

## NOTE

### SPAM IN A BOX: AMENDING CAN-SPAM & AIMING TOWARD A GLOBAL SOLUTION

*Erika Hallace Kikuchi\**

#### TABLE OF CONTENTS

I. INTRODUCTION .....	56
II. THE SPAM PROBLEM .....	58
A. <i>Spam Statistics</i> .....	58
B. <i>The Spam Monster</i> .....	60
III. THE HISTORY OF ANTI-SPAM TACTICS .....	62
A. <i>Self-Regulation and Technical Tactics to Combat Spam</i> .....	62
B. <i>Various Legal Tactics Used to Combat Spam</i> .....	63
C. <i>Attempts at Federal Spam Legislation Prior to the 108th Congress</i> .....	67
IV. THE CURRENT FEDERAL LEGISLATION .....	69
A. <i>The 108th Congress</i> .....	69
1. <i>Bills Introduced, But Not Passed</i> .....	69
2. <i>The CAN-SPAM Act of 2003</i> .....	71
3. <i>The Selection of CAN-SPAM</i> .....	75
B. <i>Problems and the Need for Change</i> .....	76
1. <i>Major Problems Still Unresolved</i> .....	76
2. <i>The Statistics and Reactions</i> .....	80
3. <i>Time For Change</i> .....	85
V. LESSONS FROM ABROAD: HOW TO MAKE CAN-SPAM MORE EFFECTIVE .....	87
A. <i>The Strong E.U. Opt-In Legislation</i> .....	88
1. <i>The E.U. Legislation</i> .....	88
2. <i>Reactions to the Directive</i> .....	90
3. <i>Feasibility of Integrating E.U. Provisions into CAN-SPAM</i> .....	91
B. <i>Japan and Cellular Spam</i> .....	94
1. <i>History Leading to Legislation</i> .....	94
2. <i>Japan's Spam Legislation</i> .....	96
3. <i>Feasibility of Integrating Japan's Legislation into CAN-SPAM</i> .....	100
VI. COMBINING APPROACHES: AIMING FOR A GLOBAL SOLUTION .....	103
A. <i>Amending CAN-SPAM To Make It More Effective</i> .....	103
1. <i>Opt-In and National "Please E-mail" Registry</i> .....	104
2. <i>Definitions and Exemptions Revised</i> .....	106
3. <i>Harvesting</i> .....	108

\* J.D., Boston University School of Law, 2004, with Honors in the Concentration in Intellectual Property; M.A. in International Relations, *summa cum laude*, Boston University, 2004; B.A., Japanese and Psychology, With Distinction, University of Michigan, 2000.

4. Wireless.....	109
5. Enforcement.....	110
B. <i>Global Harmonization and Technological Innovation</i> .....	111
1. Pursuing Global Harmony.....	111
2. Using New Technology to Aid in the Fight Against Spam ...	115
VII. CONCLUSION .....	116

## I. INTRODUCTION

Everyday, users across the globe open their e-mail accounts to find bright red messages warning that their inboxes are nearly full or that they can “Get a Bigger Mailbox for 9.99/year.”<sup>1</sup> To their chagrin, these users know that they are not simply the most popular among their e-mail buddies, but that they have once again fallen victim to “spam.”<sup>2</sup> The definition of spam is quite loose, often depending on who you ask, but the two most common definitions are unsolicited commercial e-mail and unsolicited commercial bulk e-mail.<sup>3</sup>

The U.S.’s new federal legislation defines commercial e-mail as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose.”<sup>4</sup> Sometimes, commercial e-mail is sent out in “bulk”, i.e., to a large number of recipients.<sup>5</sup> Unsolicited commercial e-mail usually falls into certain content categories: product sales (25%), financial marketing (20%), pornography (19%), various scams (9%), health care (7%), Internet-related (7%), leisure and travel (6%), spiritual (4%), and miscellaneous (3%).<sup>6</sup>

Though the new federal legislation does not define “unsolicited,” in some

---

<sup>1</sup> Yahoo displays this advertisement along with a bar graph showing users how much space is left in the user’s inbox on the Yahoo mail page.

<sup>2</sup> The term “spam” as applied to e-mail came about due to a Monty Python comedy sketch in which a chorus of Vikings sang “spam, spam, spam” at increasing decibels, overwhelming their surroundings just in the same way that commercial e-mail can overwhelm a user’s inbox. See Christopher S. Maravilla, *The Feasibility of a Law to Regulate Pornographic, Unsolicited, Commercial E-Mail*, 4 TUL. J. TECH. & INTELL. PROP. 117, 117 (2002).

<sup>3</sup> See David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 327-28 (2001).

<sup>4</sup> CAN-SPAM Act of 2003, §3 (2)(A) (2004). One weakness of the new law is the confusion it creates due to this definition. See Charles H. Kennedy & Christine E. Lyon, *The CAN-SPAM Act of 2003: A New Regime for Email Advertising*, THE COMPUTER & INTERNET LAW, February 2004, Vol. 21, No. 2, at 2.

<sup>5</sup> See Sorkin, *supra* note 3, at 330.

<sup>6</sup> See *Spam Filter Review 2004*, at <http://www.spamfilterreview.com/spam-statistics.html> (last visited Mar. 11, 2004). Compare these percentages to those from the previous year. See Robyn Greenspan, *Widespread Use Despite Abuse* (Sept. 13, 2002), at <http://www.internetnews.com/stats/article.php/1462941>.

2004]

SPAM IN A BOX

ways this definition is at the very center of a large world debate. Some countries, like the U.S., have taken the position that “unsolicited” should mean that the recipient did not previously object to, or opt-out of, the receipt of commercial e-mail.<sup>7</sup> Though the states had come up with varying definitions,<sup>8</sup> and the debate rages on even after the enactment of federal legislation, the new U.S. federal legislation has decisively implemented an opt-out system. Other countries, however, such as Australia and many European Union member countries, have enacted laws defining it to mean that the recipient did not give explicit consent to, or opt-in to, the receipt of commercial e-mail.<sup>9</sup> The opt-in system is generally stronger than the opt-out system, which tends to favor direct marketers.

The E.U., with its strong opt-in anti-spam legislation, has taken the lead in the fight against spam, and other countries around the world are beginning to follow in the E.U.’s footsteps.<sup>10</sup> Looking to anti-spam measures in other parts of the world, therefore, will provide insight into possible methods by which to improve the current U.S. spam legislation to make it more effective in the future. In addition, the nature of spam requires that countries from around the world strengthen their anti-spam legislative commitments as well, and that the whole world embark on a method of international cooperation, while remaining open to new technological solutions, in order to finally defeat the spam monster.

This paper will first describe in general why spam is problematic. Then, it will go through the history of the wide variety of anti-spam tactics that developed as spam became more problematic. Next, it will discuss the new federal legislation that passed in the 108th Congress, the reasons why it passed, and the many problems it fails to solve. This paper will then discuss recent legislation in the E.U. and in Japan, and draw on the strengths and weaknesses of such legislation in order to determine what changes should be made to the current U.S. legislation. Finally, this paper will discuss some possible changes that would improve the current legislation, and how strong domestic legislation, technological innovation and global harmonization will work

---

<sup>7</sup> CAN-SPAM Act of 2003, S. 877, 108th Cong. (2003).

<sup>8</sup> See Sorkin, *supra* note 3, at 328 (citing CAL. BUS. & PROF. CODE § 17538.4(e), 17538.45(a)(2) (Deering Supp. 2000); Illinois Electronic Mail Act, 815 ILL. COMP. STAT. ANN. 511/5 (West Supp. 2000); NEV. REV. STAT. ANN. 41.730(1) (Michie Supp. 1999); N.C. GEN. STAT. § 14-453(10) (1999); R.I. GEN. LAWS § 6-47-2(e) (Supp. 1999); Colorado Junk Email Law, ch. 388, § 1, 2000 COLO. SESS. LAWS 2031, 2032 (to be codified at COLO. REV. STAT. § 6-2.5-102(5))).

<sup>9</sup> Directive for the Protection of Personal Data and Privacy in the E-communications Sector, Council Directive 2002/58, 2002 O.J. (L 201) 37; ZDNet, *Australia’s Spam Act to Become Law in April* (Dec. 19, 2003), at [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

<sup>10</sup> Council Directive 2002/58, *supra* note 9; ZDNet, *Australia’s Spam Act to Become Law in April*, *supra* note 9, at [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

together to help solve the global spam problem once and for all.

## II. THE SPAM PROBLEM

### A. *Spam Statistics*

According to recent statistics, spam, which celebrated its tenth birthday on March 5, 2004,<sup>11</sup> has burst from its can. Brightmail, one anti-spam technology firm, estimated that there were more than five million spam attacks during August 2002 alone.<sup>12</sup> Mail-Abuse Prevention Systems, an anti-spam organization, reported that the number of spam e-mails sent between April and June of 2002 was seven hundred percent higher than the number recorded during the same period in 2001.<sup>13</sup> Meanwhile, the overall number of e-mails being exchanged was drastically increasing as well. Research firm IDC<sup>14</sup> reported that, by the end of 2002, users had exchanged thirty-one billion e-mails, and predicted that the number of e-mails exchanged would double by 2006.<sup>15</sup> However, this prediction turned out to be a grand underestimation, as numbers showed that approximately one trillion spam e-mails were sent out in 2003 alone.<sup>16</sup>

The Congressional findings that introduce the new federal legislation cite some chilling spam statistics that make the large and increasing number of e-mail even more threatening. According to the findings, spam makes up over fifty percent of all e-mail traffic, up from seven percent in 2001 and still increasing, threatening the e-mail system that is relied on by millions daily for

---

<sup>11</sup> *Spam is 10 Years Old* (Mar. 8, 2004), THE SYDNEY MORNING HERALD, at SMH.com.au, <http://www.smh.com.au/articles/2004/03/08/1078594272395.html>. It has been ten years since the first spam message was sent on March 5, 1994. The message was posted to some Usenet newsgroups by a firm of lawyers, Canter and Siegel, who advertised their services in connection with the Green Card lottery, a move that even then angered many.

<sup>12</sup> See Greenspan, *supra* note 6, at <http://www.internetnews.com/stats/article.php/1462941>.

<sup>13</sup> See Brian Morrissey, *Hotmail Users Have A Weapon Against Spam* (Sept. 18, 2002), at <http://www.internetnews.com/ent-news/article.php/1465411>.

<sup>14</sup> IDC is one of the world's leading providers of technology intelligence, industry analysis, market data, and strategic and tactical guidance to builders, providers, and users of information technology. IDC, *About IDC* (Aug. 29, 2003), at [http://www.idcresearch.com/en\\_US/st/aboutIDC.jhtml;jsessionid=SFUREKFG2J1VYCTFA4FCFFAKMUDYWIWD](http://www.idcresearch.com/en_US/st/aboutIDC.jhtml;jsessionid=SFUREKFG2J1VYCTFA4FCFFAKMUDYWIWD).

<sup>15</sup> See Keith Regan, *The Unstoppable Flood of Spam* (Oct. 29, 2002), at [www.NewsFactor.com](http://www.NewsFactor.com), [http://story.news.yahoo.com/news?tmpl=story2&cid=75&u=nf/20021029/tc\\_nf/19803&printer=1](http://story.news.yahoo.com/news?tmpl=story2&cid=75&u=nf/20021029/tc_nf/19803&printer=1).

<sup>16</sup> See Paul Rubell, *New Federal Law to Take Effect, But Will Spam Be Conquered?*, N.Y. L. J., Dec. 23, 2003, at 16.

2004]

SPAM IN A BOX

both personal and commercial purposes.<sup>17</sup> During 2003, studies showed that anywhere from two billion<sup>18</sup> to twelve billion spam e-mails were sent out each day.<sup>19</sup> In fact, spam made up twelve percent of 2003's one hundred thirty-eight billion dollar Internet commerce market.<sup>20</sup> By January 2004, estimates of the amount of spam running through the system had, somewhat predictably, increased to sixty percent of all e-mail.<sup>21</sup>

Unfortunately, the percentage of spam in inboxes will continue to increase.<sup>22</sup> Part of this extreme growth rate is due to the sharp increase in user e-mail accounts, which are estimated to grow from seven hundred million in 2004 to 1.2 billion in 2005.<sup>23</sup> Considering this, it is not as surprising that a 2003 study estimated that spam would increase sixty-three percent by 2007.<sup>24</sup> This would mean that, only three years from now, almost two trillion spam e-mails will flood U.S. users' inboxes.

