Chicago-Kent Journal of Intellectual Property

Volume 4 | Issue 1 Article 1

9-1-2004

CAN-SPAM: A First Step to No-Spam

Grant C. Young

CAN-SPAM: A First Step to No-Spam[1]

By
Grant C. Yang

On December 16, 2003, President George W. Bush signed the first federal law regulating spam.[2] The law, titled the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (CAN-SPAM), has garnered much criticism from scholars and the Internet community. Its effectiveness has even been questioned[3] by the Federal Trade Commission (FTC), the regulatory agency in charge of administering the law.[4] On the other hand, the law, effective as of January 1, 2004,[5] has the support of both Internet Service Providers (ISP)[6] and the advertising industry.[7] It has been regarded by many as a necessary step in order to combat the growing amount of spam. Critics contend that it is less effective than many of the current state laws. However, they must realize that CAN-SPAM is not meant to be a cure-all. Instead, it is a

---

[1] This article is based on information, as available to the author, as of Mar. 7, 2004. Grant Yang is a candidate for JD/LLM in International and Comparative Law, class of 2005. The author would like to thank Jason Yang, Kristen Freeman, Andrew Wasson and Dessa Baker for their help and support, as well as the staff of the Chicago-Kent Journal of Intellectual Property.

[2] Declan McCullagh, *Bush OKs Spam Bill--But Critics Not Convinced*, CNET NEWS.COM, *at* http://news.com.com/2100-1028_3-5124724.html?tag=prntfr (last modified Dec. 16, 2003).

[3] *Id.* (Tim Muris, chairman of the FTC said the measure, "could actually be harmful" to the FTC's ongoing efforts to sue spammers.).

[4] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, § 7(a), 117 Stat. 2699, 2711 (2004) ("this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57(a)(1)(B)"); *Id.* § 3(D)(3) ("COMMISSION.--The term 'Commission' means the Federal Trade Commission.").

[5] *Id.* § 16 ("EFFECTIVE DATE. The provisions of this Act, other than section 9, shall take effect on January 1, 2004.").

[6] *See Anti-Spam Law Near, But Critics Take Aim*, CNN/MONEY, Nov. 24, 2003, *at* http://money.cnn.com/2003/11/24/technology/spam_law/index.htm.

[7] Stefanie Olsen, *Ad Groups Lobby for Antispam Law*, CNET News.com, *at* http://news.com.com/2100-1024-5107059.html?tag=nl (last modified Nov. 13, 2003) (Powerful advertising trade groups such as the American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA) and the Direct Marketing Associating (DMA) have been pushing Congress to pass a federal antispam law.).

necessary first step toward uniformity in spam laws, as ultimately, the most viable solution will require an international approach.[8]

No single law or method is going to stop spam. Because of the intangible and boundary-less nature of the Internet a technical solution and international solution is necessary. Spam fighters should take their cues from law enforcement's work to curb other criminal offenses with characteristics similar to those of spam. One of the oldest international crimes, money-laundering, has many similar attributes as spam, which allow launderers to evade enforcement officials. By looking at the techniques and methods of international cooperation applied to money-laundering laws, countries can emulate the legislative and coordinating efforts used to combat money laundering and apply this to the war on spam.

Part I of this article provides a background of the medium of electronic mail (e-mail) and the types of spam. This section also describes the profile of spammers and their incentives for entering the spam market. Part II briefly examines the negative impact that spam plays in the dynamics of e-mail use. Part III illustrates the various features that CAN-SPAM provides and compares them with provisions of several state spam laws. Finally, Part IV presents many of the solutions that have been used in the fight against spam.

I. Background

E-mail has been hailed as the original "killer app" of the Internet[9] and it is a pervasive aspect of Internet life. An e-mail is a data file, usually a text message, sent from a computer,

---

[8] *See* Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Testimony and Statement of Record before the Committee on Commerce, Science and Transportation (May 21, 2003), *available at* http://www.epic.org/privacy/junk_mail/spam/spamtestimony5.21.03.html.

[9] Deborah Fallows, *Spam: How It Is Hurting Email and Degrading Life on the Internet*, PEW INTERNET & AMERICAN LIFE PROJECT, Oct. 22, 2003, *at* 6, *at* http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf. A "killer app" is the "application that actually makes a sustaining market for promising but under-utilized technology." *Dictionary Definition of "killer app"*, HOSTINGWORKS, *at* http://hostingworks.com/support/dict.phtml?jargon=killer+app (last visited Jan. 11, 2004). In other words, a "killer app" is the application that entices people to use a certain technology.

traveling through various interconnected computer networks, and arriving at a destination computer.[10] The route by which the data packets are sent through the Internet is indeterminable, as the path of the packets is decided dynamically depending on the efficiency and expediency of the path.[11] A study conducted by the Pew Internet & American Life Project stated that 93% of adult American Internet users (about 117 million people) use e-mail.[12] The number of e-mails sent each year has increased significantly with the prevalent use of the Internet.

Unfortunately, the amount of spam e-mails has risen along with the amount of legitimate e-mail. Almost 15 billion spam messages are sent daily,[13] and this number is growing in volume by 15-20% a month.[14] Spam constituted half of all e-mail traffic in 2003, up from an estimated 7% in 2001.[15] If left unchecked, experts estimate that, within a year, nine out of ten emails will be spam.[16] Surprisingly, only 25% of people see spam as a problem;[17] however, upon closer examination those who consider spam to be a big problem are more likely to have an expansive online presence and to be longtime, active members of the online community.[18] As broadband becomes less expensive and the Internet becomes more accessible, people are likely to extend their online presence and become more active members of the online community. As a consequence, spam is likely to become an increasingly burdensome problem in the years to come. Venture capitalists and technologists have recognized this trend. There are approximately

---

[10] *See* David Sorkin, *Unsolicited Commercial E-mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1005 (1997).
[11] *Id.* at 1006.
[12] Fallows, *supra* note 9, at 6.
[13] *Id.* at 7.
[14] Bill Husted & Ann Hardie, *Spam Wars Play Out Across Internet*, THE ATLANTA JOURNAL-CONSTITUTION, Dec. 14, 2003. In 2003 alone, spam increased by 77% over the previous year. McCullagh, *supra* note 2.
[15] CAN-SPAM Act of 2003 § 2(a)(2).
[16] Husted, *supra* note 14.
[17] Fallows, *supra* note 9, at 37 (In addition, 60% of e-mail users view spam as "annoying, but not a big problem," and 15% view spam as "not a problem at all.").
[18] *Id.* at 37-38. It seems to make sense that those who are significantly more involved in the online community would have a larger presence thus allowing spammers to get access to their information and e-mail address. Those users tend to do more activities online, have multiple email accounts, and whose e-mail accounts were "published" on the Internet long before spam was a problem.

a thousand businesses selling anti-spam software,[19] and the anti-spam and content filtering industry, a $1 billion market in 2003, is expected to grow 25 percent annually for the next few years.[20]

A. What is "Spam"?

It is clear that spam is a problem, but the definition of spam[21] itself is unclear. Generally, 92% of email users agree that spam is "unsolicited commercial email from a sender they do not know or cannot identify."[22] However, there is much disagreement and variation among e-mail users as the definition appears to depend upon several factors, such as the sender and the subject matter of the message.[23] These factors make it difficult to create legislation to curb the use of spam. Academics generally define spam as either Unsolicited Commercial E-mail (UCE) or Unsolicited Bulk E-mail (UBE);[24] CAN-SPAN is tailored to the UCE definition.[25]

The consensus is that spam must be unsolicited,[26] but from there scholars and experts disagree on other characteristics that may be classified as spam. CAN-SPAM does not actually

---

[19] Stephen Baker, *The Taming of the Internet*, BUSINESSWEEK, Dec. 15, 2003, at 79.
[20] Paul La Monica, *Investing in the War On Spam*, CNN/MONEY, Sept. 30, 2003, *at* http://money.cnn.com/2003/09/30/technology/techinvestor/lamonica/index.htm.
[21] The origin of the word spam is debatable. However, it is generally attributed to an incident in the 1980's when a Multi-User Shared Hallucination (MUSH) user created a macro that repeatedly typed the word "SPAM," a Monty Python skit where a restaurant served only spam, or directly from the meat product itself. *See* David Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325, 325 n.2 (2001). A MUSH is a user-extendable Multi-User Dungeon (MUD), which is a computer program, usually online, that allows users to play role-playing games. *See Multi-User Shared Hallucination*, DICTIONARY.COM, Mar. 16, 1995, *at* http://dictionary.reference.com/search?q=multi-user%20shared%20hallucination. There are variations of the requirements of spam. *See The Definition of Spam*, THE SPAMHAUS PROJECT, *at* http://www.spamhaus.org/definition.html (last visited Jan. 11, 2004).
[22] Fallows, *supra* note 9, at 9.
[23] *See id.* at 10.
[24] *See* Sorkin, *supra* note 21, at 333. It is beyond the scope of this paper to discuss the arguments of defining spam as UCE or UBE. For an in depth discussion see *id* at 334-35.
[25] *See* CAN-SPAM Act of 2003 § 2(b)(1).
[26] However, what does it mean for an e-mail to be unsolicited? According to studies, 65% of email users do not consider UCE to be spam if it comes from a sender with whom they have already done business, but 32% of email users consider any UCE to be spam and 11% say that UCE is spam even when they have given the sender permission to contact them. Fallows, *supra* note 9, at 10.

define the term "unsolicited."[27] However, CAN-SPAM does not target unsolicited spam; rather, it prohibits fraudulent commercial e-mails and requires an opt-out provision.

There are many types of spam. Most spam campaigns are fraudulent: a 1998 FTC study listed what it calls the "dirty dozen," the scams most likely to arrive via bulk e-mail.[28] For instance, "phishing" is a type of spam where an e-mail user receives an e-mail that simulates a trusted company. This leads the user to provide account or credit card information, which ultimately results in identity theft and credit card fraud.[29]

B. Spam Techniques

Spam is most effective when sent in bulk, thus spammers use various methods to gain access to e-mail addresses. Many spammers use harvesting programs to scour the Internet looking for publicly available e-mail addresses.[30] However, spam has exploded because spammers have started using techniques to obtain e-mail addresses which may not have been made publicly available by the e-mail user. For example, harvesters may implement a "dictionary attack," using an algorithm which creates variations of e-mail address combinations. When an e-mail address succeeds against the mail server, the address is automatically recorded onto an e-mail list that can be resold to other spammers.[31]

---

[27] *See* CAN-SPAM Act of 2003 § 3. In fact, other than in the preliminary congressional findings and policy section at the beginning of the act and the amendment to chapter 47 of title 18 regarding "Fraud and related activity in connection with electronic mail," CAN-SPAM does not reference the word "unsolicited." *See Id.* §§ 3 & 4.

[28] *FTC Names Its Dirty Dozen: 12 Scams Most Likely To Arrive Via Bulk Email*, July 1998, *at* http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.pdf. One of the most famous scams is the Nigerian 419 scam, named after Section 419 of the Nigerian penal code. Typically these scams can cost a victim $3,800, but the losses to individual victims have amounted to as high as $320,000. *See* Jim Stratton, *Notorious E-mail Scam Snares Volusia Retiree's Nest Egg*, SUN-SENTINEL.COM, Dec. 23, 2003.

[29] *See FTC Chair Tim Muris Hosts Ask the White House*, THE WHITE HOUSE, Dec. 16, 2003, *at* http://www.whitehouse.gov/ask/20031216.html; Baker, *supra* note 19, at 82.

[30] Andrew Leung, *Spam: The Current State*, TELUS CORPORATION, Aug. 8, 2003, at 6, *at* http://security.iia.net.au/downloads/spam%20leung%20paper.pdf. Most of these e-mail addresses are posted on websites, newsgroups, chat rooms, ICQ, message boards, etc.

[31] *Id.* at 6-7.

