws or avoiding capture. Just as state legislatures are troubled by the *interstate* nature of spam, the federal government is troubled by the *international* nature of spam. Perhaps rather than proving the need for federal regulation, these failed state laws in fact prove that *any* government regulation of spam simply will not work.

D. Colliding With the Windmill: Why CAN SPAM is Unnecessary

Because spam has taken deeper and fuller breaths despite all attempts to choke it, it seems Congress felt there was no other option than to pass a new federal law outlawing spam. I was unable to uncover any instances in which scholars or lawmakers recognize

67. *See* MD. COMM. LAW CODE ANN. § 14-3002 (2003); *see also* W. VA. CODE § 46A-6G-2 (1999).

68. *See* NEV. REV. STAT. § 41.705 (1998).

69. The Dormant Commerce Clause is defined as "[t]he constitutional principle that the Commerce Clause prevents state regulation of interstate commercial activity even when Congress has not acted under its Commerce Clause power to regulate that activity." BLACK'S LAW DICTIONARY 263 (7th ed. 1999). Therefore, if a state drafts an anti-spam law that effectively attempts to regulate the internet activity of those in other states, the law will most likely be found unconstitutional.

70. *See* Fogo, *supra* note 23, at 923–924.

71. *Id.* (citing NEV. REV. STAT. § 41.705 (1998) and H. 2752, 55th Leg., 1998 Reg. Sess., 1998 WASH. LAWS ch. 149).

72. NEV. REV. STAT. § 41.705 (1998).

73. *See* Johnson, *supra* note 21, at 6.

that the Act will likely have little or no effect on slowing spam. Similarly, the high cost likely to be associated with upholding the Act has been largely ignored.

a. Screen Door on a Submarine: Effectively Unenforceable

Due to the fact that spam, whether deceptive or not, is extremely profitable, spammers are not likely to give up their enterprise without a fight. Only one recipient in 10,000 need respond in order for a spammer to turn a profit.[74] As discussed above, the effect of prosecution under existing laws and the development of new technology to block spam has only had the effect of rendering spammers more determined and more able to circumvent both the law and technology. There is no reason to expect the effect of the CAN SPAM Act to be any different. Honest entrepreneurs using spam as an inexpensive form of advertising might be scared away from using spam, but those who care little for honesty or legality will unlikely be deterred due to the fact that the Act can easily be avoided altogether. For example, while the majority of spammers today are located in the United States, there is little to stop spam enterprises from simply sending their spam from computers located outside the United States.[75] AOL has reported that since the CAN SPAM Act went into effect, they have noted a ten percent shift in the origins of spam from U.S. internet addresses to those located outside the country.[76] The U.S. government has no jurisdiction to either prosecute or enforce the CAN SPAM Act in such instances. European legal efforts at reducing spam provide an excellent parallel to this problem.

The European Union ("EU") disallows the sending of spam to anyone who has not first given permission to receive it.[77] This is generally referred to as an "Opt-In" requirement. However, this law has done little to slow the influx of spam into EU member countries.[78] One possible reason for this is that European countries vary widely in the manner in which they enforce anti-spam laws.[79] Another is that a large percentage of spam received by citizens of EU member countries is sent from foreign addresses, thus rendering the European governments powerless in enforcing their laws.[80] While the CAN SPAM Act does not include an opt-in requirement, and our American courts are more likely to be consistent in their enforcement of the law, spammers will still be free to simply send their spam from other countries as many have been doing since the Act's passage.

One (albeit unlikely) option for filling this gap in enforcement is to convince foreign courts to recognize and enforce the judgments of our courts regarding the CAN SPAM Act. It is not uncommon for countries to extradite accused criminals or recognize a judgment against one of its citizens issued by a foreign court in order to

74. Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-Mail*, 4 VA. J. L. & TECH. 4, 15–17 (1999).

75. Johnson, *supra* note 21, at 6.

76. *Tech News Roundup*, SAN JOSE MERCURY NEWS, Jan. 8, 2004, at 2.

77. *See Spam Laws: European Union/EEA*, *available at* http://www.spamlaws.com/eu.html (last accessed Oct. 10, 2004).

78. Johnson, *supra* note 21, at 6.

79. *Id.*

80. *Id.*

either comply with the terms of a treaty or maintain good diplomatic relations. However, there are a couple of serious obstacles to this solution.

First, in order for such a solution to be effective, the United States would need to get every country in the world to agree to the enforcement of the CAN SPAM Act. Otherwise, spammers could simply move their computers to those countries that are not enforcing the Act. Just as countries with strict bank privacy laws have traditionally attracted criminals to their banks, countries not agreeing to aid the United States in enforcing the CAN SPAM Act would become quite attractive to spammers. Further, it is likely that a significant number of countries would not agree to enforce the Act due to a conflict with their own laws. An ironic example of this is provided by the case of *Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisemitisme.*[81] In that case, our own federal courts refused to enforce the judgment of a French court against Yahoo!, Inc. for violating the French law against displaying Nazi memorabilia because of a conflict with the First Amendment of our Constitution.[82]