In addition, because spammers can make use of around seventy million e-mail addresses for only around one hundred fifty dollars, spammers can afford to hit millions of inboxes with great ease.<sup>25</sup> Despite the bad reputation spam has achieved, eight percent of users still made purchases from spam e-mail in 2003,<sup>26</sup> making spam almost certainly profitable for most spammers. Altogether, this suggests that spam will continue to increase in the years to come and that the price incentive for marketers will likely attract even more spammers in the future.

The financial burden of spam is also quite shocking and, considering the anticipated spam increase, it could become a very heavy burden indeed. One research group recently estimated that the cost of handling spam in the U.S.

<sup>17</sup> CAN-SPAM Act of 2003, §2(a)(1-2) (2003); 15 U.S.C. § 7701(a)(1-2) (2004).

<sup>18</sup> Jon Swartz, *Spam's Irritating Cousin, Spim, on the Loose* (Mar. 1, 2004), USA TODAY.COM, at [http://www.usatoday.com/tech/news/2004-03-01-spim\\_x.htm](http://www.usatoday.com/tech/news/2004-03-01-spim_x.htm).

<sup>19</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

<sup>20</sup> See Rubell, *supra* note 16.

<sup>21</sup> See Press Release, Impact of CAN-SPAM? Brightmail Finds Spam is Still Flowing (Feb. 2, 2004), at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html).

<sup>22</sup> See Mike France, *Needed Now: Laws to Can Spam*, BUS. WK. ONLINE (Sept. 27, 2002), at [http://biz.yahoo.com/bizwk/020927/sb200209265958\\_1.html](http://biz.yahoo.com/bizwk/020927/sb200209265958_1.html).

<sup>23</sup> Lisa Jucca, FORBES, *OECD to Sound International Alarm Bell on Spam* (Feb. 1, 2004), at [http://www.forbes.com/home\\_europe/newswire/2004/02/01/rtr1237398.html](http://www.forbes.com/home_europe/newswire/2004/02/01/rtr1237398.html).

<sup>24</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

<sup>25</sup> See France, *supra* note 22, at [http://biz.yahoo.com/bizwk/020927/sb200209265958\\_1.html](http://biz.yahoo.com/bizwk/020927/sb200209265958_1.html).

<sup>26</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

alone amounts to at least ten billion dollars per year.<sup>27</sup> Spam costs in 2003 for non-corporate Internet users alone added up to two hundred fifty-five million dollars.<sup>28</sup> Additionally, 2002 estimates of spam costs to U.S. corporations totaled close to nine billion dollars.<sup>29</sup>

Not only is spam increasing in number and cost, but the spam phenomenon is also spreading out into other areas of technology. Instant messaging spam, now dubbed “spim,” is a growing threat that creates most of the same problems as spam.<sup>30</sup> Although there is much less spim, estimates show that around one billion spim e-mails were sent out in 2003, four times more than in 2001, and the number is expected to increase to four billion in 2004.<sup>31</sup> The numbers show that spam is not simply a temporary phenomenon, but a real problem that must be confronted quickly, efficiently and effectively before the Internet loses its most important communication tools.

### *B. The Spam Monster*

As we can see from the statistics, spam is not simply a harmless advertising method analogous to commercial letters we receive by post; it is a monster. If spam is so problematic, why doesn't the U.S. simply outlaw it completely? The answer to that makes spam seem an even more challenging enemy. First, free speech concerns play a role in preventing the complete elimination of spam. Second, spam is highly beneficial to advertisers who can reach millions of potential customers at an exceptionally low cost.<sup>32</sup> Third, spam provides users access to information about products they might not otherwise have had. In this sense, spam can be seen to some degree as a technological advance in communication, yet another wonder of the Internet age that can perhaps benefit many. Nonetheless, problems arise because of the heavy burden spam places on the majority of Internet users and Internet Service Providers (ISPs). Legislators find themselves in a situation where, on the one hand, they fear chilling free speech and preventing the desirability of e-mail as a direct marketing medium, while on the other hand, they fear inundating Internet users with useless or deceptive information to the point where the Internet loses all of its advantages. The very heavy burden that spam imposes cannot be ignored, however, and is becoming more obvious with every passing day.

---

<sup>27</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

<sup>28</sup> *See id.*

<sup>29</sup> *See id.*

<sup>30</sup> Swartz, *supra* note 18, at [http://www.usatoday.com/tech/news/2004-03-01-spim\\_x.htm](http://www.usatoday.com/tech/news/2004-03-01-spim_x.htm).

<sup>31</sup> *See id.*

<sup>32</sup> Cindy M. Rice, *The TCPA: A Justification for the Prohibition of Spam in 2002? Unsolicited Commercial E-mail: Why is it Such a Problem?*, 3 *N.C. J. L. & TECH.* 375, 379 (2002).

2004]

SPAM IN A BOX

From a technical perspective, large quantities of spam can indeed be quite hazardous. Voluminous spam consumes large amounts of network bandwidth, memory, storage space and other resources,<sup>33</sup> and can even cause networks to shut down completely.<sup>34</sup> Further, individual users must spend long periods of time reading, deleting, filtering and blocking spam.<sup>35</sup> The ISPs and e-mail services, therefore, must pay to fight spam in order to keep their users. In the end, the users may pay higher Internet rates.<sup>36</sup>

In addition, an inbox full of spam makes it almost impossible for a user to decipher which messages, if any, are commercial messages that the user actually requested or that relate to an actual business transaction, which makes it difficult for such commercial e-mail to reach the user.<sup>37</sup> On the business level, an inbox full of spam can cause problems for workers who often receive e-mail from companies who use commercial subject headers in their e-mails because they cannot easily decipher which e-mails are from their customers and which are spam. Estimates show that fifteen to twenty percent of corporate e-mail consists of spam, totaling over two million spam e-mails yearly in a one thousand person company,<sup>38</sup> and that each spam e-mail wastes on average at least 4.5 seconds of an employee's time. This adds up to at least twenty-five hundred hours per year of wasted time for a relatively small company, and these numbers are likely underestimations since spam is growing and becoming more difficult to weed out from other e-mail. Ultimately, whether due to a virus or to the difficulty of identifying spam, spam causes employee productivity to decrease.

Further, if the unwitting user makes the mistake of opening a harmlessly titled spam e-mail, possibly offensive pornographic content, or even a computer virus may be waiting. In addition, unsuspecting users who click on a link within a spam e-mail might be swept away into a world of scams or illegal activities such as identity and credit card theft.<sup>39</sup> Altogether, spam costs to users and providers are enormous, spam can crash servers and do other

---

<sup>33</sup> See Sorkin, *supra* note 3, at 336.

<sup>34</sup> See Sabra-Anne Kelin, *State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435, 437 (2001).

<sup>35</sup> See Sorkin, *supra* note 3, at 337.

<sup>36</sup> See *id.*

<sup>37</sup> See Jim Krane, *Top Marketing Lobby Seeks Spam Law* (Oct. 22, 2002), at [http://story.news.yahoo.com/news?tmpl=story&u=/ap/20021022/ap\\_on\\_hi\\_te/direct\\_marketers\\_spam\\_2](http://story.news.yahoo.com/news?tmpl=story&u=/ap/20021022/ap_on_hi_te/direct_marketers_spam_2).

<sup>38</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

<sup>39</sup> See Andrea Orr, *NetTrends: Fighting Spam Becomes Top Priority* (Oct. 10, 2002), at [http://story.news.yahoo.com/news?tmpl=story2&cid=575&u=/nm/20021010/wr\\_nm/column\\_netrends\\_dc\\_1&printer=1](http://story.news.yahoo.com/news?tmpl=story2&cid=575&u=/nm/20021010/wr_nm/column_netrends_dc_1&printer=1).

technological harm, spam defeats the effectiveness of commercial e-mails, reduces employee productivity, and can possibly sweep users into a sea of criminal content. Spam truly is a monster of a problem.

### III. THE HISTORY OF ANTI-SPAM TACTICS

#### *A. Self-Regulation and Technical Tactics to Combat Spam*

Many self-regulation tactics as well as technical tactics with which to combat the spam monster have emerged as spam has grown more problematic. Individual users, ISPs and specialized anti-spam groups often employ self-regulation mechanisms to prevent spam.<sup>40</sup> ISPs have begun to face a reality in which they must make changes in order to keep their users happy. Industry groups representing marketers and ISPs have responded to spam by posting use policies.<sup>41</sup> For example, members of the Direct Marketing Association (“DMA”), a trade association representing users and suppliers, must comply with the DMA’s “Privacy Promise,” which prohibits the sending of spam to addresses that appear in the DMA’s e-Mail Preference Service database.<sup>42</sup> Many spammers, however, can evade these attempts at self-regulation by simply ignoring the policies and, because the Internet is so difficult to monitor, the spammers often face little risk of punishment.

Recognizing the failure of self-regulation, most e-mail services now include some type of automatic spam filter.<sup>43</sup> Today, users can automatically filter out spam sent by known spammers by placing spammers on a “blacklist” that is created by a whole ISP or e-mail service community.<sup>44</sup> Some services, upon a user’s request, automatically place e-mail sent by a spammer on the blacklist in a user’s “bulk inbox” rather than the regular inbox so that the user can easily identify the e-mail as spam and delete the bulk inbox’s contents in less time.<sup>45</sup> If the e-mail service for some reason does not place the identified spammer on a blacklist, however, a user may continue to receive mail from that spammer.

---

<sup>40</sup> See Sorkin, *supra* note 3, at 344.

<sup>41</sup> See *id.* at 342.

<sup>42</sup> See *id.*

<sup>43</sup> See *id.* at 345.

<sup>44</sup> See Dianne P. Latham, *Electronic Commerce in the 21st Century: Article Spam Remedies*, 27 WM. MITCHELL L. REV. 1649, 1650 (2001).

<sup>45</sup> Yahoo mail works this way. See Yahoo, *Yahoo! Mail* (Sept. 7, 2003), at <http://help.yahoo.com/help/us/mail/spam/spam-08.html>. For example, Yahoo offers its users the option of either blocking an address, which it describes as “less effective” because it prevents delivery of only a single e-mail address and “spammers frequently change their e-mail address,” as well as an option to report the message, which is “more effective” because it sends the message to the “Yahoo! Customer Care to review and improve [its] SpamGuard™.” See Yahoo, *Yahoo! Mail* (Aug. 29, 2003), at <http://help.yahoo.com/help/mail/>.

2004]

*SPAM IN A BOX*

The user can then report the spam and place the spammer on the blacklist, or the user can choose to automatically delete a specific address or filter out certain keywords that show up in the line of undesired e-mails (sexually explicit words, for example).<sup>46</sup>

Automatic filters, however, have many costs as well as benefits that both companies and individuals should consider. Almost all filters result in some false positives, i.e., the blocking out of legitimate e-mail or the automatic sending of legitimate e-mail to a bulk inbox.<sup>47</sup> This is a risk that is especially high for companies, but one that companies must accept if they use the currently available services. E-mail services, which admit that they sometimes filter non-spam e-mails to users' bulk inboxes by mistake, usually offer the user a method by which to indicate that the e-mail is not spam and thus take it off the spam blacklist.<sup>48</sup> This spam identifying process takes time and effort. Even if users diligently report spam instead of simply deleting it, which takes at least one extra click, a user must search through the entire bulk inbox to ensure the service did not block out any legitimate e-mail. In order to identify legitimate e-mail that the service mistakenly identifies as spam, as it admittedly does, the user must browse through his "bulk inbox," spending as much time as would take to search through a typical inbox full of spam.<sup>49</sup>

Not only do the current filtering systems take time and effort, but they also fail to provide a truly effective barrier against spammers. Spam will continue to slip through these filters despite the e-mail services' best efforts. Since spammers know of these filtering devices, they use sender names that are ambiguous and constantly switch to or add new sender addresses to avoid these blacklists and anti-spam tactics.<sup>50</sup> Spammers also often "hijack" the business or personal computers of unwitting users in order to disguise their tracks.<sup>51</sup> Because spammers soon create technology to circumvent any advances in filter technology and because of the high cost of filtering technologies, spam is a heavy burden on service providers who must bear its invasion of their valuable server capacity.<sup>52</sup> Further, destination operators and intermediate networks must devote bandwidth and storage capacity to the received message despite

---

<sup>46</sup> Yahoo mail offers these options. See *id.*, at <http://help.yahoo.com/help/us/mail/spam/spam-08.html>.