Most spammers employ different tactics to serve two purposes: to evade detection and to slip past spam filtering technology. First, to evade detection spammers exploit open relays and proxies on the Internet.[32] Using this technique, e-mail can be routed through ISPs in different countries. While it does not make it difficult for law enforcement to track the e-mail, it may make it difficult to regulate ISPs.[33] Another technique, known as "spoofing," is to appropriate a company or ISP's address and to send spam under the forged sender address.[34] In addition to forging the sender address, spammers will also forge return e-mail addresses and message headers[35] to evade detection.[36] Spammers also use psychological techniques, such as spoofing the recipient's own e-mail address.[37] Most of these spam tactics amount to fraud and are specifically addressed by CAN-SPAM.[38]

Once e-mail evades ISP filters, it usually reaches its target. Fewer than 10% of companies have effective spam-filtering technologies.[39] Furthermore, companies that do employ spam-filtering software find the technology ineffective because the software tends to over-block or under-block e-mail.[40] Spammers often try to simulate or mimic real e-mail messages.[41]

---

[32] *Id.* at 7. ("Basically, they commandeer Joe Average's PC to route spam through it to cloak their origin and avoid detection. An open relay is simply a mail server, which accepts and forwards messages regardless of their source and destination addresses. Investigators will trace the spam back to Joe, but not to the marketers.").
[33] *See How to Track Spammers*, SPAMABUSE.ORG, *at* http://www.spamabuse.org/content_HowtoTrackSpammers.htm (last visited Jan. 11, 2004).
[34] Baker, *supra* note 19, at 79.
[35] Headers are, in general computer science terms, a data packet storing information about a file. In e-mail terms, they usually store information about the e-mail and the routing information. *See Reading Email Headers*, STOPSPAM.ORG, *at* http://www.stopspam.org/email/headers.html (last visited Jan. 11, 2004); *See generally What Email Headers can Tell You About the Origin of Spam*, ABOUT.COM, *at* http://email.about.com/cs/spamgeneral/a/spam_headers.htm (last visited Jan. 11, 2004); *Understanding Email Headers*, SPAMABUSE.ORG, *at* http://www.spamabuse.org/content_UnderstandingEmailHeaders.htm (last visited Jan. 11, 2004).
[36] Leung, *supra* note 30, at 7.
[37] It has been shown that e-mail users are more likely to open an e-mail that comes from a sender with a similar name or from the recipient himself. *See How Can I Be Spamming Myself?*, WEBOPEDIA.COM, *at* http://www.webopedia.com/DidYouKnow/Internet/2003/SelfSentSpam.asp (last updated Dec. 10, 2003).
[38] *See* CAN-SPAM Act of 2003 §§ 5 & 6.
[39] La Monica, *supra* note 20.
[40] *See* Doug Isenberg, *Unexpected Twists in Internet Law*, CNET NEWS.COM, Dec. 23, 2003, *at* http://news.com.com/2010-1028-5131781.html?tag=nefd_acpro. The Pew study showed that 30% of e-mailers fear

Consequently, if spam software is not "intelligent," then it may block legitimate e-mail. In fact, computer security analysts predict that it will be nearly impossible to filter spam based on keywords because spammers are now filling their e-mails with "R.a..n,d,o.,m p,u,,n,c.t,,u_a.t.1..0.n."[42] At this level of reliability, spam-filtering can only be a piece of the puzzle in the fight against spam.

C. Who Are Spammers?

One would imagine that only a sophisticated spam ring[43] would be able to amass the technical knowledge to constantly adapt to ISPs' attempts to filter spam and bombard users' inboxes. While the majority of spam comes from well-known professional spammers,[44] the truth is that the cost to spam is near zero,[45] making it easy for anyone to become a part-time spammer.[46] People are drawn to the spam industry because anyone with a little technical know-how can become a spammer.[47] Furthermore, many marketers resort to this type of advertisement because the cost of spam is comparatively lower than junk mail or telemarketing.[48] According to

---

that filtering software may filter out important desired incoming e-mail, 13% of e-mail users say they know this has happened to them, and 23% say they fear their out-going e-mail may be blocked by the intended recipients' filtering software. Fallows, *supra* note 9, at 28.

[41] *See Virus Writers Turn to Spam*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/technology/3107613.stm (last updated July 30, 2003).

[42] Peter Gregory, *Security Predictions for 2004*, COMPUTERWORLD, Jan. 1, 2004, *at* http://www.computerworld.com.au/index.php?id=2057465071&fp=16&fpid=0.

[43] *See Microsoft, Spitzer Sue Alleged Spam Ring*, ABC NEWS, Dec. 18, 2003, *at* http://abcnews.go.com/wire/Business/ap20031218_1113.html.

[44] *The ROKSO List*, THE SPAMHAUS PROJECT, *at* http://www.spamhaus.org/rokso/index.lasso (last visited Jan. 11, 2004).

[45] Rotenberg, *supra* note 8.

[46] *See* Husted, *supra* note 14.

[47] *Id.* All that is required to get into the industry is an initial start-up cost of a few computers, spam software, a high-speed Internet connection, and either e-mail harvest software or e-mail addresses sold by other spammers. A high-speed Internet connection used by businesses or small ISPs can cost approximately $1000. Harvest software can cost approximately $50. A million addresses can cost anywhere from $19.95 to $25. *See id.*; Leung, *supra* note 30, at 6. However, a "compilation of e-mail addresses of those who have purchased items offered in spam – known as the 'suckers list' – costs more." Husted, *supra* note 14.

[48] Telemarketing and junk mail incur the costs of sending the message to the recipient; however, spam costs the same if the e-mail is sent to a million users or ten. Therefore, unlike junk mail and telemarketing, spam is not tailored towards a certain consumer group. *See FTC Chair Tim Muris, supra* note 29. Thus, a 60-year-old man is as likely to receive a penis-enhancement or Viagra-pill advertisement as a 10-year-old girl.

the Pew Study, 7% of email users have ordered a product or service from UCE, but spammers report they only need a 0.001% response rate to break even.[49]

Despite the ease of entry into the market, almost 90% of spam originates from 1 of 200 professional "spam gangs."[50] One lawyer in Virginia who has sued hundreds of spammers says these types of "big-time" spammers are "hackers gone bad, or crooks gone geek."[51] Indeed, regardless of how the law is written, CAN-SPAM will not be a deterrent to these criminals.

II. Is Spam Really a Big Problem?

Most marketers are not aware of the real social costs spam is imposing on the Internet community, the e-commerce industry, and even the advertising industry.[52] Experts estimate that companies lose anywhere between $10[53] to 87[54] billion a year to lost productivity,[55] investment in technology, and other resources to filter and handle the load of spam.

The burden on the Internet community and private, individual e-mail users is heavy. Marketers cleverly mask their spam as legitimate e-mails, forcing individuals to spend time opening and reading e-mail.[56] If spammers continue this trend, according to Nicholas Graham, a spokesman for America Online (AOL), there is a "very real threat that the e-mail function is

---

[49] Fallows, *supra* note 9, at 25 (The Pew study researchers suspect the 7% response rate includes legitimate products or services, unlike the typical fraudulent products found in spam. Their definition of spam was merely that it was "unsolicited" and did not take into account the relationship with the sender and the nature of the product.).
[50] *Rationale,* THE SPAMHAUS PROJECT, *at* http://www.spamhaus.org/sbl/sbl-rationale.html (last visited Jan. 11, 2004); *See also* Stefanie Olsen, *'Buffalo Spammer' Nabbed in New York*, CNET NEWS.COM, *at* http://news.com.com/2100-1032-1001513.html?tag=nl (last modified May 14, 2003); *Cyber Promotions Hosts Hate Site*, CNET News.com, *at* http://news.com.com/2100-1023-279208.html?legacy=cnet (last modified Apr. 24, 1997).
[51] Husted, *supra* note 14.
[52] *See* CAN-SPAM Act of 2003 § 2(a)(4).
[53] *See* Anita Ramasastry, *Why the New Federal 'Can Spam' Law Probably Won't Work*, CNN, Dec. 5, 2003, *at* http://www.cnn.com/2003/LAW/12/05/findlaw.analysis.ramasastry.spam/index.html; *See also* Husted, *supra* note 14.
[54] *See* Fallows, *supra* note 9, at 7.
[55] *Comprehensive Spam Survey*, UNSPAM, Oct. 2003, *at* http://www.unspam.com/fight_spam/information/survey_oct2003.html (45% of American workers say they would be more productive if they received less spam).
[56] *See* Fallows, *supra* note 9, at 11 (For example, 47% of e-mailers say spam is hard to tell and 9% have to open their e-mail to see if it is spam.). Approximately 55% of users say it is hard for them to get to messages they want to read. *Id.* at iii.

going to rot before our very eyes."[57] Already, 25% of e-mail users say that the volume of spam has caused them to reduce their overall use of e-mail.[58] Furthermore, when spammers hack users' e-mail accounts, the users typically receive so many replies flooding their inboxes that they have to close their account completely.[59]

Spam also has a significant impact on the e-commerce and advertising industries. The problem is largely related to the fraudulent aspect of spam.[60] When a spammer spoofs a company's domain name it can disrupt the business because the company will receive an influx of e-mails consisting of returned e-mails, irate e-mails, and virus e-mails.[61] More importantly someone will have to sift through all the e-mails to find legitimate e-mails from customers.[62]

While not an infant industry, e-commerce is still relatively young[63] and far from replacing the brick and mortar method of retail. In fact, only recently has the moratorium on Internet taxes expired,[64] and Congress is debating whether to extend the moratorium,[65] signifying that Internet commerce is still in its developing stages. It is crucial for consumers to be able to trust the websites and companies from which they order goods. Spam is starting to create distrust in consumers of the young and fragile e-commerce industry. For instance, "phishing"

---

[57] Husted, *supra* note 14.
[58] Fallows, *supra* note 9, at i.
[59] *See id.* at 12.
[60] The other aspect of spam is advertising. As stated earlier, the underlying characteristic of all spam is that it is "unsolicited." However, among spam there are many different genres and different types of spammers. The thieves send fraudulent spam and scams, the marketers send commercial and advertising spam, and then there are pornography operators. The list is endless, but spam can be further characterized as either fraudulent or non-fraudulent. This is explained in greater detail below.
[61] *See* Fallows, *supra* note 9, at 12.
[62] *See id.*
[63] Amazon.com and ebay.com, two of the larger and well-known brands in e-commerce, are both only 8 years old. *See AMZN investor relations: FAQ*, AMAZON.COM, *at* http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-faq (last visited Jan. 11, 2004); *Ebay: Company Overview*, EBAY.COM, *at* http://pages.ebay.com/community/aboutebay/overview/index.html (last visited Jan. 11, 2004).
[64] The Internet Tax Freedom Act, a moratorium on Internet taxation, expired on November 1, 2003. *See* Isenberg, *supra* note 40.
[65] Declan McCullagh, *Ban on Net Tax Dead Till 2004*, CNET NEWS.COM, *at* http://news.com.com/2100-1028-5112140.html (last modified Nov. 26, 2003).

can create distrust among Internet shoppers, and this especially hurts smaller startups that have yet to create a trusted brand.[66] Small businesses, startups, and advertising companies that try to market products through spam may not get a second glance or may be filtered due to the growing distrust of unsolicited e-mail, even though 16.5% of spam is from legitimate advertisers peddling legitimate products.[67] If spam persists only the brand names will survive, and the no-names will be denied the brick-and-mortar equivalent of coveted "shelf-space."

Spam is an almost uncontrollable problem for ISPs because if spam is not filtered it may disrupt individual users' accounts.[68] Furthermore, if a spammer decides to use a particular ISP which has a weak spam filter or does not have resources to fight spam, then that ISP is at risk of being blacklisted and its e-mails rejected from the rest of the Internet community.[69] Larger ISPs such as AOL or Earthlink, however, are at less risk of being blocked than their smaller rivals.[70] ISPs may also face a legal dilemma in protecting its customers. Existing technology is not sophisticated enough to differentiate legitimate e-mail from spam. Consequently, ISPs could risk litigation on grounds of invasion of privacy, censorship, or freedom of speech and expression for filtering legitimate e-mails.

---

[66] *See* Baker, *supra* note 19, at 79.
[67] Ramasastry, *supra* note 53. *See also* Baker, *supra* note 19, at 79 (A case in point is Brava LLC which sent out 20,000 e-mails pitching a product. There was 1 response, but in spam terms this is an excellent and profitable response rate considering the amount of spam that was actually sent.); Declan McCullagh, *Direct Marketers Want Anti-Spam Laws*, CNET News.com, *at* http://news.com.com/2100-1023-962821.html?tag=nl (last modified Oct. 21, 2002) (The advertising industry, which used to be opposed to anti-spam laws changed their position when they realized the impact that spam was having on the effectiveness of e-mail as an advertising medium. E-mail users were not taking a look at e-mail as long as it was commercial.).
[68] *See* Fallows, *supra* note 9, at 12.
[69] *See Internet Service Providers*, THE SPAMHAUS PROJECT, *at* http://www.spamhaus.org/sbl/isp.lasso (last visited Jan. 11, 2004).
[70] *See* Baker, *supra* note 19, at 79.

As if the spam industry itself was not devastating enough to commerce,[71] virus writers and spammers are starting to employ each others' techniques.[72] Virus writers employ fake subject headers to entice users to open the e-mail.[73] To see how the two work together, one can look at the most recent SoBig virus, occurring in August 2003 and estimated to set the new record in damages to industry.[74] The SoBig virus operated by raiding e-mail directories and sending spam messages to victims' contacts.[75] This year, other viruses, such as the Beagle virus, are proliferating through spam.[76] Virus writers resort to spam tactics because e-mail filters and scanners look for viruses, so instead, virus writers insert hyperlinks in the e-mail that download the virus from a website.[77]

Spam is also problematic because the sexual content of spam can be offensive to e-mail users.[78] One of the motivations behind CAN-SPAM was to protect children from pornography.[79] Many women[80] and children[81] are already connected to the Internet, and the numbers are

---

[71] *See* James Middleton, *Major Viruses Cost Industry $13bn in 2001*, PERSONAL COMPUTER WORLD, Jan. 10, 2002, *at* http://www.pcw.co.uk/News/1128147 (In 2001, major viruses cost industry over $13 billion.); Deborah Ghose, *Computer Viruses, Worms, and Insurance*, ABOUT.COM, *at* http://insurance.about.com/cs/lines/a/virusesandworms.htm (last visited Jan. 11, 2004) (The Code Red worm, which struck in 2001, is said to have cost a world record $2 billion.).