The result for the United States government is a catch-22. Courts and law enforcement officials can enforce the Act aggressively and consistently, thereby encouraging spammers to send their spam from elsewhere; alternatively, they can take the less expensive route of enforcing the Act only on occasion or when pressed to do so by some private entity, in which case spam will continue to thrive in the same fashion as it does now. Therefore, if the goal is to reduce dishonesty and the costs of spam, the CAN SPAM Act seems only to create a lose-lose situation.

b. "Plead the Fifth Because You Can't Plead the First": Chilling Effect on Speech

While the CAN SPAM Act does not seem to violate the First Amendment in that it only bans spam when the receiver requests being placed on the no-spam list, the Act will undoubtedly have a chilling effect on commercial speech. Most citizens who sign up for the list will likely do so to avoid the barrage of misleading spam that they now receive. But the law is unlikely to protect these internet users. This is because those spammers who are most likely to abide by the CAN SPAM Act are those who are already honest and ethical in their use of spam. Dishonest spammers are more likely to ignore the law as they have done up until now. They will continue to send spam, either moving out of the country or relying on new technology to evade the law. Thus, the effect will be that honest businesses, from small, family-owned stores to large corporations, that use spam sparingly as an inexpensive form of advertising, will have millions of citizens removed from their reach while the fraudulent and dishonest spammers will still reach the entire internet-using public. In effect, that commercial speech that ends up in the inbox of a citizen on the no-spam list is more likely to be from a fraudulent spammer who is ignoring the law. Those citizens will not hear from

81. 169 F. Supp. 2d 1181 (N.D. Cal. 2001). In this case, the French court had ordered Yahoo! to discontinue allowing Nazi memorabilia to be sold on its French auction site. France had no way of enforcing this order, however, since Yahoo! is a California based corporation. They requested that the District Court order Yahoo! to comply with the French order, which the District Court refused to do on the grounds that doing so would amount to a violation of the First Amendment. This case shows the difficulty faced by any country in enforcing its internet laws in foreign lands.

82. *Id.*

honest, responsible, and law-abiding advertisers who stand to benefit greatly from a cheap advertising medium.

Another possible effect of the CAN SPAM Act is that smaller businesses could be dissuaded from using e-mail to advertise simply because they do not want to risk violating the law. Larger, wealthier corporations have greater access to legal advisers who can help them avoid the pitfalls of the Act while smaller companies that can not afford to pay for legal advice will be forced to abandon spam as an advertising option. While most of us are not bothered to hear that someone will be sending less spam to our inboxes, we are angry when we hear that the law favors large corporations over small business owners.

c. Fork It Over: The Cost of the Act

The FTC's Budget Summary for the fiscal year 2003 set the initial cost for establishing a national do-not-call list at $5 million.[83] This, of course, does not take into account the future costs of maintaining the list, investigating complaints, and prosecuting violations. It seems fair to assume that the costs of establishing a no-spam list will at least be similar, as will the costs of enforcement. Add to these costs the future expense of enforcing the other parts of the CAN SPAM Act, and it becomes clear that the Act will cost taxpayers a substantial amount of money over time.

Admittedly, these costs are low when compared to other government spending.[84] However, it seems that even a small amount is too much to spend on a law that will likely have little or no effect at achieving its desired end. As discussed above, the Act will probably not slow the stream of spam flowing into our inboxes if neither state action, litigation, nor technology has had made a serious impact in the past. And if the failure of stringent anti-spam laws in Europe are any indication, we cannot expect success from the CAN SPAM Act.[85] In fact, absolutely no decrease in spam has been detected in the months since the Act has been in effect.[86] It is ludicrous to spend even a small percentage of taxpayer money on a program that has not been and never will be effective.

III. CONCLUSION

The CAN SPAM Act is a misguided effort by Congress, our own Don Quixote in this instance, to attack the monstrous windmill that is spam. In both the short and long terms, the CAN SPAM Act will likely prove entirely ineffective in the battle on spam. Even if lawsuits under the Act are successful in a large number of cases, spammers will continue to develop the technology necessary to evade the government or will simply

83. Fed. Trade Comm'n, Fiscal Year 2003 Congressional Justification Budget Summary, 8 (2003), *available at* http://www.ftc.gov/ftc/oed/fmo/budgetsummary03.pdf (last accessed Oct. 10, 2004). The FTC began operating a "no-call list" to which members of the public could register their telephone number. Law forbids telemarketers from contacting any telephone number on the list. The CAN SPAM Act provides the FTC with the authority to institute a similar list with regard to spam—a "no-spam list," if you will.

84. *See id.* The total budget for the FTC in the year 2003 was $171,599,000. *Id.*

85. Johnson, *supra* note 21, at 6.

86. Anick Jesdanum, *Filtering Firms Say Anti-Spam Law Ineffective*, ARIZ. DAILY STAR, Jan. 12, 2004, at A1.

move out of the country to send their messages. While private regulation of spam via technological means is not perfect and, at this point, has been unable to stop spam altogether, its victories have had a wider impact than any government regulations. The government should save taxpayers' money rather than throwing it into the CAN SPAM Act and wasting both time and money in a futile attempt at slowing the tide of spam in America.