<sup>47</sup> See Sorkin, *supra* note 3, at 345-46.

<sup>48</sup> See Yahoo, *supra* note 45, at <http://help.yahoo.com/help/us/mail/spam/spam-08.html>.

<sup>49</sup> See *id.*, at <http://help.yahoo.com/help/us/mail/spam/spam-08.html>.

<sup>50</sup> See Sorkin, *supra* note 3, at 346-48.

<sup>51</sup> See Paul Rubell, *supra* note 16; see also Greg Wright, *With anti-spam law in effect, companies work to foil junk e-mail* (Feb. 25, 2004), at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantisamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantisamlawineffectcompaniesworktofoiljunkemail).

<sup>52</sup> See Sorkin, *supra* note 3, at 347-48.

filter mechanisms.<sup>53</sup> The adamant anti-spammer, therefore, will soon recognize the need for legal tactics to combat spam.

*B. Various Legal Tactics Used to Combat Spam*

Many laws have been created or used to prevent spam. Prior to the new U.S. federal legislation, an array of laws existed under which spammers could possibly be liable: the Lanham Act for false designation of origin and dilution of interest in service marks, state and common law unfair competition laws, the Computer Fraud and Abuse Act for exceeding authorized access and impairing facilities.<sup>54</sup> In addition, spammers could be liable for violation of state computer crimes acts, for using deceptive trade practices, for defamation, fraud, forgery, harassment, theft, libel, breach of contract, false statements in advertising and common law trespass to chattels.<sup>55</sup>

Those who wished to combat spammers in court using such causes of action have generally been successful in obtaining injunctions as long as they can identify the source of the spam and the spammer used some kind of deceptive practice.<sup>56</sup> Case law suggests at least that an e-mail provider, if not the end-user, may prevail on several different non-spam specific theories of liability against spammers who deceptively identify themselves. Certainly, case law indicates that, if a spammer is using a company's marks or name, the company has a cause of action available.<sup>57</sup> Many online service providers, such as AOL, have shown that they are prepared to take court action against spammers.<sup>58</sup>

---

<sup>53</sup> See *id.* at 347.

<sup>54</sup> See Latham, *supra* note 44, at 1651.

<sup>55</sup> See *id.*

<sup>56</sup> See *id.*

<sup>57</sup> See *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998). In 1998, America Online ("AOL") sued LCGM, Inc. because it was using "aol.com" in the "from" line of the e-mails, making members believe that AOL was the sender. The court granted AOL's summary judgment motion for a number of claims, including false designation of origin, dilution of interest in service marks under the Lanham Act, exceeding authorized access and impairing computer facilities in violation of the Computer Fraud and Abuse Act, violating the Virginia Computer Crimes Act and engaging in Virginia common law trespass to chattels. See also *Hotmail Corp. v. Van Money Pie, Inc.*, 47 U.S.P.Q.2d (BNA) 1020 (N.D. Cal. 1998). Here, Hotmail successfully claimed under theories of false designation of origin, federal and state dilution of a mark, violation of the Computer Fraud and Abuse Act, state and common law unfair competition, breach of contract, fraud and misrepresentation, and trespass to chattels.

<sup>58</sup> See *Am. Online, Inc. v. CN Productions, Inc.*, 272 B.R. E.D. Va. 879 (2002). In January 2002, AOL brought suit against CN Productions ("CN") after CN bombarded AOL users with pornographic spam. AOL had previously won an injunction against CN for swamping AOL users with e-mails advertising adult Internet sites. Here, AOL claimed CN had violated the court's injunction by sending more than a billion unwanted pornographic e-mails, resulting in more than eight million in earnings. AOL walked away with almost

2004]

SPAM IN A BOX

Even under the U.S.'s new federal legislation, state laws not specific to e-mail, including common law causes of action and laws that relate to fraud or computer crime, are not preempted.<sup>59</sup> This leaves many of the above causes of action open for future use.

In Japan, NTT DoCoMo ("Docomo"), Japan's largest service provider, like AOL, showed that it too was ready to take action against spammers despite the unfavorable spam laws at the time, but only in dire situations. In the first legal action against spammers in Japan, Docomo filed suit in the Yokohama District Court against Global Network, a cell phone spammer who was sending hundreds of thousands of randomly generated spam to Docomo customers.<sup>60</sup> On June 8, 2001, around nine hundred thousand spam messages were sent within one hour early in the day and another three hundred thousand within one hour later the same day.<sup>61</sup> Docomo decided to act before the spam caused technical problems and, on July 27, after Global Network and another firm ignored Docomo's warnings, Docomo filed a complaint requesting a provisional order to halt the spam.<sup>62</sup> At that time, the law required Docomo to maintain confidentiality of the communications that flowed through its devices and prohibited it from reading the contents of any e-mail, making it exceedingly difficult to discern spam from legitimate e-mail.<sup>63</sup> The Court in this case, however, issued an injunction.<sup>64</sup>

As the spam issue gained momentum in the U.S., many states enacted specific anti-spam laws. In 1997, Nevada became the first state to pass anti-spam legislation and, as of 2003, thirty-five states had followed suit,<sup>65</sup> most

---

seven million in statutory damages after the court's ruling. Randall Boe, executive Vice President and General Counsel of AOL, stated that this was "an important legal victory in the fight against spam and it sends the clear and distinct message to spammers that AOL is prepared to use all of the legal and technological tools available to shut down spammers who inundate AOL users' inboxes with unwanted and often offensive junk e-mail." See Tim Richardson, *AOL Wins \$7m in Porn Spam Case* (Dec. 17, 2002), at <http://www.theregister.co.uk/content/6/28600.html>.

<sup>59</sup> See Kennedy & Lyon, *supra* note 4.

<sup>60</sup> See *Court Issues Injunction on DoCoMo Spammer*, JAPAN TIMES ONLINE (Oct. 31, 2001), at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20011031a4.htm>.

<sup>61</sup> See *id.*

<sup>62</sup> See *id.*

<sup>63</sup> See *id.*

<sup>64</sup> See *id.*

<sup>65</sup> These states include Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin and Wyoming. See David E. Sorkin, *Spam Laws* (May 31, 2003), at <http://www.spamlaws.com/state/index.html>. See also Kelin, *supra* note 34, at 444.

requiring an opt-out mechanism and a subject label such as “ADV.”<sup>66</sup> Specifically, most of the laws regulated the information conveyed in the return address and the header.<sup>67</sup> Many of the laws allowed ISPs and sometimes even recipients to sue erring spammers for damages or injunctions.<sup>68</sup> Despite possible suits,<sup>69</sup> spammers responded by deliberately providing false information to hide their identities and generally improving their legal evasion techniques.<sup>70</sup> California, therefore, chose to adopt the stronger opt-in system to stop spam, but this law was preempted by the new and weaker federal legislation.<sup>71</sup>

Despite the case law in the U.S. that seems to favor of the victims of spam, most successful suits<sup>72</sup> have involved blatant violations, such as sending messages with forged headers, unauthorized third-party relaying and refusal to comply with opt-out demands.<sup>73</sup> Similarly, Docomo’s victory was more likely due to the actual system failure that Docomo experienced, rather than any other reason, which shows that other parts of the world were also having difficulty dealing with spammers without broader laws or federal legislation in place.<sup>74</sup>

Nonetheless, the U.S. cases together implied that an efficient system of communication between businesses, which would alert companies when their name or mark is used improperly, coupled with the laws could help significantly reduce spam.<sup>75</sup> The more successful suits companies bring

---

<sup>66</sup> *See id.*

<sup>67</sup> *See* Kelin, *supra* note 34, at 444.

<sup>68</sup> *See id.*

<sup>69</sup> In *Individual Investor Group, Inc. v. Howard*, a company once again prevailed against a spammer. In this case, the plaintiffs sued under Nevada’s Electronic Mail Statute. NEV. REV. STAT. 41.705-41.735 (2000). Howard sent spam that contained an inaccurate return address as well as the Individual Investor Group’s trademarks and Internet domain names, giving the impression that the Group was responsible for the spam. In January 2000, the Group obtained a settlement including a permanent injunction, five thousand dollars in payment, a public apology and an agreement by Howard to assist the Group in clearing its name from spam blacklists. *See* Press Release, Brown Raysman Millstein Felder & Steiner LLP, Brown Raysman Millstein Felder & Steiner LLP Obtains An Injunction And Public Apology In Internet “Spamming” Lawsuit (Jan. 27, 2003), at <http://www.brownraysman.com/firm/press/spam.html>.

<sup>70</sup> *See* Kelin, *supra* note 34, at 445.

<sup>71</sup> *See* Cal. Bus. & Prof. Code 17529 (2003).

<sup>72</sup> *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d at 444.; *Hotmail Corp.*, 47 U.S.P.Q.2d (BNA) at 1020; Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

<sup>73</sup> Sorkin, *supra* note 3, at 356.

<sup>74</sup> *See id.*

<sup>75</sup> If Company A (or perhaps also an individual user, though this is less clear in the case law) is continuously receiving spam from a certain spammer and has reason to believe the spammer is incorrectly identifying itself as Company X, it should certainly bring the

2004]

SPAM IN A BOX

against spammers, the greater the overall deterrent effect. If companies are willing to communicate their concerns to others or to take strong legal action themselves, then they would certainly have a much greater chance of success in decreasing the amount of incoming spam.

It is unlikely, however, that such an information exchange will occur on a large enough scale to create the necessary deterrent effect and, even if it does, the burden of overflowing inboxes and the high cost of handling spam, in addition to the burden of taking legal action, suggest that a only a low-level deterrent effect is not enough. Even if it were enough, spammers would find ways to avoid falling within the sphere of the case law, or they would simply choose to ignore the law in hopes of not being brought to court. This leaves the victims of spam with very little choice except to look for additional ways to proceed against spammers, such as developing more creative self-help methods to deal with spam,<sup>76</sup> or waiting patiently and hopefully for truly effective federal legislation to pass. Although some self-help tactics could be satisfying for those who considered it their mission to bring down spammers,<sup>77</sup> when one

---

spammer to the attention of its e-mail service provider or ISP as well as to the attention of Company X. Company A should do this because, though Company A likely has no direct cause of action against the spammer, Company X will likely prevail in court. If Company X prevails, Company A will receive less spam (at least from that particular spammer) and would, without much effort, contribute to the fight against spam.

<sup>76</sup> See Michael Singer, *Stopping Spam with Poetry and the Law* (Aug. 21, 2002), at <http://siliconvalley.internet.com/news/article.php/1449851>. One Silicon Valley startup developed its own version of "poetic" justice by requiring its clients to embed a trademarked and copyrighted haiku poem in the headers of the e-mails that they send to the company. The company's plan was to block out via filter any e-mail that did not contain the haiku: "winter rainy day/playing in the big puddle/water everywhere." The spammer would have to reproduce both the trademark and the copyright in the header to avoid the filter, making them liable for infringement, though the functionality of the haiku might weaken the copyright and trademark claims. The company could thus sue under trademark and copyright law, and possibly win penalties of up to one million dollars or more, injunctions and criminal penalties. Although this strategy might seem to be both innovative and, to some degree, effective, one must question its commercial desirability. The company who employs these tactics would necessarily risk blocking out e-mail from new clients, and online advertising would be difficult because spammers could gain access to the needed haiku password. In addition, this system would require licenses in order to do business or even potential business with a company (a simple e-mail inquiry) and customers would find this to be overly burdensome (Under this arrangement, A owns the haiku and licenses it Company B, who sublicenses it to customers X, Y, Z, etc. These licenses require X, Y and Z to promise not to send any spam e-mails to Company B). In the end, this self-help method might cost the company even more through lost customers than it would if they continued sorting through spam e-mail.

<sup>77</sup> See Tim Richardson, *Spammer Gets Junk Mailed* (Dec. 11, 2002), at <http://www.theregister.co.uk/content/6>

/28525.html. More recently, anti-spammers took the offensive by signing up bulk e-mailer,

looks beneath the surface, they are nothing more than a desperate cry, a clear signal that users, service providers and businesses everywhere were desperate for effective federal legislation.