[72] This seems to make sense as they both use the same medium, namely e-mail.

[73] Middleton, *supra* note 71.

[74] *See* Ghose, *supra* note 71.

[75] Baker, *supra* note 19, at 82 ("This undermined the popular 'white list' defense, which limits entry to approved e-mailers"). The "white list" defense will be discussed in the alternative solutions section, *infra* note 224.

[76] *Spammers Launch Scavenging Virus*, CNN, Jan. 19, 2004 (on file with author).

[77] *Virus Writers Turn to Spam*, *supra* note 41.

[78] Pornography is degrading to women, and not surprisingly women are bothered by obscene or pornographic spam. *See* Fallows, *supra* note 9, at 29.

[79] *See* Press Release, Office of the Press Secretary, Fact Sheet: President Bush Signs Anti-Spam Law (Dec. 16, 2003), *at* http://www.whitehouse.gov/news/releases/2003/12/print/20031216-4.html.

[80] Already, women represent 52% of Internet users in the US. Robyn Greenspan, *Europe, U.S. on Different Sides of the Gender Divide*, CYBERATLAS, Oct. 21, 2003, *at* http://cyberatlas.internet.com/big_picture/demographics/article/0,,5901_3095681,00.html.

[81] A Nielsen/NetRatings survey showed that 2-in-10 Internet users in 2003 were children between the ages of 2 and 17. *2-in-10 Are Connected Kids*, CYBERATLAS, *at* http://cyberatlas.internet.com/big_picture/demographics/article/0,,5901_3110071,00.html (last visited Jan. 11, 2004).

expected to rise for these demographics over the next few years.[82] Pornographic spam is often cited by parents to be the worst type of spam.[83] Spam makes pornographic content even more accessible[84] and offensive, as the content is often visually forced upon an unsuspecting e-mail user.[85]

III. CAN-SPAM: Better Than Having No Law At All?

The U.S. declared the war on spam long ago. Thirty-seven states already have anti-spam laws in effect.[86] CAN-SPAM is criticized for being less effective and less stringent than state laws. However, CAN-SPAM has many similarities to many of the state laws and in some ways is stricter than some international laws. In addition, having a federal law is advantageous because it will protect the residents of the 13 other states that currently do not have an anti-spam law in place.

A federal law also would not face the same constitutional challenges to which state spam laws are vulnerable. Already two state laws, California and Washington, have been challenged on grounds that they violated the Dormant Commerce Clause under the theory that they placed an undue burden on interstate commerce.[87] Though in both cases the statutes were found unconstitutional by state courts,[88] they were both reinstated in their respective states' appeals

---

[82] *See Internet Demographics & Trends*, COMPUTER ECONOMICS, *at* http://www.computereconomics.com/page.cfm?name=Internet%20Demographics%20%26%20Trends (last visited Jan. 11, 2004).
[83] *See* Fallows, *supra* note 9, at 29.
[84] Already, 18% of spam consists of pornography. David Ho, *Most Spam E-mail Messages Are Deceptive, FTC Contends*, THE MERCURY NEWS, *at* http://www.bayarea.com/mld/mercurynews/business/5750233.htm (posted on Apr. 30, 2003).
[85] Seventeen percent of adult content contains automatically downloaded images. Fallows, *supra* note 9, at 31.
[86] Olsen, *supra* note 7.
[87] *See* Sorkin, *supra* note 21, at 383; John Magee, *The Law Regulating Unsolicited Commerce E-Mail: An International Perspective*, 19 Santa Clara Computer & High Tech. L.J. 333, 361-62 (2003).
[88] *See* Magee, *supra* note 87, at 361.

courts.[89] Nevertheless, other state spam laws have faced similar challenges.[90] With the passage of CAN-SPAM this is no longer a concern.

Critics have declared that spammers will simply ignore the laws. FTC Chairman Muris has stated that he believes spammers would ignore a Do-Not-Spam registry.[91] Steve Linford, founder of The Spamhaus Project,[92] believes that the "problem with these [anti-spam] laws is that they are geared to spammers being honest and respecting laws … Of course there are no honest spammers – the whole profession is based on deceit."[93] However, spammers' willful disobedience of the law does not necessarily mean that a federal law, such as CAN-SPAM, would not solve many jurisdictional and constitutional problems as well as the difficulty in international cooperation posed by state spam laws.

Another commonly voiced criticism is that CAN-SPAM essentially gives spammers the right to spam e-mail users. Critics worry that if each of the 22.9 million small businesses in the country decides to send non-fraudulent spam, then we could see a short-term rise in spam as well as a loss in productivity while e-mail users take the time to opt-out.[94] However, before CAN-SPAM, many businesses could have advertised through spam without fear of legal retribution. These businesses did not spam before CAN-SPAM and most likely will not after it is effective

---

[89] *See id.*; Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 155 Cal. Rptr. 2d 258 (Cal. App. 1st Dist. 2002); State v. Heckel, 24 P.3d 404 (Wash. 2001).
[90] *See* Sorkin, *supra* note 21, at 383 n.280 ("The Louisiana spam law has also been challenged, although the case was dismissed on procedural grounds.").
[91] Ramasastry, *supra* note 53.
[92] The Spamhaus Project keeps lists and databases of notorious spam gangs in a Register of Known Spam Operations (ROKSO), a Spamhaus Block List (SBL) of IP addresses used to send spam, and a list of ISPs that do not filter for spam. Their website, http://www.spamhause.org, contains news and general information about spam.
[93] *New Laws on Spam Come Into Force*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/technology/3308989.stm (last updated Dec. 11, 2003).
[94] McCullagh, *supra* note 2.

because "few legitimate businesses, if any, engage in bulk email marketing for fear of offending potential customers."[95]

Instead, legitimate businesses try to entice e-mail users to allow them access to their inbox through promotions or gifts.[96] For example, US Airways gives 1,000 frequent-flier miles to passengers who sign up for their newsletter,[97] and companies that want to advertise through e-mail can become affiliated with Opt-In Marketing Databases.[98] Eventually, to resurrect e-mail as an effective method of marketing, companies will have to give e-mail users incentive to read e-mail advertisements.

Despite the various methods of categorizing spam, the stated purpose of CAN-SPAM is to regulate commercial electronic mail.[99] One way to approach spam is to divide it into two types: fraudulent and non-fraudulent. To put it in the policy perspective, non-fraudulent, which can be controlled by laws, and fraudulent, which will require more progressive and encompassing measures than statutes can provide. While CAN-SPAM allows legitimate commercial e-mail, it also delineates the methods by which legitimate e-mail can be sent, thus allowing any "good" spam software to be able to filter it out. Spam filters are ineffective against fraudulent spam. As the Australian government recognized when enacting their spam bill, legislation combating spam should be a part of a "multi-layered" approach and is meant to complement the use of technology.[100]

---

[95] *FTC Names Its Dirty Dozen, supra* note 28.
[96] Baker, *supra* note 19, at 79.
[97] *Id.*
[98] One Opt-In Marketing Database is MyPoints which has been operating since 1997. The MyPoints model allows e-mail users to choose to receive "spam," and they earn points for clicking on links to commercial websites for which the points can be redeemed for gift certificates. For general information about MyPoints, visit their website at http://www.mypoints.com.
[99] CAN-SPAM Act of 2003 § 2(b)(1). Another opt-in marketing company is OptInRealBig.com whose website is http://www.optinbig.com/.
[100] James Pearce, *Australian Antispam Legislation Tabled in Parliament*, ZDNET AUSTRALIA, Sept. 18, 2003, *at* http://www.zdnet.com.au/newstech/ebusiness/story/0,2000048590,20278732,00.htm.

Ultimately, anti-spam legislation should serve two purposes: to penalize fraudulent spam and to promote commerce by protecting non-fraudulent commercial e-mail. Legitimate marketers and businesses have a right to be put on notice about the jurisdiction and laws regarding the methods they may put to use to stimulate their business. We should not ask businesses to stop sending advertising through e-mail. Rather, we should find a balance so that businesses treat e-mail as a means to reach potential consumers.

Therefore, the real question is, how effective will CAN-SPAM be against fraudulent e-mail? One way to measure CAN-SPAM's potential effectiveness is to analyze each major provision and compare that to similar provisions of state laws.

A. Targeting Spam Tactics

CAN-SPAM aims to regulate spam by ensuring that commercial e-mail is not misleading or fraudulent.[101] Most anti-spam laws prohibit fraudulent content, as that is the primary method that spammers use to infiltrate an e-mail user's inbox. CAN-SPAM only prohibits fraudulent commercial e-mail that contains false header information[102] and deceptive subject headings.[103] Half of state anti-spam laws also have this requirement.[104] CAN-SPAM also amends the crimes and criminal procedure code to preclude interstate or international spam.[105] It is a violation under CAN-SPAM to send commercial e-mail to an address obtained through address harvesting

---

[101] CAN-SPAM Act of 2003 § 2(b)(2).

[102] *Id.* § 5(a)(1) ("PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION.--It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading.").

[103] *Id.* § 5(a)(2) ("PROHIBITION OF DECEPTIVE SUBJECT HEADINGS.--It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).").

[104] Vanessa A. Nelson, *Use of UCE: State Laws Regarding Unsolicited Commercial Electronic Mail Advertisements*, 58 Bus. Law. 1203, 1204 (2003).

[105] *See* CAN-SPAM Act of 2003 § 4. The Act amends Chapter 47 of title 18, which is the Fraud and False Statements section of Crimes and Criminal Procedure.

and dictionary attacks.[106] CAN-SPAM also prohibits spammers to take control of other computers or routing the spam through open relays.[107] To combat this, the FTC recently launched a campaign called "Operation Secure Your Server," encouraging system operators to configure their computers to prevent routing of spam.[108]

B. Opt-out vs. Opt-in

Anti-spam legislation generally has either an opt-out or an opt-in mechanism. The opt-out model allows a spammer to send e-mail until the e-mail user indicates he does not wish to receive further e-mails from that particular spammer. The opt-in model requires that the spammer receive prior consent from the e-mail user before the spammer may assail the user with e-mail. In effect, the spam stops being "unsolicited." Currently most spam e-mail does not have an effective opt-out mechanism. Often e-mail users do not use an opt-out mechanism if provided because the request is often ignored, and users fear that it would only confirm that the e-mail address is active.[109]

---

[106] *Id.* § 5(b)(1) ("(1) Address harvesting and dictionary attacks--
(A) IN GENERAL.--It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that--
(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or
(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.").
Id. § 5(b)(1)(A)(i) would be "harvesting" and *id.* § 5(b)(1)(A)(ii) would be dictionary attacks. It is also important to note that a violation of the provision requires that an e-mail be sent from a harvested address. Hence, this general provision would not prevent automated "web crawling," the technique used by search engines to gather Universal Resource Locators (URL) and index the Internet.

[107] *See id.* § 5(b)(3).

[108] *FTC Launches 'Operation Secure Your Server'*, CNN, Jan. 30, 2004, *available at* http://www.cnn.com/2004/TECH/internet/01/30/ftc.spam.ap/index.html; Letter from the Federal Trade Commission, to Administrator of Open Relay Mail Server (Jan. 29, 2004); *FTC and International Agencies Announce "Operation Secure Your Server"*, Federal Trade Commission, Jan. 29, 2004, *available at* http://www.ftc.gov/opa/2004/01/opsecure.htm.

[109] *See* Fallows, *supra* note 9, at 24.

CAN-SPAM requires a "clear and conspicuous" opt-out mechanism.[110] At least thirteen states offer similar opt-out mechanisms.[111] To facilitate with the opt-out mechanism, CAN-SPAM requires that spam e-mails contain a valid and functioning return address.[112] CAN-SPAM allows additional opt-out mechanisms such as menus to allow recipients to choose between different types of spam they may wish to receive or opt-out.[113] The opt-out mechanism has been criticized by the National Association of Attorneys General (NAAG) as a potential way of allowing spammers to confuse consumers.[114] However, it is important here to distinguish between the fraudulent and non-fraudulent e-mail. Confusing opt-out mechanisms, as noted by CAN-SPAM's co-authors, are not the primary tools of the spam trade.[115] If a particular spam e-mail were to hide the opt-out mechanism in text or to create confusing menus, one could surmise that the e-mail was from an illegitimate business and could most likely be prosecuted on other grounds in CAN-SPAM, such as fraudulent header information or subject lines. On the other hand, the opt-out mechanism can be viewed as a way for legitimate businesses to tailor e-mails to potential customers. Advertising companies would want comply with opt-out mechanisms if they hope that e-mail can once again become an effective advertising medium.

Under CAN-SPAM, once the e-mail user makes a request to opt-out, the spammer has 10 business days to comply with the opt-out request.[116] Many experts would agree that this is an ineffective time period. According to some reports, AOL and Microsoft each block 2.4 billion

---

[110] *See* CAN-SPAM Act of 2003 § 5(a)(5)(ii).
[111] *See* Nelson, *supra* note 104, at 1204-05.
[112] CAN-SPAM Act of 2003 § 5(a)(3)(A).
[113] *Id.* § 5(a)(3)(B).
[114] *See* Letter from Internet Committee of the National Association of Attorneys General, to Representatives and House Energy and Commerce Committee, (Nov. 4, 2003), *available at* http://www.epic.org/privacy/junk_mail/spam/agltrs877.pdf.
[115] Ron Wyden & Conrad Burns, *Why We've Finally Canned Spam*, CNET NEWS.COM, Dec. 16, 2003, *at* http://news.com.com/2010-1028-5125699.html?tag=nl.
[116] CAN-SPAM Act of 2003 § 5(a)(4)(A)(i).

spam e-mails daily.[117] If spammers were allowed to legally continue this for the next 10 days, one can imagine the heavy burden that e-mail users would incur by spam that was transmitted legally. However, CAN-SPAM remedies this concern by providing the FTC with supplementary rulemaking authority to reduce the compliance time period.[118]

In the ultimate form of opting out, CAN-SPAM authorizes, but does not require, the FTC to establish a national Do-Not-E-Mail registry, similar to the Do-Not-Call registry already established by the FTC.[119] The public supports a national Do-Not-E-Mail registry,[120] and some believe that the registry is CAN-SPAM's "key to success." It also solves some Fourteenth Amendment Due Process and Dormant Commerce Clause issues.[121] As explained by a U.S. consultancy company, Unspam:

> An email address does not reveal its user's jurisdiction and thus does not put a sender on notice of what laws apply when sending mail to that jurisdiction. In the United States that creates a 14th Amendment/Due Process concern because a sender has not "purposely availed" themselves [sic] of the recipient's jurisdiction, but the problem appears in every modern democracy. The benefit of a no-spam

---

[117] *Spam Numbers & Statistics*, UNSPAM, *at* http://www.unspam.com/fight_spam/information/spamstats.html?ses=ylqQE-EsVVFqz15q-LcaFjauk_vzKd6l5LAbKjlA (last visited Jan. 12, 2004).

[118] CAN-SPAM Act of 2003 § 5(c)(1) ("SUPPLEMENTARY RULEMAKING AUTHORITY.--The Commission shall by regulation, pursuant to section 13--
(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable").

[119] *Id.* § 9(b) ("AUTHORIZATION TO IMPLEMENT.--The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act."); *See National Do Not Call Registry*, Federal Trade Commission, *at* https://www.donotcall.gov/FAQ/FAQDefault.aspx (last visited Jan. 18, 2004); *See also FTC Chair Tim Muris, supra* note 29.

[120] *See Comprehensive Spam Survey*, *supra* note 55 (A national Do-Not-E-Mail registry has the support of 3 out of 4 Americans according to a survey conducted in October of 2003); Joseph Lee, *Will an Anti-Spam List Work?*, CNN, Oct. 23, 2003, *at* http://money.cnn.com/2003/10/23/technology/spam_bill/index.htm (Matthew Prince, co-founder of Unspam, an anti-spam consulting firm, believes that a Do-Not-Spam registry is "long overdue.").

[121] Patrick Gray, *U.S. Senate Moves to Can Spam*, ZDNET AUSTRALIA, Oct. 24, 2003, *at* http://www.zdnet.com.au/newstech/security/story/0,2000048600,20280112,00.htm.

registry is that it can tie an email address to a particular jurisdiction and solve this problem.[122]

The greatest danger for the Do-Not-Spam registry is that spammers will ignore it[123] since, as stated earlier, 90% of spam comes from spam gangs who generally ignore the law. For spammers who would violate CAN-SPAM, the list would provide e-mail addresses that spammers know are valid and are most likely users' primary e-mail addresses. In addition, Do-Not-Call and Do-Not-E-Mail have different costs to implement, as it is much easier for spammers to hide behind a false e-mail address than it is for telemarketers to mask their phone number. Nevertheless, legitimate marketers have a right to be put on notice with regard to the laws and jurisdiction that govern the e-mails. Spam should be regulated by a federal law "because it's at the very least a national marketplace."[124] These are factors that the FTC will have to consider if it decides to establish the registry.

C. Enforcement

Unlike most state laws regulating unsolicited commercial e-mail, which provide a private right of action for damages,[125] CAN-SPAM will be enforced primarily by the FTC,[126] and civil actions brought by State attorney generals[127] or ISPs.[128] However, States are required to give the FTC notice prior to any action, at which time the FTC may intervene if it chooses.[129] State laws provide broader rights to ISPs. Almost a third of state laws allow ISPs to prohibit spam

---

[122] *Spam News Ticker: US Anti-Spam Registry Approach May Solve Jurisdictional Problems Worldwide*, UNSPAM, Oct. 24, 2003, *at* http://www.unspam.com/fight_spam/articles/1150.html.
[123] Elizabeth Dunbar, *E-mail Tax May Help Stop Spam, Dayton Says*, STAR TRIBUNE, Nov. 19, 2003.
[124] McCullagh, *supra* note 2.
[125] Nelson, *supra* note 104, at 1212.
[126] CAN-SPAM Act of 2003 § 7(a).
[127] *Id.* § 7(f).
[128] *Id.* § 7(g).
[129] *Id.* § 7(f)(5).

according to their own policies, granting ISPs great power over defining and controlling spam that passes through their networks.[130]

1. State, ISP, and Private Rights of Action

Critics are discontented with the exclusion of a private right of action[131] that is allowed in many state laws and other proposed federal laws.[132] However, for now, private actions would tie up the system, and furthermore they do not have the same impact that ISPs or state attorney generals would have on the spam community. As the co-authors of CAN-SPAM[133] have noted, "it will be important for enforcement authorities to bring a few high-profile cases shortly after the bill is enacted. That will send a clear message to the kingpin spammers that the game has changed."[134] Furthermore, ISPs and states have already been independently and cooperatively aggressively suing and prosecuting spammers.[135] Some ISPs have achieved a measure of success; for example, AOL won a $7 million judgment against a spam company last December.[136] In the future, Congress should consider allowing a private right of action. However, at this nascent stage of the federal anti-spam system, it may be best to have ISPs and states remain proactive, expending the resources that private citizens would not have, to flush out any loopholes and prevent adverse legal precedents that spammers may exploit or pursue in litigation.

---

[130] Nelson, *supra* note 104, at 1205.
[131] *See* Rotenberg, *supra* note 8.
[132] McCullagh, *supra* note 2.
[133] CAN-SPAM was co-authored by Senators Ron Wyden (D-Ore.) and Conrad Burns (R-Mont.).
[134] Wyden, *supra* note 115. In fact, Wyden and Burns also wrote a letter to Chairman Muris requesting that he bring high-profile cases against "kingpin" spammers. *See* Letter from Senator Conrad Burns and Senator Ron Wyden, to Timothy Muris, Chairman, Federal Trade Commission (Dec. 11, 2003), *available at* http://wyden.senate.gov/leg_issues/letters/12112003_ftcspam.html.
[135] *See* Brad Wright, *Virginia Indicts Two on Spam Felony Charges*, CNN, Dec. 12, 2003, *at* http://www.cnn.com/2003/TECH/internet/12/12/spam.charges/index.html; *Microsoft, Spitzer Sue, supra* note 43; Marguerite Reardon, *Microsoft, New York Launch Spam Lawsuits*, CNET NEWS.COM, *at* http://news.com.com/2100-1028_3-5128806.html?tag=nefd_top (last modified Dec. 18, 2003).
[136] *Half of All E-mails Are Spam*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/technology/2950408.stm (last updated May 31, 2003).

Without a private right of action, some spam experts, such as Ray Everett-Church of ePrivacyGroup,[137] believe that the scarcity of state attorney generals and FTC enforcement will not prove to be enough of a threat to deter spammers.[138] Nevertheless, while there is a lack of personnel policing the law, the potential amount of damages and possibility of imprisonment should prove to be a deterrent to most potential spammers. Wyden and Burns hope that a few high-profile cases will deter spammers.[139] Already, four of the biggest e-mail providers – Microsoft, AOL, Earthlink and Yahoo – are filing lawsuits under CAN-SPAM against six of the most prolific spam operations.[140]

Moreover, the FTC and ISPs should take a lesson from the Recording Association of America (RIAA). Their first wave of lawsuits created a lot of publicity. According to Nielsen/NetRatings, there was a direct correlation between the announcing of the lawsuits and a drop in the amount of file-swapping.[141] Like the RIAA, the FTC should be able to settle with most individual spammers. For those cases that are brought to trial, the FTC can recoup the costs in accordance with CAN-SPAM.[142] The lawsuits should prove enough to deter large-scale

---

[137] ePrivacyGroup is a technology company that frequently advises companies and government agencies on spam. Their website is http://www.eprivacygroup.com.
[138] McCullagh, *supra* note 2.
[139] *See* Wyden, *supra* note 115.
[140] Michelle Delio, E-mail Providers Slam Spammers, WIRED, Mar. 10, 2004, *available at* http://www.wired.com/news/business/0,1367,62606,00.html?tw=wn_story_top5.
[141] John Borland, *RIAA Files 80 New File-Swapping Suits*, CNET NEWS.COM, *at* http://news.com.com/2100-1027_3-5099738.html (last modified Oct. 30, 2003). The RIAA has been extremely aggressive, using a shotgun approach to file lawsuits. They've even gone as far as suing 12 year old girls, 60 year old grandmothers, and have sued people who did not even share files on their computer. *See* John Borland, *RIAA Settles With 12-year-old Girl*, CNET NEWS.COM, *at* http://news.com.com/2100-1027-5073717.html?tag=nl (last modified Sept. 9, 2003). The effects of the lawsuits on filesharing have been confirmed by a PEW study. Lee Rainie et al., PEW INTERNET & AMERICAN LIFE PROJECT & COMSCORE MEDIA METRIX, Jan. 4, 2004, *The Impact of Recording Industry Suits Against Music File Swappers*, *at* http://www.pewinternet.org/pdfs/PIP_File_Swapping_Memo_0104.pdf; *But, see* Marguerite Reardon, *Oops! They're Swapping Again,* CNET News.com, *at* http://news.com.com/2100-1027_3-5142382.html?tag=nefd_top (last modified Jan. 16, 2004) (On the other hand, recent research shows an upturn in peer-to-peer usage since the lawsuits.); *See More Song Swappers Sued*, CNN, Jan. 21, 2004, *at* http://money.cnn.com/2004/01/21/technology/riaa_suits/index.htm?cnn=yes (Possibly due to the resurgence of file-sharing, the RIAA stepped up its attack and sued another 532 file swappers.).
[142] CAN-SPAM Act of 2003 § 7(f)(4).

spammers, and it should also curb small-time spammers from entering the spam industry, which, until CAN-SPAM, had low-financial and low-risk entry barriers.