*C. Attempts at Federal Spam Legislation Prior to the 108th Congress*

Indeed, Congress heard the cry from the many Americans who had grown to hate spam.<sup>78</sup> During the 106<sup>th</sup> Congress, eleven bills were introduced that related to spam, but none of them passed into law.<sup>79</sup> Again, in the 107<sup>th</sup> Congress, eight spam bills were introduced, showing the persistent nature of the spam issue.<sup>80</sup> The bills dealt with issues such as false identification

---

Alan Ralsky, for multiple spam e-mail lists. Alan Ralsky, a spammer who made millions by sending out up to a billion e-mails per day, ironically, became the one flooded by incoming spam. Alan Ralsky, however, views this taste-of-your-own medicine tactic as nothing more than harassment, and he may have a point, especially considering the anti-spammers of Slashdot went so far as to post online an aerial view of his neighborhood. It is highly unlikely that the solution to the spam problem will come in the form of an offensive battle between spammers and anti-spammers. Instead, such tactics would likely escalate the situation, leading to even more aggressive tactics on both sides in an effort to defend what each group considers to be "right."

<sup>78</sup> If one simply recalls [www.elated.com](http://www.elated.com)'s online computer game "Spamwars", similar to the "Torture a Spammer" game (*see infra* note 275) that found such popularity in Japan. *See* Jennifer Lee, *Something Fun: A Torture Chamber for Spammers*, N.Y. TIMES, Sept. 30, 2002, at C3. In Elated's game, the player battles against "evil Sid the Spammer" who is "intent on spamming you to death." Of course, you can fight back by "shooting the spams before they reach your computer." *See* Elated Communications, Ltd., *Sick of Spam?* (Jan. 1, 2003), at <http://www.elated.com/spamwars/>. Congress is playing this game in reality, though it has yet to achieve victory.

<sup>79</sup> These bills were the CAN SPAM Act, H.R. 2162, 106th Cong. (1999); the E-Mail User Protection Act, H.R. 1910, 106th Cong. (1999); the Inbox Privacy Act of 1999, S. 759, 106th Cong. (1999); the Internet Freedom Act, H.R. 1686, 106th Cong. (1999); the Internet Growth and Development Act of 1999, H.R. 1685, 106th Cong. (1999); the Netizens Protection Act of 1999, H.R. 3024, 106th Cong. (1999); the Protection Against Scams on Seniors Act of 1999, H.R. 612, 106th Cong. (1999); the Telemarketing Fraud and Seniors Protection Act, S. 699, 106th Cong. (1999); Unsolicited Electronic Mail Act of 1999, H.R. 3113, 106th Cong. (1999); the Telemarketing Fraud and Seniors Protection Act of 1999, S. 2542, 106th Cong. (2000); and the Wireless Telephone Spam Protection Act, H.R. 5300, 106th Cong. (2000). *See* David E. Sorkin, *Spam Laws* (May 31, 2003), at <http://www.spamlaws.com/federal/list107.html>.

<sup>80</sup> The bills are: The Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001); the Wireless Telephone Spam Protection Act, H.R. 113, 107th Cong. (2001); the Anti-Spamming Act of 2001, H.R. 718, 107th Cong. (2001); the Anti-Spamming Act of 2001, H.R. 1017, 107th Cong. (2001); the Who Is E-Mailing Our Kids Act, H.R. 1846, 107th Cong. (2001); the Protect Children From E-Mail Smut Act of 2001, H.R. 2472, 107th Cong. (2001); the Netizens Protection Act of 2001, H.R. 3146, 107th Cong. (2001); and the "CAN SPAM" Act of 2001, S. 630, 107th Cong. (2001). *See* Sorkin, *supra*

2004]

*SPAM IN A BOX*

information and sexually explicit spam.<sup>81</sup> One point on which the bills varied revolved around whether they would apply to unsolicited bulk commercial e-mail, unsolicited bulk e-mail, unsolicited commercial e-mail, or a combination, and whether or not they completely preempt state law.<sup>82</sup> Again, none of the bills passed.<sup>83</sup> In comparison, the E.U.'s legislation applies to any e-mail that is sent for the purposes of direct marketing, whether in bulk or not, and required member states to comply with the provisions.<sup>84</sup>

The bills included several other provisions, the ideas of which would also continue into the next Congress. Three of the bills required spammers to provide effective opt-out instructions and two required spam labels.<sup>85</sup> One bill even created criminal liability for failing to label sexually-oriented spam.<sup>86</sup> One bill was amended to prohibit spammers from using e-mail addresses that they harvested from web sites in violation of posted restrictions,<sup>87</sup> while another bill prohibited spammers from using a provider's facilities to send spam in violation of the provider's posted policies.<sup>88</sup> One bill, the Netizen bill, required ISPs to notify their customers of their spam policies and introduces the interesting spam provision that would allow Internet providers to sue customers who violate their spam policies.<sup>89</sup> Finally, the Wireless Telephone Spam Protection Act addressed cellular phone spam by completely prohibiting the use of wireless messaging systems to send any unsolicited advertisements.<sup>90</sup>

Altogether, the U.S. spam bills in the 107th Congress provided a concrete framework for the major themes that appeared in the 108th Congress. The

---

note 79, at <http://www.spamlaws.com/federal/list107.html>.

<sup>81</sup> Anti-Spamming Act of 2001, H.R. 1017, 107th Cong. (2001); "CAN SPAM" Act of 2001, S. 630, 107th Cong. (2001); Netizens Protection Act of 2001, H.R. 3146, 107th Cong. (2001); The Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).

<sup>82</sup> House Report 1017 applies to unsolicited commercial bulk e-mail, Senate Bill 630 and House Report 95 apply to unsolicited commercial e-mail, House Report 718 only applies to unsolicited bulk e-mail, and one part of House Report 3146 applies to any unsolicited e-mail while another part only applies to unsolicited bulk e-mail.

<sup>83</sup> See Sorkin, *supra* note 79, at <http://www.spamlaws.com/federal/list107.html>.

<sup>84</sup> Council Directive 2002/58, *supra* note 9, at Art. 13, Art. 17.

<sup>85</sup> "CAN SPAM" Act of 2001, S. 630, 107th Cong. (2001); Netizens Protection Act of 2001, H.R. 3146, 107th Cong. (2001); The Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).

<sup>86</sup> Anti-Spamming Act of 2001, H.R. 1017, 107th Cong. (2001).

<sup>87</sup> "CAN SPAM" Act of 2001, S. 630, 107th Cong. (2001).

<sup>88</sup> The Unsolicited Commercial Electronic Mail Act of 2001, H.R. 95, 107th Cong. (2001).

<sup>89</sup> Netizens Protection Act of 2001, H.R. 3146, 107th Cong. (2001).

<sup>90</sup> See Sorkin, *supra* note 79, at <http://www.spamlaws.com/federal/list107.html>.

107th bills paved the way to the enactment of the first federal anti-spam legislation in U.S. history, the first step in the war against spam.

#### IV. THE CURRENT FEDERAL LEGISLATION

##### *A. The 108th Congress*

###### 1. Bills Introduced, But Not Passed

The flurry of spam bills continued in 2003 as Congress introduced nine spam-related bills in the 108th Congress, eight of which it did not pass.<sup>91</sup> Six of the bills showed a continued concern with, and directly prohibited, falsified identification information in e-mail headers.<sup>92</sup> As in the 107th Congress, the definition of spam was a point of difference among the bills. This time around, three bills targeted unsolicited commercial e-mail,<sup>93</sup> two targeted all commercial e-mail,<sup>94</sup> two targeted unsolicited bulk commercial e-mail,<sup>95</sup> and one targeted all bulk commercial e-mail.<sup>96</sup> In addition, the bills dealt again with the question of preemption of state laws.<sup>97</sup> Glaringly apparent was the

---

<sup>91</sup> The bills that did not pass were: CAN-SPAM Act of 2003, S. 877, 108th Cong. (2003); Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003); Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, S. 1052, 108th Cong. (2003); Computer Owners' Bill of Rights, S. 563, 108th Cong. (2003); Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003); Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003); REDUCE Spam Act of 2003, H.R. 1933, 108th Cong. (2003); Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003); Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003). See Sorkin, *supra* note 79, at <http://www.spamlaws.com/federal/list107.html>.

<sup>92</sup> These bills were: Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003); Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003); REDUCE Spam Act of 2003, H.R. 1933, 108th Cong. (2003); Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003); Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, S. 1052, 108th Cong. (2003); Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003).

<sup>93</sup> Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003); Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003); Computer Owners' Bill of Rights, S. 563, 108th Cong. (2003).

<sup>94</sup> Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003); Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003).

<sup>95</sup> REDUCE Spam Act of 2003, H.R. 1933, 108th Cong. (2003); Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, S. 1052, 108th Cong. (2003).

<sup>96</sup> Criminal Spam Act of 2003, S. 1293, 108th Cong. (2003).

<sup>97</sup> The Reduction in the Distribution of Spam Act and the Anti-Spam Act require that state laws that prohibit unsolicited commercial e-mail or commercial e-mail, respectively, in addition to regulating opt-out procedures, or requiring subject-line labels would be preempted, while state laws that merely regulate the falsification of message headers would remain in effect. Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong.

2004]

SPAM IN A BOX

lack of opt-in procedures among the bills. Four bills required some type of standard opt-out procedure,<sup>98</sup> while two bills required a new national registry that the public could use to opt-out.<sup>99</sup> The bills also introduced various provisions that required labeling<sup>100</sup> and adherence to ISP policies.<sup>101</sup> Some bills prohibited harvesting<sup>102</sup> and one prohibited wireless phone spam.<sup>103</sup>

2. The CAN-SPAM Act of 2003

For six years prior to the CAN-SPAM Act (“CAN-SPAM” or the “Act”), Congress debated the need for federal legislation.<sup>104</sup> CAN-SPAM, originally dubbed the Burns-Wyden Act because Republican Senator Burns of Montana and Democratic Senator Wyden of Oregon introduced it in April 2003, is the only federal anti-spam legislation that Congress has passed into law.<sup>105</sup> CAN-SPAM was based in part on at least five bills: the CAN SPAM Act of 2001,<sup>106</sup> the Stop Pornography and Abusive Marketing Act,<sup>107</sup> the Criminal Spam Act,<sup>108</sup> the REDUCE Spam Act,<sup>109</sup> and the Ban on Deceptive Unsolicited Bulk

---

(2003); Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003).

<sup>98</sup> Anti-Spam Act of 2003, H.R. 2515, 108th Cong. (2003); Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003, S. 1052, 108th Cong. (2003); REDUCE Spam Act of 2003, H.R. 1933, 108th Cong. (2003); Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Cong. (2003).

<sup>99</sup> Stop Pornography and Abusive Marketing Act, S. 1231, 108th Cong. (2003); Computer Owners’ Bill of Rights, S. 563, 108th Cong. (2003).

<sup>100</sup> The Stop Pornography and Abusive Marketing Act, the Reduction in Distribution of Spam Act, the Anti-Spam Act, and the REDUCE Spam Act all require labels that to be clear and conspicuous or a standard “ADV” label.

<sup>101</sup> The Stop Pornography and Abusive Marketing Act makes it illegal to send any commercial e-mail in violation of an Internet service provider’s policies.

<sup>102</sup> The Stop Pornography and Abusive Marketing Act, the Reduction in Distribution of Spam Act, the Ban on Deceptive Unsolicited Bulk Electronic Mail Act and the Anti-Spam Act all do this in some way.

<sup>103</sup> Wireless Telephone Spam Protection Act, H.R. 122, 108th Cong. (2003).

<sup>104</sup> See Amalia Deligiannis, *Anti-Spam Law Burdens Businesses, Not Spammers-Legal Experts Warn CAN-SPAM Law Won’t Eliminate Junk E-Mail*, CORP. LEGAL TIMES, Mar. 2004, at 16.

<sup>105</sup> See Sorkin, *supra* note 79, at <http://www.spamlaws.com/federal/list107.html>. CAN-SPAM Act, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. 7701 -13; 18 U.S.C. 1001, 1037; 28 U.S.C. 994; and 47 U.S.C. 227).

<sup>106</sup> S. 630 (2001).

<sup>107</sup> This bill was worked into an amendment to CAN-SPAM (S.AMDT.1892) ordering a six-month study of a national do-not-spam registry. *Numerous Spam Bills Find Home in Senate-Clearing Package*, Wash. Internet Daily, Oct. 24, 2003, Vol. 4, Issue 206, available at 2003 WL 16118519.

<sup>108</sup> See *id.* Pushed for by the proponents of REDUCE, Republican Senator Hatch and Democrat Senator Leahy. The original CAN-SPAM bill categorized false header

Electronic Mail Act.<sup>110</sup> The Senate approved the final version of the Act ninety-seven to zero in November 2003, and the House of Representatives approved it three hundred ninety-two to five in December 2003.<sup>111</sup> President Bush signed the law on December 16, 2003 and it became effective as of January 1, 2004.<sup>112</sup>

The purpose of the Act is “To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.”<sup>113</sup> CAN-SPAM aims to accomplish this task through several main provisions. The Act prohibits the sending of multiple<sup>114</sup> commercial e-mails with the intent to mislead or deceive recipients.<sup>115</sup> The Act also prohibits the use of deceptive subject line information,<sup>116</sup> falsified

---

information as a misdemeanor, but the Hatch-Leahy amendment upgraded this to a felony sentence of up to five years’ imprisonment while a spammer who used someone else’s computer would face three years’ imprisonment. The amendment also adds the Department of Justice as an enforcement agency. In addition, the amendment restricts the number of domain names a spammer could register in order to make it easier to block spammers by domain name categorizes as a felony the transmission of more than twenty-five hundred e-mails in a twenty-four hour period, twenty-five thousand in thirty days or two hundred fifty thousand in one year. Senator Hatch argued that children open pornographic e-mails and seniors’ are scammed by fraudulent health care spam, as well as ID theft.

<sup>109</sup> *See id.* The amendment based on this bill, both of which were called for by the Democratic Senator Corzine of New Jersey, directs the Federal Trade Commission to develop a system for rewarding those who supply information about violations of this Act and a system for requiring ADV labeling on unsolicited commercial electronic mail. S.AMDT.1896. The original bill, based on an idea first proposed by Stanford professor Lawrence Lessig, would have had the F.T.C. create a bounty system, rewarding people who reported fraudulent spammers if such a report led to a fine. This amendment diluted the original bill while in negotiations with the bill’s sponsors to instead request a report from the F.T.C. on the subject within nine months of the bill’s enactment.

<sup>110</sup> *See id.* The Hatch-Leahy amendment also worked in the language of this bill, which called on the U.S. Sentencing Commission consider enhanced sentences for spammers who committed fraud or identity theft, or who sent child pornography.

<sup>111</sup> Declan McCullagh, *House Passes Antispam Bill*, CNET News.com, at <http://news.com.com/2100-1024-51106222.html> (Nov. 22, 2003).

<sup>112</sup> *See* Peter J. Pizzi & M. Trevor Lyons, *Opting In: Congress Passes the CAN-SPAM Act of 2003* (February 17), at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>113</sup> CAN-SPAM Act, Pub. L. No. 108-187, 117 Stat. 2699 (2003).

<sup>114</sup> “Multiple” here means more than one hundred electronic mail messages during a twenty-four hour period, more than one thousand electronic mail messages during a thirty-day period, or more than ten thousand electronic mail messages during a 1-year period. 18 U.S.C. § 1037(d)(3) (2004).

<sup>115</sup> 18 U.S.C. § 1037(a)(2).

<sup>116</sup> 15 U.S.C. § 7704(a)(2) (2004). The statute prohibits a 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

2004]

*SPAM IN A BOX*

header information,<sup>117</sup> or falsified e-mail account registration information.<sup>118</sup> In addition, the Act also prohibits one from falsely representing that one is the registrant of five or more Internet Protocol addresses from which one initiates the transmission of multiple commercial messages.<sup>119</sup>

The provision of the Act that likely receives the most attention is the one that requires a functioning return e-mail address or comparable Internet-based mechanism by which a recipient can opt-out.<sup>120</sup> The Act prohibits the transmission of commercial e-mail more than ten days after the receipt of the recipient's opt-out request.<sup>121</sup> These e-mails must also include a clear and conspicuous notice of the availability of the opt-out mechanism,<sup>122</sup> a clear and conspicuous label that it is an advertisement or solicitation,<sup>123</sup> the sender's valid physical postal address,<sup>124</sup> and a subject line label identifying sexually oriented commercial e-mail as such.<sup>125</sup>

---

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. . .”

<sup>117</sup> 18 U.S.C. § 1037(a)(3). CAN-SPAM amends Chapter 47 of Title 18, U.S.C. by adding Section 1037, which deals with fraud and related activity in connection with e-mail. CAN-SPAM Act of 2003, S. 877, 108th Cong. (2003). The statute defines “header information” as “the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.” 15 U.S.C. § 7702 (2004). A different section of the statute prohibits sending ANY e-mail with either materially false or materially misleading header information to a protected computer. 15 U.S.C. § 7704(a)(1).

<sup>118</sup> 18 U.S.C. § 1037(a)(4). Under a different section, the statute prohibits the automated creation of multiple electronic mail accounts, making it “unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful” under the provisions in 15 U.S.C. § 7704(a), such as failing to include the proper opt-out procedure. 15 U.S.C. § 7704(b)(2).

<sup>119</sup> 18 U.S.C. § 1037(a)(5).

<sup>120</sup> 15 U.S.C. § 7704(a)(3)(A). The opt-out mechanism can consist of a list of choices so that a user can choose to receive certain kinds of commercial e-mail, as long as there is an option to opt-out of all such e-mail from that sender. 15 U.S.C. § 7704(a)(3)(B).

<sup>121</sup> 15 U.S.C. § 7704(a)(4)(A). Also, a sender may not sell, lease, exchange or otherwise transfer the opted-out of address. The ten day time period is subject to revision if it is determined by the F.T.C. to unreasonable. 15 U.S.C. § 7704(c).

<sup>122</sup> 15 U.S.C. § 7704(a)(5)(A)(ii).

<sup>123</sup> 15 U.S.C. § 7704(a)(5)(A)(i).

<sup>124</sup> 15 U.S.C. § 7704(a)(5)(A)(iii).

<sup>125</sup> 15 U.S.C. § 7704(d)(1)(A). In addition, the sexually oriented e-mail cannot have the sexually oriented matter in the material that is initially viewable to the recipient when the message is opened and must make this clear to the recipient in the e-mail description

CAN-SPAM also outlaws the unauthorized access and use of third-party computer systems, which are often used by spammers in order to hide the origin of the spam so as to avoid blacklisting.<sup>126</sup> In addition, the Act prohibits harvesting and dictionary searches in violation of posted website notices, but only if used to send spam that violates other provisions.<sup>127</sup> The principle authority that will enforce CAN-SPAM is the Federal Trade Commission (F.T.C.), although ISPs and state attorney generals can also file suit.<sup>128</sup> Penalties for violation can consist of fines, imprisonment, both, and/or damages.<sup>129</sup> The Act preempts most state law provisions except for those prohibiting falsity and deception in e-mails.<sup>130</sup> The Act does not preempt state laws not specific to e-mail, including state trespass, contract, or tort law.<sup>131</sup>

CAN-SPAM also contains several provisions that require study for future determinations.<sup>132</sup> For example, the Federal Communications Commission (F.C.C.) has two hundred seventy days to make rules to protect consumers from unwanted mobile service commercial messages.<sup>133</sup> Interestingly, the rules at first seem to require much stronger provisions for wireless than for e-mail, requiring what appears to be a quasi-opt-in procedure.<sup>134</sup> Of course, this

---

viewable before opening. 15 U.S.C. § 7704(d)(1)(B). Strangely, Section (d)(2) creates a loophole because failure to opt-out of the receipt of the sexual spam negates the above obligations. This loophole would not exist with an effective opt-in system.

<sup>126</sup> 18 U.S.C. § 1037(a)(1); 15 U.S.C. § 7704(a)(1)(c); 15 U.S.C. § 7704(b)(3). *See* Wright, *supra* note 51, *at* [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withanti-spamlawineffect-companiesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withanti-spamlawineffect-companiesworktofoiljunkemail).

<sup>127</sup> 15 U.S.C. § 7704(b)(1). In other words, a sender who harvested an e-mail and uses it to send a message that complies with the Act's requirements by including an identifier, opt-out mechanism and notice, physical address, opt-out, etc. is not in violation of the harvesting provision. In addition, the statute prohibits offenders who have harvested e-mail addresses knowingly or with knowledge fairly implied by objective circumstances that the e-mail address was obtained using an automated means from an Internet website or proprietary online service operated by another person, and the website or service had posted a notice stating the operator would not give, sell or transfer addresses maintained on the website to any party who will use them to send spam. It also prohibits e-mail addresses that were obtained using an automated means that generates possible addresses by combining names, letters or numbers in various permutations. Harvesting may lead to an enhanced sentence. 15 U.S.C. § 7703(a)(2)(A)(i) (2004).

<sup>128</sup> 15 U.S.C. § 7706 (2004).

<sup>129</sup> 15 U.S.C. § 7703, § 7706.

<sup>130</sup> 15 U.S.C. § 7707(b)(1) (2004).

<sup>131</sup> 15 U.S.C. § 7707(b)(2).

<sup>132</sup> *See* Kennedy & Lyon, *supra* note 4 (discussing in depth the provisions of the new Act and future determinations that are required).

<sup>133</sup> 15 U.S.C. § 7712(b) (2004).

<sup>134</sup> The F.C.C. "shall" "provide subscribers to commercial mobile services the ability to

2004]

*SPAM IN A BOX*

is tempered by a provision requiring the F.C.C. to make a determination as to whether the nature of the provider and subscriber relationship is such that only an opt-out procedure should be required.<sup>135</sup>

Another example of a required study authorizes, but does not require, Congress to create a national do-not-email registry.<sup>136</sup> The conclusions of the registry study are due to come out in June 2004 and the F.T.C. must decide whether or not to implement such a registry by September.<sup>137</sup> Finally, for our purposes, the F.T.C., in consultation with the Department of Justice, has two years to submit a report on the effectiveness and enforcement of the new law.<sup>138</sup>

3. The Selection of CAN-SPAM

After Congress failed to pass nineteen spam bills,<sup>139</sup> one wonders what motivated Congress to take action this time around. A strong direct marketing lobby and a lack of consensus about what the law should be previously prevented attempts to create federal spam legislation. The impetus behind Congress's recent action emerged in the form of a large public outcry in

---

avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender." 15 U.S.C. § 7712(b)(1). The F.C.C. "shall" also "allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the sender." 15 U.S.C. § 7712(b)(2). Although this could be interpreted to simply require an opt-out, § 7712(b)(3) makes it clear that more is required when it says that if the F.C.C. decides not to require the above, an opt-out should be implemented.

<sup>135</sup> 15 U.S.C. § 7712(b)(3).

<sup>136</sup> 15 U.S.C. § 7708 (2004). The study must "(1) set forth a plan and timetable for establishing a nationwide Do-Not-E-Mail registry; (2) include an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the [F.T.C.] has regarding such a registry; and (3) include an explanation of how the registry would be applied with respect to children with e-mail accounts."

<sup>137</sup> *See id.*

<sup>138</sup> 15 U.S.C. § 7709(a) (2004). The report should include "(1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act; (2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and (3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic." 15 U.S.C. § 7709(b).

<sup>139</sup> *See* Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

response to spam and concern over the varying forms of anti-spam legislation passed in thirty-five states.<sup>140</sup> Even direct marketing groups began to advocate a new federal law in order to avoid the confusion of complying with conflicting state laws.<sup>141</sup> In addition, when the national Do Not Call Registry gained public support and political momentum in 2003, a national do-not-email registry began to gain more political appeal, which helped spur the creation of the Act and its required study of a registry.<sup>142</sup> The CAN-SPAM Act took shape, and, in the end, was finally passed into law with the support of the Bush Administration.<sup>143</sup> The Act, which leaves room for future change, is a good first step in the fight against spam.