2. Bounty System

Although individuals may not have a private right of action, the FTC is currently studying the feasibility of allowing bounty hunters to track down fraudulent spammers.[143] U.S. Rep. Zoe Lofgren (D-Calif.), who authored an alternative federal anti-spam legislation,[144] pushed to include the provision in CAN-SPAM.[145] The bounty idea was devised by Stanford Law Professor Lawrence Lessig,[146] who is so confident that it will substantially reduce spam that he has bet his job that it will work.[147] Others are cautiously optimistic, such as John Palfrey, executive director of the Berkman Center for Internet & Society at Harvard University's law school, who believes that a bounty system is a "promising approach" to catching spammers.[148] One indication of the effectiveness of a bounty system may be Microsoft's establishment of a $5

---

[143] *Id.* § 11 ("The Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce--
(1) a report, within 9 months after the date of enactment of this Act, that sets forth a system for rewarding those who supply information about violations of this Act, including--
(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that--
(i) identifies the person in violation of this Act; and
(ii) supplies information that leads to the successful collection of a civil penalty by the Commission"); *See generally* Marilyn Geewax, *Feds May Turn to Bounty Hunters to Catch Spammers*, Dayton Daily News, Dec. 13, 2003.
[144] REDUCE Spam Act of 2003 (H.R. 1933), *available at* http://www.spamlaws.com/federal/108hr1933.html.
[145] Tim Lemke, *Spam Law Allows Bounty Hunts*, THE WASHINGTON TIMES, Dec. 22, 2003, *at* http://washingtontimes.com/business/20031221-100042-1315r.htm.
[146] Professor Lessig has worked with Rep. Lofgren on her proposed legislation. *See generally* Lawrence Lessig, *Code Breaking: A Bounty on Spammers*, CIO INSIGHT, Sept. 16, 2002, *at* http://www.cioinsight.com/article2/0,1397,1454839,00.asp; Michael Bazeley, *New Weapon for Spam: Bounty,* MERCURY NEWS, Apr. 26, 2003, *at* http://www.mercurynews.com/mld/mercurynews/business/5722718.htm. Professor Lessig frequently writes about the spam topic on his weblog. *See* Stanford Law School: Lawrence Lessig, Apr. 2003, *at* http://www.lessig.org/archives/2003_04.shtml (last visited Jan. 18, 2004).
[147] Declan McCullagh, *A Modest Proposal to End Spam*, CNET NEWS.COM, Apr. 28, 2003, *at* http://news.com.com/2010-1071-998513.html (The wager would be judged by Declan McCullagh, Chief political correspondent of CNET News.com, and he would deem the law to fail if it does not "substantially reduce the level of spam.").
[148] Geewax, *supra* note 143.

million fund to pay for tips for the eventual capture of virus writers[149] and SCO Group's $250,000 reward for information leading to the arrest and conviction of the author of the MyDoom virus.[150]

While the FTC is commissioned to study the possibility, some FTC attorneys already recognize that locating spammers is difficult without subpoena power.[151] Others believe a bounty system would be counterproductive. For example, the FTC may spend more resources on maintaining the bounty system and settling disputes over rewards.[152] Spam analysts believe that a bounty could lead to false leads and doubt that few individuals have the necessary expertise to identify and locate spammers.[153] Others believe that a bounty is unnecessary because spam is unpopular enough that an incentive is not needed.[154] Furthermore, many ISPs already spend significant resources tracking down spammers.[155] A bounty system would also not have the deterrent power like that of a private right of action.[156] However, much like a private right of action, it may be best to wait to see the impact of federal anti-spam legislation before implementing alternative measures.

3. Federal vs. State Law

One area of controversy is that CAN-SPAM preempts any state law regulating commercial e-mail.[157] Critics charge that having a federal law is advantageous but urge that it should complement rather than preempt stronger state laws.[158] In a letter to Congress, the

---

[149] Reuters, *Despite Bounties, No Virus Arrests Yet* (Feb. 24, 2004).
[150] Andrew Stein, *Microsoft Offers MyDoom Reward*, CNN/Money, Jan. 30, 2004, *at* http://money.cnn.com/2004/01/28/technology/mydoom_costs/index.htm.
[151] Geewax, *supra* note 143.
[152] *Id.*
[153] Lemke, *supra* note 145.
[154] *Id.*
[155] Geewax, *supra* note 143.
[156] Lemke, *supra* note 145.
[157] CAN-SPAM Act of 2003 § 8(b).
[158] *See* Letter from Internet Committee, *supra* note 114.

Internet Committee of NAAG stated its disapproval of CAN-SPAM, citing a list of loopholes and barriers to enforcing the law.[159] However, states such as Minnesota, California, Missouri, and Tennessee, most likely anticipating the eventual enactment of a federal law, explicitly state that their laws would be superseded by federal law or inoperative once a federal law is enacted.[160]

Despite the criticism from the state and federal officials tasked to enforce CAN-SPAM, many in the technology industry support the law, such as ISPs like AOL.[161] In fact, AOL recently had a lawsuit dismissed in Virginia for lack of jurisdiction over Florida-based defendants, even though the spam was directed to AOL's servers.[162] Professor Sorkin, one of the foremost authorities on spam laws, has stated that "it doesn't make sense to regulate a relatively borderless environment with laws that vary according to geography."[163] Spam travels between states causing jurisdictional concerns and causing difficulty in coordinating enforcement measures.[164] CAN-SPAM centralizes the coordination effort under the FTC. While some state laws may be tougher, a fair amount of spam is generated outside the US, making it difficult for states to enforce the law without international cooperation.[165] Having a federal law unify the regulation of spam is a first step to the eventual and necessary unification of spam regulation on the international level.

D. Third Party Liability

---

[159] *See id.*
[160] *See* Nelson, *supra* note 104, at 1213-14; Cal. Bus. & Prof. Code § 17538.4(i) (West Supp. 2003).
[161] *See Anti-Spam Law Near, supra* note 6.
[162] Reuters, *AOL Antispam Suit Dismissed, but Company May Refile* (Dec. 31, 2003), *available at* http://news.com.com/2100-1032_3-5134306.html?tag=st_lh.
[163] Paul Festa, *A Cybersage Speaks His Mind*, CNET NEWS.COM, Sept. 19, 2002, *at* http://news.com.com/2008-1082-958576.html?tag=nl. Sorkin maintains the frequently cited website http://www.spamlaws.com, which contains up-to-date spam laws in the US and the rest of the world.
[164] Rotenberg, *supra* note 8.
[165] *See* La Monica, *supra* note 20. Most state laws provide for long-arm jurisdiction as long as the spam recipients are located in the state. Therefore, regardless of where the spam originates, a state would have legal jurisdiction. However, the difficulty of enforcing spam is locating the spammer. This would require international cooperation that would be more easily facilitated by the federal government.

CAN-SPAM holds not only the spammer liable but also third parties that request the services of the spammer.[166] However, a violation occurs only if the seller, who hires the spammer, knows or should have known, that the seller's goods were being promoted through fraudulent e-mail.[167] FTC chairman Tim Muris charges that the standard of intent requires "proof of both the seller's and spammer's level of knowledge…These requirements to prove intent pose a serious hurdle that we do not have to meet to obtain an injunction under our current jurisdiction."[168] However, CAN-SPAM only preempts laws specific to electronic mail, and as most spammers are involved in related criminal acts, actions can still be brought under existing state laws.[169] In fact, Chairman Muris has already indicated his intention to prosecute spammers with pre-existing laws even after CAN-SPAM is effective.[170]

E. Damages

CAN-SPAM as well as many of the state and international laws vary widely on the types of civil and criminal penalties. However, generally a court can award general damages of up to $2 million for State actions[171] and $1 million for actions brought by ISPs.[172] This is on par with

---

[166] *See* CAN-SPAM Act of 2003 §§ 6(a) & 6(b).
[167] *See Id.* § 6(a)(1) ("(a) IN GENERAL.--It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person--
(1) knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message").
[168] Declan McCullagh, *FTC Chair: Antispam Proposals Lacking*, CNET NEWS.COM, *at* http://news.com.com/2100-1028-5065739.html?tag=nl (last modified Aug. 19, 2003).
[169] *See* CAN-SPAM Act of 2003 § 8(b)(2) ("(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.--This Act shall not be construed to preempt the applicability of--
(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.").
[170] *See* McCullagh, *supra* note 2.
[171] CAN-SPAM Act of 2003 § 7(f)(3). For aggravated damages, where the spammer willfully and knowingly violated the act, the court may triple the damages. *Id.* § 7(f)(3)(C).
[172] *Id.* § 7(g)(3).

or greater than laws from states with stronger spam laws.[173] Furthermore, at the court's discretion, the State or ISPs may be awarded reasonable attorney fees.[174] Criminal charges may be brought under CAN-SPAM's amendment to Chapter 47 of Title 18 of the United States Code, with a maximum sentence of 5 years.[175]

Although CAN-SPAM provides fairly strict guidelines for measuring damages, Professor Ramasastry[176] has argued that even if spammers lose a suit under CAN-SPAM, enforcing the judgments may prove difficult.[177] Many spammers consist of individuals or small businesses and may not be able to pay "even if they are inclined to, which is unlikely."[178] This concern is specifically addressed by Wyden and Burns who believe that someone who benefits from the e-mail, either spammers or those who hire spammers, will have the liability and the resources to be able to pay for the large damages.[179] Attacking either spammers or their customers will both serve to decrease the amount of spam.

F. Pornography

Due to the greater contempt of pornographic spam, CAN-SPAM has an additional subject heading requirement that e-mail containing sexually oriented material[180] contain a mark or

---

[173] *See* Wash. Rev. Code Ann. §19.190.040; Cal. Bus. & Prof. Code §17538.45(f), *available at* http://www.spamlaws.com/state/ca1.html; Va. Code Ann. §18.2-152.12; *See also* La Monica, *supra* note 20. One can surmise that the reason that states like California, Washington, and Virginia have tougher spam laws is because the largest and most powerful ISPs are located in those states; namely, Yahoo in California, Microsoft in Washington, and AOL in Virginia.

[174] CAN-SPAM Act of 2003 §§ 7(f)(4) & 7(g)(4).

[175] *See id.* § 4(b)(1).

[176] Anita Ramasastry is an associate professor of law at the University of Washington School of Law in Seattle and a director of the Shidler Center for Law, Commerce & Technology. The website is available at http://www.law.washington.edu/lct/.

[177] *See* Ramasastry, *supra* note 53.

[178] *Id.*

[179] Wyden, *supra* note 115.

[180] CAN-SPAM Act of 2003 § 5(d)(4) ("Sexually oriented material" is given the same meaning as "sexually explicit conduct" in 18 U.S.C. §2256. This is the chapter regarding "sexual exploitation and other abuse of children." The definition of "sexually explicit conduct" means actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area of any person.) *See* 18 U.S.C. § 2256 (2003).

notice.[181] The FTC proposed a rule requiring senders of adult-related e-mail to include the label "Sexually-Explicit-Content:" in e-mail headers and within the text of the message.[182] While CAN-SPAM only has a subject heading requirement for spam with sexual conduct, many state laws impose a subject line requirement for all unsolicited e-mails.[183] However, despite state requirements, the FTC found that less than 2% of spam used the required label.[184]

G. Other Arguments and Concerns

CAN-SPAM, recognizing e-mail is becoming prevalent on cell phones, has provisions for anti-spam measures on wireless systems to be administered by the Federal Communications Commission (FCC).[185] Short message service (SMS) spam is currently a large problem for Asia, and will like spread to the US as SMS becomes more common.[186] Furthermore, a British report indicated that "65 percent of Europe's cell phone users report receiving up to five unsolicited text messages a week."[187] In the coming years the FTC must study the effectiveness of CAN-SPAM on limiting spam, as consumers have indicated that their threshold for tolerating SMS spam is significantly lower than for e-mail spam.[188] Also, CAN-SPAM addresses another common concern that US-based spammers will be able to move their operations offshore.[189]

---

[181] CAN-SPAM Act of 2003 § 5(d)(1)(A) ("IN GENERAL.--No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and--
(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection").
[182] Stefanie Olsen, *FTC Proposes Adult Spam Labels*, CNET NEWS.COM, *at* http://news.com.com/2100-1028-5149613.html?tag=nefd_hed (last modified Jan. 28, 2004).
[183] Nelson, *supra* note 104, at 1210. Typically, the states requirement the notice "ADV:," for advertisement, to precede any other text in the subject heading.
[184] Ho, *supra* note 84.
[185] CAN-SPAM Act of 2003 § 14.
[186] Reuters, *Spam Invasion Targets Mobile Phones* (Feb. 5, 2004), *available at* http://www.cnn.com/2004/TECH/ptech/02/04/cellphone.spam.reut/index.html.
[187] Reuters, *Study: More Spam Served Up to Cell Phones* (Feb. 18, 2004).
[188] *Id.*
[189] Ramasastry, *supra* note 53.

CAN-SPAM has provisions that hold third parties liable for hiring those off-shore spammers,[190] which is a key CAN-SPAM feature that is frequently cited by Wyden and Burns.[191]

Another element that is required under CAN-SPAM, which state laws do not require, is a "valid physical postal address of the sender."[192] It is difficult to tell how useful this requirement will be in stopping spam. While 95% of spammers are complying with the unsubscribe feature, only 56% include a postal mailing address.[193] Those spammers that do obey the requirement have been using deceitful means to mask their addresses from filters. For example, some spammers include hidden characters between letters so that "Houston, TX" might appear to e-mail users as "H o u s t o n, T X," but to spam filters as "Hxoxuxsxtxoxn, TxX."[194] Others embed the postal address in graphic images, invisible to filters and e-mail that is not HTML-enabled.[195]

IV. Alternative Solutions

It has taken almost four years for CAN-SPAM to finally become the first national anti-spam legislation.[196] While Congress was debating the issue, legislators and interest groups have been developing alternative methods and theories to fight spam. While spam requires enforcement from a legal standpoint, different solutions suggested are based on theories grounded in law, economics, technology, self-help, and international cooperation.

A. Legal Alternatives

---

[190] CAN-SPAM Act of 2003 § 6(a).
[191] Wyden, *supra* note 115.
[192] CAN-SPAM Act of 2003 § 5(a)(5)(A)(iii).
[193] Loren McDonald, *Complying and Confused: EmailLabs CAN-SPAM Audit of Permission Based Emails*, Jan. 2004, *available at* http://www.emaillabs.com/article_CANSPAMAudit.html.
[194] Lance Ulanoff, *Spam: A Reality Check*, PC MAGAZINE, Feb. 18, 2004, *available at* http://www.pcmag.com/article2/0,4149,1529307,00.asp.
[195] Chris Ulbrich, *Spam Travels Into Gray Area*, WIRED, Jan. 29, 2004, *available at* http://www.wired.com/news/technology/0,1282,62087,00.html.
[196] Press Release, United States Senator Conrad Burns, Burns-Wyden "CAN-SPAM" Bill Expected to Become First National Anti-Spam Law (Nov. 25, 2003), *available at* http://burns.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=1030.