### *B. Problems and the Need for Change*

#### 1. Major Problems Still Unresolved

The CAN-SPAM Act, which is actually an acronym for Controlling the Assault of Non-Solicited Pornography and Marketing Act, is not nearly as tough as its name suggests, and will likely accomplish very little in the fight against spam. It is not unreasonable to say that Congress appears to have passed the new law mostly so it could show the public it was working to fight “the phenomenon that everyone loves to hate, rather than out of a conviction that this legislation is an answer to the problem.”<sup>144</sup> Many have argued that CAN-SPAM is not only weak, but it has preempted the stronger state anti-spam laws like California’s opt-in system that was to go into effect January 1, 2004.<sup>145</sup> The problem, however, is not that the strong state laws were

---

<sup>140</sup> *See id.*

<sup>141</sup> *See id.*

<sup>142</sup> *See id.*

<sup>143</sup> *See* Press Release, The White House, Fact Sheet: President Bush Signs Anti-Spam Law (Dec. 16, 2003), at <http://www.whitehouse.gov/news/releases/2003/12/20031216-4.html>. According to the White House, the new law is a “pro-consumer measure” which will establish a framework to help individuals, businesses, and families combat spam. The Bush Administration gives four reasons for the passage of this bill. First, the Administration sees this law as a “well-balanced” approach that will help end some harmful forms of spam, while capping statutory damages for civil violations and providing certainty for businesses that previously faced an array of state spam laws. Second, the law is part of the “Administration’s efforts to empower consumers with choices in the technology field” by giving consumers an opt-out mechanism. Third, the Administration stresses that the law will help its agenda to help protect children from pornography by requiring labels. Finally, the Administration cites to the harmful effects of deceptive and misleading spam. Though the Administration claims it wants to crack down on the spam problem, it obviously leaned at least somewhat toward protecting direct marketers.

<sup>144</sup> *See* Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>145</sup> *See* Cal. Bus. & Prof. Code 17529 (2003). *See* W. David Gardner, *Can-Spam*

2004]

SPAM IN A BOX

preempted, because preemption only works to create uniformity,<sup>146</sup> but rather it is that the uniform federal law being imposed is much too weak to have any substantial effect.

CAN-SPAM, as is, will fail to make any difference in the world of spam. First and foremost, it requires only the weaker opt-out system, rather than the stronger opt-in system, toward which the international trend seems to be geared.<sup>147</sup> The rationale that proponents of the opt-out system gave was that the Act is an attempt to create a system that allows for e-mail marketing generally, but that weeds out the deceptive marketing messages from the rest to increase the efficiency of e-mail marketing and legitimate commercial uses of e-mail as a whole.<sup>148</sup> Even assuming that this is a realistic goal, an opt-out requirement does not solve any of the serious problems relating to spam, which the E.U. countries, as well as Australia, have certainly begun to recognize by including opt-in systems.<sup>149</sup>

For one, most spammers will not provide proper opt-out mechanisms even under this law unless they truly fear being caught and punished. Even Finding Nine of the Act points out that many senders do not include opt-out mechanisms or refuse to honor the ones they do have.<sup>150</sup> Even if all commercial e-mail complied with the law, it would be in such great quantities that it would still flood servers and inboxes. In other words, the amount of commercial e-mail is not likely to decrease under an opt-out regime. One can easily imagine an inbox overflowing with fully complying, non-deceptive e-mail advertisements for real non-scam related products. This is the apparent goal of the Act, which, even if achieved, is not desirable.

The new law, in requiring nothing more than an opt-out procedure, in effect legalizes spam<sup>151</sup> and gives the green light to spammers to go ahead and spam

---

*Changes Life for Legit E-Mailers* (Feb. 10, 2004), at [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc\\_cmp/17602978](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc_cmp/17602978); see also McCullagh, *supra* note 111, at <http://news.com.com/2100-1024-51106222.html> (stating that, among the five dissenters in the House's final vote, two were Democratic legislators from the heart of Silicon Valley: Zoe Lofgren and Mike Honda).

<sup>146</sup> Finding Eleven explains that state law preemption is needed because the varying state statutes impose different standards, creating unpredictability in the law for law-abiding businesses. 15 U.S.C. § 7701(a) (2004).

<sup>147</sup> 15 U.S.C. § 7704(a)(3)(A); 15 U.S.C. § 7704(a)(4)(A). See EuroCauce, Countries, at <http://www.euro.cauce.org/en/countries/index.html> (last visited Apr. 3, 2004).

<sup>148</sup> See Deligiannis, *supra* note 104.

<sup>149</sup> See EuroCauce, *supra* note 147, at <http://www.euro.cauce.org/en/countries/index.html>.

<sup>150</sup> 15 U.S.C. § 7701(a).

<sup>151</sup> While some are wary of coming to this conclusion, even some spammers claim this, along with several European anti-spam groups, arguing that CAN-SPAM will actually encourage the flow of spam because it legalizes the sending of unsolicited e-mail. Anti-spam advocate Spamhaus, which favored the California law, stated that "with the passage of

to their hearts' content, at least until a recipient opts-out, assuming the opt-out mechanisms even work. The effectiveness of the Act depends on spammers' fear of being caught, and when there are many ways to make a spam e-mail appear to comply, there is much less fear of being caught. January saw an array of new spam that gave the illusion of compliance, which unfortunately, only makes it more difficult for users and filters to determine which e-mails are spam.<sup>152</sup> Under an opt-in regime, if users receive commercial e-mail from someone they do not do business with or have not recently done business with, then that sender is in violation, and no spammer tricks could change that. An opt-in regime would thus be more easily understood and more easily enforced.

In addition, an opt-out system is burdensome because both the sender and those acting on behalf of the sender must comply with opt-out requests, which will drastically affect joint marketing relationships because multiple parties must communicate with each other very efficiently to comply with opt-outs within the required ten days.<sup>153</sup> This will likely lead to the creation of massive lists of opted-out addresses that will need to be passed down a long line of vendors in order to comply, creating a huge burden on businesses who endeavor to comply with the Act. The opt-out system is therefore, ineffective, inefficient, and burdensome.

Another problem revolves around the possible future decision to create a national do-not-email registry, which CAN-SPAM seems to at least encourage.<sup>154</sup> While many have touted the triumphs of the national Do-Not-Call List,<sup>155</sup> which noticeably targeted many so-called "legitimate" direct marketers, others are uncertain whether a do-not-spam list would see anything close to the same success.<sup>156</sup> Even the F.T.C. has come out strongly against

---

Can-Spam, spamming is officially legal throughout the United States." See Gardner, *supra* note 145, at [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc\\_cmp/17602978](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc_cmp/17602978). This "legalization" of spam can lead to an increase in spam, as it did in South Korea (by a factor of eleven in three months) after the enactment of a similar bill. Vircom, *Can Laws Block Spam?*, at <http://www.vircom.com/Products/Modus3/Whitepapers.asp> (last visited Mar. 10, 2004).

<sup>152</sup> See Press Release, Can Spam Act Generates Host of 'New and Improved' Spam (Jan. 27, 2004), at [http://biz.yahoo.com/prnews/040127/dctu006\\_1.html](http://biz.yahoo.com/prnews/040127/dctu006_1.html). Top methods of "compliance" include spam with graphic messages containing a disclaimer letter and physical address, spam claiming its primary purpose is non-commercial, and spam that still offers suspicious opt-out mechanisms, such as a mail-in opt-out to a foreign country.

<sup>153</sup> See Deligiannis, *supra* note 104.

<sup>154</sup> 15 U.S.C. § 7708.

<sup>155</sup> Do-Not-Call Implementation Act of 2003, Pub. L. No. 108-10, 117 Stat. 557 (codified at 15 U.S.C. 6101-6108 (2003)).

<sup>156</sup> Associated Press, *Poll: Don't-call List Works, Spam Law Doesn't* (Feb. 19, 2004), available at <http://www.cnn.com/2004/US/02/19/ap.poll.do.not.call.ap/index.html>, CNN.com,

2004]

*SPAM IN A BOX*

the national do-not-email registry because it is too expensive, unworkable and not a good allocation of resources, yet it must still continue its study and make a proposal according to CAN-SPAM.<sup>157</sup>

Some have voiced concerns that spammers, being the delinquent group that they are, would simply ignore a national do-not-email registry, while only legitimate companies would heed it.<sup>158</sup> Others have voiced a concern that a do-not-spam list would only invite more spammers.<sup>159</sup> That spammers would use such a list for all of the wrong reasons seems fairly certain, as even now spammers go through a lot of trouble to figure out which e-mail addresses have actual users behind them. It is fairly predictable that the greedy-eyed spam monster would lick its chops at what it would see as the first freely compiled and accurate database of working e-mail addresses, and the spam attack to follow would likely be devastating.

In addition to the above problems, the Act only contains a weak prohibition on harvesting, contingent on violations of other parts of the anti-spam law even though Finding Ten of the Act expresses a fear that users will not be able to make full use of websites and Internet services if their addresses are constantly being harvested by senders of spam.<sup>160</sup> If, for example, a spam e-mail sent to an address harvested by automated means<sup>161</sup> or to an address alphanumerically created by automated means, includes the proper identifier, opt-out mechanism, and other requirements, the harvesting or creation of that address is legal.

This weak provision neither prohibits alphanumeric automated creation of addresses and harvesting altogether, nor requires harvesting consent from users. Not only must other provisions be violated for harvesting to be illegal, but the prohibition only holds in cases where either the address was created alphanumerically by automatic means or the website or service from which the information was taken posted a notice prohibiting the harvesting of the addresses in order to send spam. So, spam sent to harvested or alphanumerically created addresses that complies with the Act is not in violation. Also, in a case where a spammer sends spam to an address harvested from a website that failed to post the proper notice, the spammer is not in violation.

One can easily imagine the multitudes of non-commercial websites that

---

<sup>157</sup> See Deligiannis, *supra* note 104.

<sup>158</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usa\\_today/withantispamlawineffect\\_companiesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usa_today/withantispamlawineffect_companiesworktofoiljunkemail).

<sup>159</sup> Associated Press, *supra* note 156, available at CNN.com, [http://www.cnn.com/2004/US/02/19/ap.poll.do\\_not.call.ap/index.html](http://www.cnn.com/2004/US/02/19/ap.poll.do_not.call.ap/index.html).

<sup>160</sup> 15 U.S.C. § 7701(a); 15 U.S.C. § 7704(b)(1)(A).

<sup>161</sup> “Automated means” would presumably include invisible tracking devices such as cookies or other systems by which spammers can gather a large number of e-mail addresses.

contain e-mail addresses and whose “operators” are individuals who are unaware of or would not bother with the notice requirement. Even if the service provider can take charge and automatically insert such a notice, this will not only disturb the user’s online creation, but it will place a needless burden on the service provider. Although some may think it is a good idea to give an incentive to website operators to post such notices, placing such a burden on website operators seems unnecessary and counter-productive. The law could just as easily prohibit harvesting altogether, thus negating the need for such notices or, at least, prohibit harvesting if the spammer violated the anti-spam law by doing so, without any website notice contingency. There is no reason for this additional complexity, which can only serve to create confusion, and place additional burdens on parties other than spammers.

Other problems revolve around the provisions that are still under study. The rules regarding unwanted mobile service commercial messages is one area where the F.C.C. needs to make a big decision as to whether to require an opt-in or opt-out or something in between.<sup>162</sup> In addition to other problems, an opt-out would not stop the flood of spam that is ever increasing in the cellular phone context, while a complete opt-in system may have the negative effect of defeating one perhaps desirable benefit of wireless Internet-service – namely, the ability to receive commercial area-sensitive information. So far, CAN-SPAM shows no willingness to demand more than an opt-out system, however, which would certainly have dire consequences for the cellular phone world.

Last but not least, CAN-SPAM does nothing to solve the problem that derives from the global nature of the Internet, and spam. While February 2004 statistics show that the U.S. is by far the biggest source of spam,<sup>163</sup> spam can and does come from other countries as well, or is rerouted through other countries from U.S. sources.<sup>164</sup> Many argue that the serious spammers will simply move out of the country to avoid enforcement, while others respond that many U.S.-based marketers will not want to move overseas, and because compliance is easy, there is no real incentive for them to do so.<sup>165</sup> This argument overlooks the fact that many of the most delinquent spammers would find the law difficult to comply with, and if their business is profitable enough,

---

<sup>162</sup> 15 U.S.C. § 7712(b).

<sup>163</sup> United States, 56.74%; Canada, 6.80%; China (including Hong Kong), 6.24%; South Korea, 5.77%; Netherlands, 2.13%; Brazil, 2.00%; Germany, 1.83%; France, 1.50%; United Kingdom, 1.31%; Australia, 1.21%; Mexico, 1.19% Spain, 1.05%; Others, 12.23%. TechWeb, *Study Says U.S. Is Biggest Source of Spam* (Feb. 26, 2004), at [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040227/tc\\_cmp/18200812](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040227/tc_cmp/18200812).

<sup>164</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usa\\_today/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usa_today/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>165</sup> See Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

2004]

SPAM IN A BOX

they would most likely move elsewhere. Apparently, however, many spammers have indeed set up shop recently in China,<sup>166</sup> Thailand and other foreign countries in order to avoid CAN-SPAM.<sup>167</sup> This has forced many companies like Yahoo and America Online to try to create new technological defenses because the law is not nearly enough to stop spam.<sup>168</sup> That most spam originates in the U.S., however, only makes it more clear that U.S. law should have the strongest anti-spam laws in the world, yet all the U.S. currently offers to angry countries who must handle the U.S.'s spam is the weak and ineffective CAN-SPAM Act.

2. The Statistics and Reactions

The post-CAN-SPAM statistics, and the reactions to them, have started to roll in, and it looks like so far, no good. The year 2003 alone ushered in a bewildering one trillion spam messages.<sup>169</sup> According to Brightmail's study using a collection of millions of decoy email accounts, sixty percent of all email sent in January 2004 was spam, showing a two percent increase over the December statistics.<sup>170</sup> In February 2004, one study showed that more than eighty-six percent of spam violated at least one aspect of CAN-SPAM, while most violated all of the provisions.<sup>171</sup> As of the beginning of March 2004, one leading email defense provider revealed the results of its study, which showed that only three percent of spam complied with the requirements of CAN-SPAM during February, representing no change from its January results.<sup>172</sup>

<sup>166</sup> China appears, however, to finally be taking steps to combat spam, so at least one former safe haven for spammers is disappearing. See news24.com, *China blacklists spam servers* (Feb. 19, 2004), at [http://www.news24.com/News24/Technology/News/0,,2-13-1443\\_1486065,00.html](http://www.news24.com/News24/Technology/News/0,,2-13-1443_1486065,00.html).

<sup>167</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>168</sup> See *id.*

<sup>169</sup> See Rubell, *supra* note 16.

<sup>170</sup> See Press Release, *supra* note 21, at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html)

<sup>171</sup> See Press Release, *CAN-SPAM Law Violations Continue At High Rate for Second Month in a Row, According to Audiotrieve InBoxer Anti-spam Study* (Feb. 10, 2004), at [http://biz.yahoo.com/bw/040210/105509\\_1.html](http://biz.yahoo.com/bw/040210/105509_1.html). Only 143 of the 1040 messages analyzed contained the information required by CAN-SPAM, but Audiotrieve did not try to verify that the required physical addresses were correct or whether using the unsubscribe really would work. Therefore, the non-compliance rate could be even higher.

<sup>172</sup> See Press Release, *MX Logic Finds Only 3 Percent of Unsolicited Commercial Email Complied with CAN-SPAM Act in February, Representing No Improvement over January* (Mar. 4, 2004), at [http://biz.yahoo.com/bw/040304/45\\_424\\_1.html](http://biz.yahoo.com/bw/040304/45_424_1.html). MX Logic tracked CAN-SPAM compliance by examining a random sample of unsolicited commercial Internet email each full week in February.

Another company also noted no change between January and February and concluded that ninety-eight percent of spammers are not taking the new law seriously.<sup>173</sup>

As expected, spammers are finding ways to evade the new law and are creating new problems because of the law. Apparently, spammers are now spamming inboxes with anti-spam service offers or CAN-SPAM compliance service offers as a cover for more suspect services.<sup>174</sup> In fact, one out of every twenty spam e-mails during a February study included some form of compliance-like information to create the appearance of legitimacy.<sup>175</sup> One new trick spammers are using to avoid falling within the ambit of the law is to include non-promotional content to switch the focus of the e-mail from a primarily commercial purpose to some other purpose, which could possibly lead to a categorization as something other than commercial e-mail, making the Act inapplicable.<sup>176</sup> This may help explain why recently, when users mistakenly open a spam e-mail, the beginning of it may consist of a random poetry selection.

The violations that one can find by looking through one's inbox are so prolific, blatant, and obviously intentional that one can only conclude that spammers have little fear of being caught or facing the penalties of CAN-SPAM.<sup>177</sup> Despite the civil and criminal penalties, many spammers are not convinced that they will be caught and prosecuted. Deviant spammers will continue to simply include a non-existent physical address or faulty opt-out mechanism in order to "comply" with CAN-SPAM and avoid prosecution.<sup>178</sup> Since many never test the opt-out mechanism for fear of confirming the existence of their e-mail address and adding to spammers' database of usable addresses, spammers who do not comply are often never discovered.<sup>179</sup> In all likelihood, Congressional Finding Nine of the Act, which points out that many

<sup>173</sup> See Press Release, Commtouch Reports Spammers Use of 'New Alphabet' in January Defies CAN-SPAM Law Requirements (Feb. 4, 2004), at [http://biz.yahoo.com/bw/040204/45313\\_1.html](http://biz.yahoo.com/bw/040204/45313_1.html).

<sup>174</sup> See Press Release, *supra* note 152, at [http://biz.yahoo.com/prnews/040127/dctu006\\_1.html](http://biz.yahoo.com/prnews/040127/dctu006_1.html).

<sup>175</sup> See Lance Ulanoff, *Spam: A Reality Check-Recent Developments in the Fight Against Junk E-Mail* (Feb. 20, 2004), at [http://abcnews.go.com/sections/scitech/ZDM/spam\\_commentary\\_pcmag\\_040220.html](http://abcnews.go.com/sections/scitech/ZDM/spam_commentary_pcmag_040220.html).

<sup>176</sup> See *id.*

<sup>177</sup> See Press Release, *supra* note 171, at [http://biz.yahoo.com/bw/040210/105509\\_1.html](http://biz.yahoo.com/bw/040210/105509_1.html)

<sup>178</sup> See Press Release, *supra* note 21, at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html).

<sup>179</sup> See Michael Rollins, *Heading off spam at the pass*, JAPAN TIMES ONLINE (Mar. 27, 2003), at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nc20030327mr.htm>. This author and likely many others advise, "Never click on the "Remove Me" link in a UCE message. All this does is let the spammer know that your address is valid and working properly, meaning it will most likely be sold to someone else."

2004]

SPAM IN A BOX

spammers do not include opt-out mechanisms or refuse to honor the ones they do have,<sup>180</sup> will not likely change in any significant way under the new law. Furthermore, with a belief that they will not be caught and with a few recipients still making purchases from the spam, spammers still have a powerful economic incentive to keep spamming.<sup>181</sup>

Because it is so easy for deviant spammers to evade the law and not be caught, many honest businesses that send out commercial e-mail to customers, are left with a sense of unfairness as they find themselves scrambling to comply with the new law.<sup>182</sup> These businesses argue that CAN-SPAM will have little impact on unethical businesses that already engage in fraud or deception because they will endeavor to avoid prosecution or they will locate their servers offshore, while the greatest impact will be on legitimate businesses that use email as a customer service medium.<sup>183</sup> Part of the reason many businesses feel that this law imposes such a great burden is due to the fact that the law covers e-mails stemming from ongoing business relationships or e-mails sent out in small quantities, so almost every possibly commercial e-mail has to comply with the Act.<sup>184</sup> The feeling that CAN-SPAM impacts only the businesses that will comply with its provisions, while spammers continue to ignore or evade the new law, is strong.<sup>185</sup> Unfortunately, it is these businesses that the F.T.C. will most likely take action against first as spammers are so difficult to find.<sup>186</sup> Notably, this result is the opposite of the intended goal of the Act, which was to weed out only the spammers who use deceptive practices.

Moreover, the businesses that are making the effort to comply with the Act are confused about how to do so, with over fifty percent reporting in January

---

<sup>180</sup> 15 U.S.C. § 7701(a).

<sup>181</sup> Rice, *supra* note 32.

<sup>182</sup> See Deligiannis, *supra* note 104.

<sup>183</sup> See Kennedy & Lyon, *supra* note 4.

<sup>184</sup> See Deligiannis, *supra* note 104. CAN-SPAM exempts from its reach “transactional or relationship messages” e-mail the primary purpose of which is to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender, among other things. 15 U.S.C. § 7702(17)(A)(i). CAN-SPAM does not omit e-mail sent to recipients with whom the sender has an ongoing business relationship. CAN-SPAM, therefore, requires businesses that contact their customers not regarding a specific “transaction” to observe all the restrictions that apply to emails that CAN-SPAM covers. The CAN-SPAM Act does, however, authorize the F.T.C. to modify the above as needed to accommodate changes in technology and email practices and to accomplish the purpose of the Act. CAN-SPAM Act of 2003, §3(17)(B).

<sup>185</sup> See Gardner, *supra* note 145, at [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc\\_cmp/17\\_602978](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc_cmp/17_602978).

<sup>186</sup> See Deligiannis, *supra* note 104.

that they did not understand the law.<sup>187</sup> Certainly, the Act is long, convoluted and confusing. Comprehension of the new law will improve, however, when the F.T.C. makes the exemption for “transactional and relationship messages” and the definition of commercial e-mail more clear.<sup>188</sup>

Although the statistics and problems weigh heavily against the Act as it is currently written, many remain optimistic. Even Brightmail believes that CAN-SPAM will play an important role in the fight against spam.<sup>189</sup> After all, the first lawsuits under CAN-SPAM have just started to trickle in, beginning with complaints in February from America Online and EarthLink, each of which has taken a strong stance against spammers.<sup>190</sup> On March 4, 2004, the California ISP Hypertouch filed a complaint against BVBWebTies, owner of Bobvila.com, for allegedly sending spam that failed to supply a physical address, used deceptive header information and randomly generated and harvested addresses including previously opted-out addresses.<sup>191</sup> These suits show that at least several ISPs are willing to begin to fight spammers using CAN-SPAM as a tool. Certainly, the public cannot expect a true deterrent factor until spammers start to pay.<sup>192</sup>

This trend has continued when America Online, Earthlink, and Yahoo joined forces and filed six lawsuits against hundreds of people for allegedly sending

---

<sup>187</sup> See Press Release, CAN-SPAM Survey Reveals Most E-Mail Marketing Non-Compliant; Data Reveals Marketplace Does Not Understand New Legislation (Jan. 26, 2004), at <http://biz.yahoo.com/iw/040126/062198.html>.

<sup>188</sup> A message is not a commercial electronic mail message unless advertisement or promotion is the message’s primary purpose. 15 U.S.C. § 7702(2)(A). Unfortunately, the terms “advertisement,” “promotion” and “primary purpose” are not defined. Spammers will thus try to evade the law by creating a false primary purpose that is neither a promotion or advertisement to avoid the law, though this may be difficult to do as these terms are quite broad. Also, because the broad definition of “promotion,” many business to business e-mails that do not advertise a product or service will still be subject to the law. See Kennedy & Lyon, *supra* note 4.

<sup>189</sup> See Press Release, *supra* note 21, at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html).

<sup>190</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>191</sup> See Ron Miller, *First Can Spam Suit Filed* (Mar. 5, 2004), at <http://www.internetnews.com/xSP/article.php/3322311>; See Matt Hines, *ISP Hammers Bob Vila Site With Spam Suit* (Mar. 5, 2004), at [http://zdnet.com.com/2100-1105\\_2-5170631.html](http://zdnet.com.com/2100-1105_2-5170631.html). The suit was filed in the Northern District of California against BVBWebTies and its partner, BlueStream Media, for spamming Hypertouch’s customers with Bob Vila’s “Home Again Newsletter.”

<sup>192</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

2004]

SPAM IN A BOX

spam in violation of CAN-SPAM.<sup>193</sup> Many of the defendants, however, were only named as “John Doe” defendants, suggesting that even the major ISPs could not discover the identity of most of the spammers.<sup>194</sup> Nonetheless, if the major ISPs continue to be willing to sue under the Act, there may be some hope that even the Act’s currently weak provisions will have some deterrent effect, especially if criminal penalties are sought.<sup>195</sup> Hopefully such a deterrent effect will cause the public, having tasted a world with less spam, to hunger for an even stronger version of CAN-SPAM.