While many politicians hope that CAN-SPAM will serve to be the primary weapon used to fight spam, many individuals and ISPs have long used alternative means to bring actions against spammers.[197] Legal causes of action can and have been brought against spammers under trespass,[198] nuisance,[199] conversion,[200] and the Computer Fraud and Abuse Act.[201] Furthermore, as spam is often a vehicle for fraudulent activities, there are many alternative theories which a prosecutor may choose to indict a spammer, such as identity theft, forgery, fraud, etc.[202] Therefore, although CAN-SPAM preempts state laws specific to commercial e-mail,[203] it leaves ample alternative state causes of action[204] which ISPs, state attorney generals, and most importantly private individuals may utilize in the fight against spam.

For a period of time, private individuals were bringing suits against spammers under the US Junk Fax law, the TCPA.[205] Interestingly, the first spam-related lawsuit was, in fact, brought under the TCPA.[206] The plaintiff successfully argued that the TCPA's definition of "facsimile

---

[197] *See* Magee, *supra* note 87, at 349-56; Paul L. Schmehl, *First Amendment Issues Related to UBE*, *at* http://www.utdallas.edu/~pauls/spam_law.html (last visited Jan. 18, 2004). For a listing of cases involving junk e-mail visit http://legal.web.aol.com/decisions/index.html or http://www.netlitigation.com/netlitigation/spam.htm. Many of these cases have been brought against Cyber Promotions, a notorious spam company. Cyber Promotions was once the most well-known spam company on the Net. Its president, Sanford "Spamford" Wallace, is the veritable Larry Flynt of spam litigation, and his company had been legally challenged by countless corporations, ISPs, and individuals, which have tested the reaches of legal means to fight spam. *See* Courtney Macavinta, *Cyber Promotions Under Siege*, CNET NEWS.COM, *at* http://news.com.com/2100-1023_3-202295.html (last modified Aug. 12, 1997). In fact, his company had also dabbled in some online First Amendment issues that have earned him the title of being "one of the most hated men on the Internet." *Cyber Promotions Hosts Hate Site*, *supra* note 50.

[198] *See* Schmehl, *supra* note 197 (*citing* Earthlink Network Inc. v. Cyber Promotions, Inc., No. BC167502, slip op. (CA Super. Ct. May 7, 1997)); Press Release, AOL Legal Department, Earthlink v. Cyber Promotions Press Release (May 7, 1997), *available at* http://legal.web.aol.com/decisions/dljunk/earthlinkp.html.

[199] *See* Web Systems Corp. v. Cyber Promotions, Inc., No. 97-30156, *available at* http://legal.web.aol.com/decisions/dljunk/websysc.html.

[200] *See id.*

[201] *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 437 (E.D. Pa. 1996); 18 U.S.C. § 1030.

[202] *See* Olsen, *supra* note 50.

[203] CAN-SPAM Act of 2003 § 8(b)(1).

[204] *See id.* § (8)(b)(2).

[205] Paul Festa, *Spam Law a Matter of Fax?*, CNET NEWS.COM, *at* http://news.com.com/2100-1028-994076.html (last modified Mar. 26, 2003).

[206] Sorkin, *supra* note 21, at 357.

machine" covered electronic mail.[207] Since then others have sued spammers under TCPA with success; however, many of these cases were in small claims courts, which carry very little value as precedents.[208] Unfortunately, this argument is not as applicable today, as much spam is delivered by technology that "couldn't remotely be construed as involving a modem."[209] Another problem with using the TCPA to attack spam is that there is nothing in the legislative history indicating that TCPA would cover spam sent using e-mail.[210] The Pennsylvania Superior Court has already held that the TCPA does not apply to e-mail spam,[211] and this holds "persuasive authority" with other courts.[212] Furthermore, Professor Sorkin believes that it is unlikely other courts would find that TCPA applies to e-mail, thus leaving many e-mail users without protection from spammers.[213] However, these plaintiffs had to resort to the TCPA because there were no state laws regulating spam at the time,[214] but CAN-SPAM provides the necessary protection. While CAN-SPAM currently does not give individuals a private right of action, as stated earlier, this need for a private right of action may be remedied by future amendments to CAN-SPAM.

B. Economic Alternatives

---

[207] *Id.*
[208] Festa, *supra* note 205. (As the founder of antispam group Junkbusters said, "such forums don't set precedents in concrete--or even Jell-O").
[209] *Id.* The TCPA requires that transmissions be through a "telephone facsimile machine," and modems are the electronic devices that would connect a telephone to the Internet. *See* Telephone Consumer Protection Act of 1991 § 3(a)(6)(d)(1)(A); *Modem*, HyperDictionary, *at* http://www.hyperdictionary.com/dictionary/modem (last visited Jan. 18, 2004).
[210] Aronson v. Bright-Teeth Now, LLC., 57 Pa. D. & C. 4th 1, 3 (2002).
[211] Aronson v. Bright-Teeth Now, LLC., 2003 Pa. Super 187.
[212] Festa, *supra* note 205.
[213] *See Aronson*, 57 Pa. D. & C. 4th at 3; Festa, *supra* note 205.
[214] Pennsylvania did not approve a law regulating e-mail until Dec. 16, 2002. *See* 18 PA. CONS. STAT. ANN. § 7661 (2002), *available at* http://www.spamlaws.com/state/pa.html.

Spam is profitable because there are essentially zero costs, regardless of how many e-mails are transmitted.[215] Unlike every other form of advertisement, such as telemarketing, fax spam, newspapers, door-to-door solicitors, and junk mail, the costs are the same regardless of how many times an ad is repeated or sent. Therefore, one solution that has been proposed is to tax all e-mail,[216] and the idea already has some support from legislators.[217]

An e-mail tax shifts the burden from the recipients and ISPs over to the senders or spammers.[218] Furthermore, if only a small tax is placed on e-mails, the cost would be negligible for the typical consumer. In fact, taxes could be levied only on e-mail amounts greater than a "reasonable threshold" a month, as the average consumer does not send much e-mail.[219] For bulk senders, even a tax as low as a suggested one quarter of one cent per message would render the cost-effective bulk e-mail methodology unworkable.[220]

However, charging for e-mail is not without its disadvantages. An inherent flaw in any spam solution is that spammers are criminals, and if they will resort to fraud or identity theft,

---

[215] *FTC Chair Tim Muris, supra* note 29; *See generally The Economics of Spam*, ePrivacyGroup, *at* http://www.eprivacygroup.com/article/articlestatic/58/1/6 (last visited Jan. 20, 2004).
[216] Jim Nail, *Commentary: Spammers Must Pay*, CNET News.com, Dec. 16, 2003, *at* http://news.com.com/2030-1028-5125275.html?tag=nl.
[217] Dunbar, *supra* note 123 (citing support for the tax from Sen. Dayton (D-Minn.)).
[218] Nail, *supra* note 216.
[219] *Id.* This threshold amount is a necessary aspect for two reasons: (1) consumer support would largely be against a solution requiring them to pay for services they are accustomed to receiving for free and (2) charging for e-mail may otherwise increase the digital divide. The first concern, as stated later in the article, is a significant barrier for establishing the e-mail tax solution. The second concern is important because charging for e-mail may be considered a minimal cost for the technological elite, but it may increase the digital divide. The Digital Divide is essentially the gap between those who have access to the Internet and those that do not. APPU KUTTAN & LAURENCE PETERS, FROM DIGITAL DIVIDE TO DIGITAL OPPORTUNITY 3 (2003). Typically those that do have access are economically privileged. There is also a marked divide of information access in the world. *See* Jane Black, *The Cost of Communication*, BBC NEWS, Oct. 14, 1999, *at* http://news.bbc.co.uk/1/hi/special_report/1999/10/99/information_rich_information_poor/472445.stm; Norman Y. Mineta, *Falling Through the Net: Toward Digital Inclusion*, U.S. DEPARTMENT OF COMMERCE, Oct. 2000, at xiii, *available at* http://search.ntia.doc.gov/pdf/fttn00.pdf. Hence, even if the US can get other countries to agree to charge for e-mail, it will not help bridge the gap in the worldwide digital divide so that the other 98% of the world can have access to the Internet. *See* Black, *supra.*
[220] Nail, *supra* note 216.

they could also use phony credit cards to pay for the e-mail tax.[221] There is also no secure mechanism to charge for e-mail, thus the industry would have to create a new standard that all ISPs would have to adopt.[222] This could be costly and it will be as difficult to get technologists to agree on such a system, as it was for Congress to finally agree on the provisions of CAN-SPAM. Furthermore, there would be a question of how to enforce the tax collection because the US would not be able to tax spammers in other countries. Nevertheless, the idea of a tax on spam has proven to be politically unpopular,[223] and so the US may have to wait till the next round of negotiations before a tax system could be proposed.

C. Technical Solutions

Currently, most businesses and individuals already invest in technical solutions to counter spam, but these spam-filters are ineffective as spammers are constantly adapting. Large ISPs are constantly innovating to make their systems spam proof. For example, Microsoft plans to implement white lists,[224] Yahoo plans to include features in its mail service, such as dummy e-mail addresses when subscribing to services on the Internet,[225] and AOL "is testing an antispam filter intended to accurately trace the origin of e-mail messages."[226] Of course, services also have to be careful with the methods with which to filter spam. If they are overzealous they may end up blocking legitimate e-mail and anger e-mail users.[227] While individual ISPs may

---

[221] Dunbar, *supra* note 123.
[222] *Id.*
[223] *Id.*
[224] A white list is a list of approved senders that the e-mail user accepts. E-mail from senders not on the list are typically rejected, deleted, or are diverted to other folders. This method is still highly susceptible to virus attacks, especially those that use an e-mail users address book to propagate itself.
[225] Paul Festa, *Hotmail Tries to Fry More Spam*, ZDNET AUSTRALIA, Oct. 24, 2003, *at* http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20280106,00.htm.
[226] Stefanie Olsen, *AOL Tests Caller ID for E-mail*, CNET NEWS.COM, *at* http://news.com.com/2100-1032-5145065.html?tag=nl (last modified Jan. 22, 2004).
[227] *See* Lisa M. Bowman, *Hotmail Spam Filters Block Outgoing E-mail*, CNET NEWS.COM, *at* http://news.com.com/2009-1023-251171.html?legacy=cnet (last modified Jan. 18, 2001).

implement spam prevention features, this does very little to stem the torrent of spam passing through the hundreds of other ISPs in the world.

Any technical solution would require a new standard or protocol that all ISPs would implement. FTC Chairman Muris has called for a revision of the Simple Mail Transport Protocol (SMTP).[228] Yahoo is developing an open-source "Domain Keys" software to require authentication of a message's sender.[229] Another ISP, Earthlink, is developing Challenge/Response systems that would send a form back to a sender not on a user's white list, requiring the form to be filled out and returned before the e-mail is accepted.[230] The idea is that only a human sender would be able to answer the form because spammers' automated software is not sophisticated enough to respond to the form. However, this can cause delays, and people frequently receive automated e-mails or important mass e-mailings if they are on e-mail lists.[231]

Experts realize that any approach that requires authentication or a cryptographic solution will require computing overhead or extra bandwidth, and though this may not affect a normal user, it would require larger companies and ISPs to absorb the costs.[232] Furthermore, any system that requires a change in protocol requires every ISP in the world to accept it.[233] However, if the largest ISPs agree to work together[234] to accept one standard then there is potential to make a dent in the amount of spam.[235]

---

[228] McCullagh, *supra* note 168.
[229] *See* Ben Berkowitz, *Yahoo Proposes New Internet Anti-Spam Structure*, REUTERS, Dec. 5, 2003, *available at* http://www.usatoday.com/tech/news/techinnovations/2003-12-05-yahoo-spam-switch_x.htm.
[230] Baker, *supra* note 19, at 80.
[231] *Id.*
[232] *See* Berkowitz, *supra* note 229.
[233] *Id.*
[234] *See* Press Release, Microsoft PressPass, *America Online, Microsoft and Yahoo! Join Forces Against Spam* (Apr. 28, 2003), *available at* http://www.microsoft.com/presspass/press/2003/apr03/04-28JoinForcesAntispamPR.asp.
[235] Berkowitz, *supra* note 229.

Microsoft has a solution that shows promise of being effective – the Penny Black project.[236] Taking from the economic theory that the only way to reduce spam is to make it "costly" for spammers, the technique forces them to pay in terms of time. If a sender sends an e-mail to a recipient, and the sender is not in the recipient's safe-list, then the sender will be required to solve a puzzle as a "proof of effort" specific to the message, the sender, and the recipient.[237] The puzzle or CPU-function requires the sender's computer to expend a certain amount of CPU time to calculate, and occurs at no expense to the recipient, thus shifting the "cost" of spam back onto spammers.[238] The common example is to suppose there are 80000 seconds in a day[239] and the computational function costs a sender ten-seconds of computational time. A spammer would only be able to send a maximum of 8000 spam messages a day per computer.[240]

There are many companies and ISPs developing full-fledged technological solutions. However, any standard or cryptographic solution that would be implemented requires full support from a significant number of ISPs, otherwise it will fail. Furthermore, it is important that the software is open-source or open-standard[241] and that the technology is not patented.[242]

---

[236] *The Penny Black Project*, MICROSOFT RESEARCH, *at* http://www.research.microsoft.com/research/sv/PennyBlack/ (last visited Jan. 18, 2004).

[237] *See* Jo Twist, *Microsoft Aims to Make Spammers Pay*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/technology/3324883.stm (last updated Dec. 26, 2003); Mike Burrows et al., *No Spam at Any (CPU) Speed*, http://www.research.microsoft.com/research/sv/PennyBlack/demo/index.html (last visited Jan. 18, 2004).

[238] *See* Twist, *supra* note 237; Burrows, *supra* note 237.

[239] This is a rounded figure. There are actually 86,400 seconds in a day.

[240] Twist, *supra* note 237; Burrows, *supra* note 237.

[241] Twist, *supra* note 237; Burrows, *supra* note 237. An open-standard SMTP extension that has gaining popularity is SPF (Sender Policy Framework) which contains a registry of valid domains and IP addresses and gives ISPs the ability to reject spam before it is downloaded. Mark Baard, *Going Upstream to Fight Spam*, WIRED, Jan. 20, 2004, *available at* http://www.wired.com/news/infostructure/0,1377,61971,00.html?tw=wn_story_related; *See Sender Policy Framework (SPF)*, *at* http://spf.pobox.com/ (last visited Feb. 28, 2004);

[242] *See generally* Festa, *supra* note 163. While many ISPs, such as Microsoft, participate in developing open-source anti-spam technology, they also develop patented technology only to be used for their servers, or to be licensed. *See* Press Release, Microsoft PressPass, *Microsoft Offers Technology Designed to Help Protect Inboxes From Spam,*

Otherwise, it would be unlikely that other ISPs would implement the solution. It would also be highly deceptive and unethical for any ISP to help establish or push for a standard for which it has patented technology.[243]

D. Self-Help

While governments and companies are starting to realize the threat of spam, individual e-mail users are still encouraged to engage in self help. This is not to be mistaken with taking affirmative action against spammers;[244] rather e-mail users are encouraged to take steps to protect themselves from the onslaught of spam.[245] For example, individual users can install anti-spam filters, though this can be costly.[246] Many e-mail users also set up "spam accounts" to use to sign up for services or to post on the Internet.[247] E-mail users that are afraid their e-mail may be blocked or filtered can simply set their subject headings to say, "Not Spam," and recipients can set their filters to accept any e-mail that has this subject heading.[248] Spammers would not be able to use this technique because their subject headings would be fraudulent and actionable under CAN-SPAM. However, this solution requires the end user to download the message in order to filter it, which takes up bandwidth. Eventually, anti-spam technology and legislation

---

(Nov. 17, 2003), *available at* http://www.microsoft.com/presspass/press/2003/nov03/11-17ComdexAntiSpamPR.asp.

[243] The FTC filed an antitrust case against Rambus alleging that they participated in standards-setting for the PC memory industry while pushing for standards based on patented Rambus technology. Tom Krazit, *FTC opens case against Rambus*, COMPUTERWORLD, Apr. 30, 2003, *at* http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,80820,00.html. The patents were upheld by the Federal Circuit in January, 2003. *See* Tom Krazit, *FTC, Rambus Set to Square Off in Court*, PC WORLD, Apr. 30, 2003, *at* http://www.pcworld.com/news/article/0,aid,110526,00.asp; Tom Krazit, *Rambus Patents Upheld*, PC WORLD, Jan. 29, 2003, *at* http://www.pcworld.com/news/article/0,aid,109084,00.asp. Ultimately, the FTC administrative law judge dismissed the case against Rambus. Dawn Kawamoto, *Rambus Wins Major Round in FTC Case*, CNET NEWS.COM, *at* http://news.com.com/2100-1004-5160694.html?tag=nefd_hed (last modified Feb. 18, 2004).

[244] Elise Ackerman, *Spam Sends Local Man Into Rage*, SILICONVALLEY.COM, Nov. 22, 2003, *at* http://www.siliconvalley.com/mld/siliconvalley/7326032.htm (After receiving one too many penile enlargement spams, a man was arrested for sending death threats to the alleged spammer.)

[245] For general methods for system administrators and e-mail users to protect themselves from spam, see *The FAQs*, RAW LOGIC SOFTWARE, *at* http://www.rawlogic.com/thefaqs.html (last visited Jan. 11, 2004).

[246] Leung, *supra* note 30, at 11.

[247] *See* Baker, *supra* note 19, at 80 (Twelve percent of AOL users have a spam account.).

[248] Sorkin, *supra* note 21, at 345-46.

should become more sophisticated so that the bulk of the work is not required on the user side, but rather on the ISP and FTC end.[249]

E. International Solutions

As the Internet has no boundaries, the solution must also be co-extensive; stopping spam will inevitably require an international solution. In 2002, the European Union (EU) lost nearly $3 billion in lost productivity due to spam.[250] Most of the spam in the EU comes from abroad, particularly the US.[251] Thus, many countries in the world have been waiting to see the approach the US will use to try and stop spam,[252] but in the meantime, in 2003, Australia[253] and the United Kingdom[254] passed anti-spam legislation.

There are already efforts by countries to try and find a solution together; and they frequently look to developments in other countries. The UK, for example, was glad that the US had passed a law,[255] and as one Member of the House of Commons stated, "Even a flawed law is

---

[249] In fact, the bulk of the cost should be on industry because the FTC is particularly deferential to industry self-regulation. Courtney Macavinta, *FTC Searches for Spam Solution*, CNET NEWS.COM, *at* http://news.com.com/2100-1023-200486.html?legacy=cnet (last modified June 12, 1997).

[250] Chris Morris, *New EU Laws Tackle Spam*, BBC NEWS, *at* http://news.bbc.co.uk/1/hi/world/europe/3231861.stm (last updated Oct. 13, 2003).

[251] *Id.* (last updated Oct. 13, 2003). A Sophos study shows that 56.74% of spam originates in the United States. *Sophos Outs 'Dirty Dozen' Spam Producing Countries*, SOPHOS, Feb. 26, 2004, *at* http://www.sophos.com/spaminfo/articles/dirtydozen.html.

[252] *See* Magee, *supra* note 87, at 381.

[253] Spam Act 2003, passed on November 28, 2003, royal assent was given on December 2, 2003, and will come into full operation 120 days after assent was granted, hence April 10, 2004. The law will be policed by the Australian Communications Authority. *See* Chris Jenkins, *Spam Bill Passed*, THE AUSTRALIAN, Dec. 2, 2003; *Analysis of Spam Bills 2003*, ELECTRONIC FRONTIERS AUSTRALIA, *at* http://www.efa.org.au/Publish/spambills2003.html (last updated Nov. 1, 2003).

[254] Effective as of December 11, 2003, Britain's implementation of the EU Privacy and Electronics Communication Directive came into force as the Privacy and Electronic Communications (EC Directive) Regulations 2003. *See About the Regulations*, INFORMATION COMMISSIONER, *at* http://www.informationcommissioner.gov.uk/eventual.aspx?id=783 (last visited Jan. 18, 2004); Graeme Wearden, *UK Joins Australia in Banning Spam*, ZDNET AUSTRALIA, Sept. 19, 2003, *at* http://www.zdnet.com.au/newstech/communications/story/0,2000048620,20278757,00.htm.

[255] Wearden, *supra* note 254.

better than no law at all."[256] Of course, the UK was highly criticized in its own implementation of anti-spam laws because it distinguishes between personal and corporate accounts, only making it illegal to spam personal accounts.[257] However, both the UK and US recognize that international cooperation will be the key to stopping spam.[258] Before international cooperation can begin, countries like the US and UK have to stabilize the problem within their own borders. Only then can they help rein in spammers located in Russia and China - neither country has an anti-spam law.[259] In addition, on December 10, 2003, the United Nations convened the first-ever World Summit on the Information Society and discussed the topic of spam.[260] Other countries are already taking action for global cooperation; for example, even before the passage of their spam bill, Australia signed a memorandum of understanding (MoU) with the Republic of Korea to promote the regulation of spam.[261]

Spam actually has many similarities with another international problem, money-laundering, which uses very similar tactics as spam that make it difficult to prevent. Money laundering is essentially taking illegally-obtained money and giving it the appearance of originating from a legitimate source.[262] Money is laundered by placing the ill-gotten money into the financial system ("placement"), moving the funds through various financial institutions

---

[256] Tim Lemke, *Britain Asks U.S. For Law on Spam*, THE WASHINGTON TIMES, Oct. 15, 2003, *at* http://washingtontimes.com/business/20031014-092600-3179r.htm. The UK and Australian governments had hoped that the US would adopt opt-in measures similar to its own laws. *See also* Pearce, *supra* note 100.
[257] Wearden, *supra* note 254.
[258] Roy Mark, *U.S., U.K. Call for Anti-Spam Cooperation*, ASPNEWS.COM, Oct. 14, 2003, *at* http://www.aspnews.com/news/article.php/3091911. Co-author Wyden believes that even with the passage of CAN-SPAM, international cooperation is still needed. This sentiment is echoed by UK "e-Envoy" to the US, Andrew Pinter. *Id.*
[259] *See id.*.
[260] Paul Quigley, *UN Hosts Summit on Spam*, ENTERPRISE CONTENT MANAGEMENT, Oct. 11, 2003, *at* http://www.contentmanagement365.com/Information_Architecture_Analysis/Article1755.aspx.
[261] *Australia and Korea Sign Spam MoU*, FINDLAW, Oct. 21, 2003, *at* http://www.findlaw.com.au/news/default.asp?task=read&id=17089&site=LE.
[262] Kristine Karsten, *Money Laundering: How it Works and Why You Should Be Concerned, in* ARBITRATION: MONEY LAUNDERING, CORRUPTION AND FRAUD 16 (Kristine Karsten & Andrew Berkeley eds., 2003); *See also Basic Facts About Money Laundering*, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, *at* http://www1.oecd.org/fatf/MLaundering_en.htm (last updated Oct. 9, 2003).

around the world ("layering"), and then finally having the funds re-enter the legitimate economy ("integration").[263] Money launderers frequently scatter their money through jurisdictions that do not have money laundering laws or financial institutions that are not diligent in questioning depositors.[264] Launderers engage in evasive tactics such as structuring their bank deposits into smaller amounts, a technique known as "smurfing."[265]

Many countries have realized that the only way to solve the money-laundering problem is to work together. The Financial Action Task Force (FATF), an inter-governmental body, was created for the purpose of establishing policies and standards, called the Forty Recommendations, which member countries can enact in legislation.[266] The Forty Recommendations provides definitions and scope of crimes including mental intent required,[267] measures to be taken by financial institutions,[268] and the establishment of authorities to monitor money laundering[269] and provide mutual legal or other cooperative assistance to other countries.[270] For example, financial institutions are recommended to "maintain, for at least five years, all necessary records on transactions … to enable them to comply swiftly with information requests from the competent authorities."[271] In order for countries to be able to cooperate effectively to initiate these measures there needs to be, at least, (1) a treaty imposing mutual

---

[263] Bernardo M. Cremades & David J.A. Cairns, *Transnational Public Policy in International Arbitral Decision-Making: The Cases of Bribery, Money Laundering and Fraud, in* ARBITRATION: MONEY LAUNDERING, CORRUPTION AND FRAUD 70 (Kristine Karsten & Andrew Berkeley eds., 2003); *See Basic Facts About Money Laundering*, *supra* note 262.
[264] *See Basic Facts About Money Laundering*, *supra* note 262.
[265] Kristine Karsten, *Money Laundering: How it Works and Why You Should Be Concerned, in* ARBITRATION: MONEY LAUNDERING, CORRUPTION AND FRAUD 17 (Kristine Karsten & Andrew Berkeley eds., 2003); *See Money Laundering*, NATIONAL DRUG INTELLIGENCE CENTER, Oct. 2001, *at* http://www.usdoj.gov/ndic/pubs/647/money.htm.
[266] *See More About the FATF and Its Work*, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, *at* http://www1.oecd.org/fatf/AboutFATF_en.htm (last updated Dec. 5, 2003).
[267] *See The Forty Recommendations*, Financial Action Task Force, R. 1-2 (2003), *available at* http://www1.oecd.org/fatf/40Recs_en.htm (last updated Nov. 5, 2003).
[268] *See id.* at R. 4-25.
[269] *See id.* at R. 26-34.
[270] *See id.* at R. 36-40.
[271] *Id.* at R. 10.

obligations, (2) legislation in the sending State, and (3) legislation in the receiving state. Furthermore, the FATF also monitors member countries to ensure the effectiveness of the implementation of the standards.

Similar to money laundering, spam is typically a vehicle to facilitate an underlying crime.[272] Spam also works by being routed, typically through open relays and different jurisdictions to avoid detection. Much like "smurfing," spam software can be programmed to throttle the rate of sending e-mail and send the e-mail between mid-night and 6 A.M, when ISPs are less vigilant.[273] Therefore, in order to find an international solution to spam, governments need to cooperate in the manner they have cooperated to fight against money laundering.

An inter-governmental anti-spam organization should be established to make recommendations regarding implementing various provisions in national laws, such as, opt-in vs. opt-out, subject line headings, criminal provisions and level of intent, third-party liability, etc. To ensure cooperation and harmonization, governments would have to be willing to subject themselves to monitoring by the international anti-spam organization. Recommendations should be given for establishing governmental policing organizations similar to the FTC in the US, and possibilities of world-wide Do-Not-Spam registries. If recommendations are followed, then the governments will effectively locate and punish spammers.

The organization can recommend actions to be implemented by ISPs (the spam equivalent of financial institutions), as they are the primary institutions that spam will travel through. Recommendations can include detecting threshold levels of bulk messages, setting privacy standards when filtering e-mail, or encouraging the implementation of secured e-mail standards, etc. Furthermore, similar to requiring financial institutions to keep financial

---

[272] *See id.* at Introduction.

[273] Leung, *supra* note 30, at 7. Throttling e-mail means to send e-mail in bursts at a rate below the rate at which an ISP may set their servers to alert network administrators to potential bulk e-mail.

transaction data, e-mail traffic data may need to be kept for several years, and, in fact, the European Union (EU) has considered proposals to regulate ISP data retention.[274] Also, the organization may very well recommend that countries require their ISPs to implement technical protocols as suggested above. There is already much promise of cooperation from countries and also from ISPs. Countries are already working together, as the FTC and related foreign agencies have already participated in international efforts like that of Operation Secure Your Server.[275] Industry leaders, such as AOL, Microsoft, and Yahoo! Inc. have announced their commitment to work together,[276] and Microsoft has already sent letters to Congress and the FTC suggesting the need for an authority to implement certain technology.[277]

If countries with high volumes of citizens that are "connected" implement these recommendations, then other countries will likely follow suit. Ninety-eight percent of the world is still not connected to the Internet, but as the digital divide[278] decreases, there will inevitably be need for more regulation.[279] Poorer countries have an incentive to implement the recommendations when creating or expanding their Net infrastructure because they want to avoid the bandwidth and productivity costs of spam. Furthermore, developing countries do not want to be known as safe havens for spammers and scammers,[280] nor do these countries want their ISPs

---

[274] Paul Meller, *EU Ministers Debate ISP Data Retention Rules*, CNN, Nov. 28, 2001, *at* http://www.cnn.com/2001/TECH/internet/11/28/data.retention.debates.idg/.
[275] Grant Gross, *Vulnerable Servers Warned*, PC WORLD, Jan. 29, 2004, *available at* http://www.pcworld.com/news/article/0,aid,114528,00.asp.
[276] *America Online, Microsoft and Yahoo!, supra* note 234.
[277] *See Trusted Email Open Standard*, EPRIVACYGROUP, *at* http://www.eprivacygroup.com/teos (last visited Jan. 18, 2004).
[278] For an explanation of the digital divide, see supra text accompanying note 219.
[279] *See* Black, *supra* note 219.
[280] *See* Brian Sullivan, *Nigeria Launches Web Site to Target E-mail Scams,* COMPUTERWORLD, Mar. 26, 2002, *at* http://www.computerworld.com/softwaretopics/software/story/0,10801,69562,00.html.

to be blocked by other countries.[281] Ultimately, all countries will have an incentive to cooperate and participate in the war on spam.

V. Conclusion

While critics are quick to assert the failings of CAN-SPAM provisions, it is important to emphasize that no individual law has been able to stop spam. It is beyond the scope of this paper to discuss which provisions of the US, UK, other nations, or state legislations are most effective. However, what should be recognized is that CAN-SPAM criminalized tactics of spammers and put spammers on notice in a federal law. Already, there is indication that professional spammers are being cautious and attempting to comply with the law.[282] CAN-SPAM has enabled the FTC and ISPs to use those provisions in the fight against spam. So far only one ISP has filed a lawsuit under CAN-SPAM and is asking for $100 in damages.[283] CAN-SPAM will have to be used more aggressively if it hopes to deter spamming in the US.

CAN-SPAM is also a first indication of the US government entering the global fight against spam. Although some believe that there may be difficulty in reaching agreements to stop spam because the EU and the US approach spam with different policies,[284] this has not stopped these countries from coming to agreements in other areas of intellectual property.[285] The most

---

[281] *See* Will Sturgeon, *China Blocks Spam Servers*, CNET NEWS.COM, *at* http://news.com.com/2100-1028-5073441.html (last modified Sept. 9, 2003); Zen Lee, *China Threatens to Block Junk E-mailers*, CNET NEWS.COM, *at* http://news.com.com/2100-1024_3-5162355.html?tag=nefd_top (last modified Feb. 20, 2004).

[282] Saul Hansell, *Unrepentant Spammer to Carry on, Within the Law*, THE NEW YORK TIMES, *at* http://www.nytimes.com/2003/12/30/technology/30spam.html (Alan Ramsky, a notorious spammer, states that he is worried about the potential fines under CAN-SPAM and expects to comply with the law.); Saul Hansell, *Spam Keeps Coming, but Its Senders Are Wary*, THE NEW YORK TIMES, Jan. 7, 2004, *at* http://www.nytimes.com/2004/01/07/technology/07spam.html (Although there is still rampant violations of spam laws, bulk e-mailers are expecting an increasing number of cases brought against spammers.).

[283] Amit Asaravala, *ISP Files First Can-Spam Lawsuit*, WIRED, Mar. 6, 2004, *available at* http://www.wired.com/news/politics/0,1283,62559,00.html?tw=wn_tophead_1.

[284] Festa, *supra* note 163. (Professor Sorkin states that "The Europeans view spam as a privacy and data-protection issue, while [the US] think[s] of it as a nuisance, a property offense, and increasingly, a threat to security.")

[285] For example, in the area of copyright the traditional U.S. and British policies were completely different from European copyright systems. However, eventually all countries signed on to the Berne Convention for the Protection of Literary and Artistic works which favored the moral rights of authors according to French policy.

important indication that these countries are willing to stop spam is that they have already taken the first step to controlling spam, enacting national anti-spam legislation. For the US, that first step, though a tentative step, is CAN-SPAM.[286] The next step is to cooperate with other countries, establish an inter-governmental organization, and create treaties and MoU's.[287] The Australian government's approach to combating spam is the most effective approach, and that is to combine "domestic legislation with international negotiation, public education, the development of industry codes of practice and of technical counter-measures."[288]

Congress recognizes that CAN-SPAM is imperfect, and the FTC is required to submit a report on the effectiveness of CAN-SPAM in 2 years.[289] While some would say that CAN-SPAM is about replacing "bad" spam with "good" spam, that may not be a bad tradeoff.[290] After all, "good" spam is controllable, and CAN-SPAM and future federal laws can aim to eliminate fraudulent spam. CAN-SPAM should work to eliminate the different areas of spam, such as the "amateurs" and the criminal spammers in the US.[291] It also serves as a template for more cooperative efforts with the international effort to fight spam.

However, even if CAN-SPAM does minimize e-mail spam, legislators and companies still have to be watchful about protecting other mediums of the Internet. Already, virus writers

---

Thus, copyright laws were harmonized. FREDERICK ABBOTT ET AL., THE INTERNATIONAL INTELLECTUAL PROPERTY SYSTEM: COMMENTARY AND MATERIALS 82 (Kluwer Law International 1999).

[286] Critics must also keep in mind, as Sen. Burns pointed out, "we don't really know what the completely enacted law will look like, because the FTC and FCC are currently in the process of creating the rules of enforcement." Ulanoff, *supra* note 194.

[287] Sen. Burns notes that spammers' "worst fear is that the international community will come together." Ulanoff, *supra* note 194.

[288] Jenkins, *supra* note 253.

[289] CAN-SPAM Act of 2003 § 10 ("IN GENERAL.--Not later than 24 months after the date of the enactment of this Act, the Commission, in consultation with the Department of Justice and other appropriate agencies, shall submit a report to the Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions.").

[290] Ray Everett-Church, *It's Not Called 'Can' Spam for Nothing*, CNET News.com, Dec. 16, 2003, *at* http://news.com.com/2010-1028-5125192.html?tag=nl.

[291] Ben Berkowitz, *Get Out of Debt! AOL Releases Top Spam List*, FORBES, Dec. 31, 2003, *at* http://www.computercops.biz/modules.php?name=News&file=article&sid=4595.

are attacking Instant Messaging (IM) services,[292] and where virus writers tread, spammers are quick to follow. However, IM is more highly controlled by the services that offer them, and thus the problem does not appear to be as threatening. Also, though already detested among Internet users, pop-ups may become an even more prevalent form of advertising.[293] However, pop-up advertising companies, such as Gator Corporation,[294] well-known for its deceptive tactics of installing ad spyware,[295] have already been sued by various Web sites.[296] The FTC is even starting to keep tabs on search engines, as Internet users are finding that search results are becoming less effective and more commercial.[297]

Spam has indeed changed the face of the Internet. The Internet used to be an open forum for people to share ideas, information, and to meet new people; however, this is an "old school" belief that spam, viruses, and worms have eliminated.[298] Since spam has been flooding inboxes people have become less trustful; for example, 73% of e-mail users now avoid giving out or

---

[292] Dennis Fisher, *New Worm Spreads Via MSN Messenger*, EWEEK, Dec. 31, 2003, *at* http://www.eweek.com/article2/0,4149,1424750,00.asp.

[293] Saul Hansel, *As Consumers Revolt, a Rush to Block Pop-Up Online Ads*, THE NEW YORK TIMES, Jan. 19, 2004, *at* http://www.nytimes.com/2004/01/19/technology/19popup.html?ex=1075093200&en=f6d48b974bf00064&ei=5062&partner=GOOGLE.

[294] Gator Corporation is now known as Claria Corporation, whose websites can be found at http://www.gator.com and http://www.claria.com.

[295] *Spyware*, searchCIO.com Definitions, *at* http://searchcio.techtarget.com/sDefinition/0,,sid19_gci214518,00.html (last updated Dec. 9, 2003) ("In general, spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.").

[296] Todd R. Weiss, *News Sites Settle Pop-Up Lawsuit*, PC WORLD, Feb. 11, 2003, *at* http://www.pcworld.com/news/article/0,aid,109305,00.asp.

[297] Lev Grossman, *Search and Destroy*, TIME, Dec. 22, 2003, at 50. For example, Google, a premier search engine, may feel pressured to advertise; however, as it expands its business to e-mail it will have to find ways to advertise without creating the same aggravations as spam. In fact, it would have to implement anti-spam technology in its e-mail service, much like Yahoo and MSN. Reuters, *Sources: Google Developing Ad Service for E-mail* (Jan. 19, 2004), *available at* http://www.cnn.com/2004/TECH/internet/01/19/google.email.reut/index.html.

[298] Paul Roberts, *Study: ISPs should block 'Net attack ports*, INFOWORLD, Sept. 8, 2003, *at* http://www.infoworld.com/article/03/09/08/HNispstudy_1.html.

posting their e-mail addresses.[299] It is no surprise that Dr. Vint Cerf, known as the "Father of the Internet," calls spam the "scourge of electronic-mail and newsgroups on the Internet."[300] There is a worry that the spirit of the Internet and free communication will be disrupted. Spam is balkanizing the net into small, trusted, closed communities where only people with the right key or identity can share their information.[301] However, there was once a time where people used to trust each other and leave their doors unlocked. Those times are gone in the physical world, and it appears that the abuses of the Internet are finally causing the same distrust to arise in the digital world. However, Dr. Cerf is still a great proponent of the Internet, and, during the 30th Anniversary of the Internet, he stated, "The internet is a reflection of our society and that is going to be reflecting what we see. If we do not like what we see in that mirror the problem is not to fix the mirror, we have to fix society."[302] Unfortunately, if the Internet is any reflection of society, then users should buy a digital deadbolt for their inbox.

---

[299] Fallows, *supra* note 9, at ii.
[300] *The Problem*, Coalition Against Unsolicited Commercial Email, *at* http://www.cauce.org/about/problem.shtml (last visited Jan. 27, 2004).
[301] Baker, *supra* note 19, at 80.
[302] Mark Ward, *What the Net Did Next*, BBC NEWS, Jan. 1, 2004, *at* http://news.bbc.co.uk/1/hi/technology/3292043.stm.