As for enforcement, CAN-SPAM gives no private right of action to recipients, but only allows the F.T.C., state attorney generals and ISPs to file charges against CAN-SPAM violators. While on one hand this serves to protect businesses from the potential of multiple state suits by individual recipients,<sup>196</sup> on the other hand, it will prevent a flood of litigation that would make any positive aspects of the law unmanageable. Indeed, one redeeming quality of the Act is that, even though it gives primary enforcement authority to the F.T.C.,<sup>197</sup> it also gives a broad grant of enforcement power to the ISPs and to the states.<sup>198</sup>

ISPs can, and apparently are willing to, seek injunctive relief and statutory damages, which can be up to one hundred dollars per message, capped by a one million dollar total limit, or a three million dollar total limit in the case of a willful and knowing violation, or if other aggravated damages are available.<sup>199</sup>

---

<sup>193</sup> Associated Press, *Internet Providers Sue Hundreds for Unsolicited E-mail* (Mar. 10, 2004), at N.Y. TIMES ON THE WEB, <http://www.nytimes.com/aponline/technology/AP-Internet-Spam.html?hp>. See also FindLaw News Document Archive, Spam Litigation, at <http://news.findlaw.com/legalnews/documents/index.html#spam> (last visited on Mar. 10, 2004) (listing the newly filed complaints).

<sup>194</sup> See *id.*, at <http://www.nytimes.com/aponline/technology/AP-Internet-Spam.html?hp>.

<sup>195</sup> The Act’s criminal provisions make violations punishable by up to five years in prison and a substantial fine. 15 U.S.C. § 7706. Actions that can lead to criminal penalties include: sending bulk spam from a computer accessed without authority; sending bulk spam through open relays with the intent to deceive recipients or ISPs about the message’s origin; falsifying header information; and registering five or more e-mail accounts or IP addresses using information that falsifies the actual registrant’s identity. The Act directs the U.S. Sentencing Commission to issue guidelines on sentencing for these crimes. See D. Reed Freeman, Jr., *A Detailed Look At What the New Act Means For e-Commerce: Marketers May Still Have A Say*, E-COMMERCE L. & STRATEGY, Jan. 14, 2004, at 1.

<sup>196</sup> See Deligiannis, *supra* note 104.

<sup>197</sup> The F.T.C. can seek injunctions and civil penalties of up to eleven thousand dollars for each separately addressed e-mail and there is no cap on the amount of penalties the F.T.C. may recover. See Freeman, *supra* note 195.

<sup>198</sup> See Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>199</sup> 15 U.S.C. § 7706(g)(3). Aggravated damages are available if the spammer harvested, used automated means to create multiple email accounts, or relayed or retransmitted the

In addition, each state attorney general can bring suit on behalf of the residents of the state. State attorney generals may soon do this, considering consumers are making complaints to the F.T.C. regarding violations of the Act at a rate of up to three hundred thousand complaints per day.<sup>200</sup>

If state attorney generals follow in the footsteps of the ISPs, the Act may carry more clout than previously expected, especially considering the large statutory damage amounts that are available. Statutory damages in a suit by a state attorney general can be up to two hundred fifty dollars per message, capped by a two million dollar total limit, or a six million dollar total limit if a willful and knowing violation or if aggravated damages are available.<sup>201</sup> In addition, consumers are making complaints to the F.T.C. regarding violations of CAN-SPAM, evidently at a rate of up to three hundred thousand complaints per day.<sup>202</sup>

CAN-SPAM is a truly important step in the fight against spam,<sup>203</sup> assuming more steps are to follow. After all, CAN-SPAM creates a uniform national law that can impose both criminal and civil liability for most of the worst spam offenses.<sup>204</sup> Congress has, in effect, claimed a desire to stop spam, and it has the Congressional findings to back up this desire. So, when legislators witness the ineffectiveness of CAN-SPAM, they may be inspired to change it so that it actually works.

### 3. Time For Change

There is still reason to believe that a substantial change in the federal spam law may yet occur. As a change of political party may take place in the White House in 2004, and the public is still heated over the spam issue, it would not be surprising to see the spam issue, along with other controversial technology

---

spam through an unauthorized computer.

<sup>200</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>201</sup> 15 U.S.C. § 7706(f)(3).

<sup>202</sup> See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>203</sup> See Press Release, *supra* note 21, at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html); See Wright, *supra* note 51, at [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail); See Mike Langberg, *Optimism Grows in Fight Against Torrent of Spam* (Feb. 27, 2004), at [http://story.news.yahoo.com/news?tmpl=story&u=/sv/20040227/tc\\_sv/optimismgrowsinfigh](http://story.news.yahoo.com/news?tmpl=story&u=/sv/20040227/tc_sv/optimismgrowsinfigh) tagainst torrentofspam, (calling it the “first rung on the legislative ladder”); see Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>204</sup> See Gardner, *supra* note 145, at [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc\\_cmp/17\\_602978](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040211/tc_cmp/17_602978).

2004]

*SPAM IN A BOX*

issues like music file sharing, give rise to even more public discussion in the year to come. Either party may go for a much stronger anti-spam bill despite protests from direct marketers if the public outcry is strong enough and the opposing party supports a stronger bill, though there have not yet been any signs of this. Although there is currently no clear party divide over whether to have a relatively weaker or a relatively stronger anti-spam bill,<sup>205</sup> there is certainly a sense of necessity on both sides to show the public that the party is working to fight spam,<sup>206</sup> which could easily take the form of a stronger anti-spam law in the future.

In addition, CAN-SPAM itself to some degree allows for the possibility of a strengthened bill in the future. The F.T.C. has the ability under CAN-SPAM to modify the exemption for situations in which the Act does not apply<sup>207</sup> and must make a final decision by September as to whether it will implement a national do-not-email registry.<sup>208</sup> Also, the F.C.C. must decide by August on rules to protect consumers from unwanted mobile service commercial messages.<sup>209</sup> Finally, the F.T.C., along with the Department of Justice, must study the effects of CAN-SPAM for the next two years and make a report as to the effectiveness and enforcement of the new law.<sup>210</sup>

The two-year study should include “an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act.”<sup>211</sup> The study should also include an analysis with recommendations “concerning how to address commercial electronic mail that originates in or is transmitted through facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions.”<sup>212</sup> The first of these two aspects of the study could easily bring into consideration the spread of spam to

---

<sup>205</sup> Democrats and Republicans have joined together in their efforts to propose many of the bills that have been introduced in Congress, including the CAN-SPAM Act. See Sorkin, *supra* note 79, at <http://www.spamlaws.com/federal/list107.html>.

<sup>206</sup> See Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>207</sup> 15 U.S.C. § 7702(17)(B) (2004).

<sup>208</sup> 15 U.S.C. § 7708. The study must “(1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry; (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the [F.T.C.] has regarding such a registry; and (3) include an explanation of how the registry would be applied with respect to children with e-mail accounts.”

<sup>209</sup> 15 U.S.C. § 7712(b).

<sup>210</sup> 15 U.S.C. § 7709(a).

<sup>211</sup> 15 U.S.C. § 7709(b)(1).

<sup>212</sup> 15 U.S.C. § 7709(b)(2).

new technologies such as instant messaging and new technological spam defenses, which has recently been dubbed “spim.”<sup>213</sup>

The second aspect brings the international nature of the Internet into the foreground, and shows that even the supporters of CAN-SPAM recognize that inboxes will not be spam-free unless some global solution can be achieved. Indeed, Senator Burns, one of the proponents of CAN-SPAM, stated that the U.S. had been in contact with members of Parliament in the U.K and with the chairman of the communications Board in Australia, and had come to the joint conclusion that “spam truly is an international problem.”<sup>214</sup> In May 2004, the International Telecommunications Union<sup>215</sup> will meet to discuss the global scope of the spam problem.<sup>216</sup>

All of the above points to a recognition that the status quo is insufficient, and to the likelihood of change in the near future. The CAN-SPAM Act itself recognizes that change may be necessary. The statistics and reactions that have arrived in the wake of the Act, unless they drastically improve in the upcoming months, point to the need for a stronger law. Senator Burns’s dream of creating a law that weeds out only deceptive spam, while the “legitimate” spam remains,<sup>217</sup> misses the forest for the trees. Most likely, there is little spam that is actually “legitimate” except commercial e-mail dealing with business transactions and relationships with preexisting customers, though users should have the ability to choose to receive even this type of e-mail. Since most users and ISPs would be content with a world devoid of spam, the few businesses or users that wish to receive spam should simply be required to choose to receive it. This and many other changes can be made to strengthen CAN-SPAM so that it really works.

#### V. LESSONS FROM ABROAD: HOW TO MAKE CAN-SPAM MORE EFFECTIVE

Spam is not just a local monster, but one that is attacking the four corners of the globe. An examination of legislation in the E.U. and Japan will provide a framework by which to strengthen U.S. legislation. One reason to turn to the E.U. legislation is because the E.U. has created a strong and progressive opt-in framework that can serve as a guide for future changes to the Act. An

<sup>213</sup> Anita Hamilton, *You’ve Got Spim!*, TIME, Feb. 2, 2004, at 77.

<sup>214</sup> See Ulanoff, *supra* note 175, at [http://abcnews.go.com/sections/scitech/ZDM/spam\\_commentary\\_pcmag\\_040220.html](http://abcnews.go.com/sections/scitech/ZDM/spam_commentary_pcmag_040220.html).

<sup>215</sup> The purpose of the ITU, which currently has one hundred eighty-nine member countries, is to be an “impartial, international organization within which governments and the private sector could work together to coordinate the operation of telecommunication networks and services and advance the development of communications technology.” The ITU’s official website can be accessed at: <http://www.itu.int/home/index.html>.

<sup>216</sup> See Ulanoff, *supra* note 175, at [http://abcnews.go.com/sections/scitech/ZDM/spam\\_commentary\\_pcmag\\_040220.html](http://abcnews.go.com/sections/scitech/ZDM/spam_commentary_pcmag_040220.html).

<sup>217</sup> See *id.*

2004]

SPAM IN A BOX

examination of Japan's recent legislation will also be instructive in that Japan is much more experienced than the U.S. with the cellular phone spam problem, as it has an advanced and widely used cellular network with advanced Internet capabilities.<sup>218</sup> Looking to anti-spam measures in both the E.U. and Japan, therefore, will provide insight into possible ways to improve the current U.S. spam legislation to make it more effective in the future.

A. *The Strong E.U. Opt-In Legislation*

1. The E.U. Legislation

Most likely prodded by the two and a half billion Euro e-business loss in 2002,<sup>219</sup> on May 30, 2002, the European Parliament, after a year of debate,<sup>220</sup> finally approved a draft of what would become the E.U.'s anti-spam legislation.<sup>221</sup> The Directive on Privacy and Electronic Communications (the "Directive") concerns "the processing of personal data and the protection of privacy in the electronic communications sector."<sup>222</sup> This legislation makes up the final portion of the Telecommunications Regulatory Package,<sup>223</sup> which was adopted on February 14, 2002.<sup>224</sup> The European Council, after coming to an agreement with the European Parliament, the European Commission and the Spanish Presidency of the Council of the European Union, formally adopted the Directive,<sup>225</sup> which entered into force on July 31, 2002 by publication in the Official Journal of the European Communities.<sup>226</sup>

The E.U. members were then supposed to have until October 31, 2003 to each individually pass the regulations as part of their own national laws.<sup>227</sup> As

<sup>218</sup> See Evan Cramer, *The Future of Wireless Spam*, 2002 DUKE L. & TECH. REV. 21, 21 (2002).

<sup>219</sup> Lauha Fried, eFINLAND, *Combating Spam Requires Global Co-Operation* (Nov. 1, 2003), at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=18707>.

<sup>220</sup> See generally Tim Richardson, *Europe Holds Key Vote on Spam Tomorrow* (Oct. 7, 2001), at <http://www.the-register.co.uk/content/archive/20290.html>; see also Kieren McCarthy, *EU Anti-spam Legislation Up Again this Evening* (Oct. 22, 2001), at <http://www.theregister.co.uk/content/archive/22387.html>; see Tim Richardson, *EU says 'Oui' to Spam* (Oct. 23, 2001), at <http://www.theregister.co.uk/content/6/22418.html>.

<sup>221</sup> Council Directive 2002/58, *supra* note 9.

<sup>222</sup> See *id.*

<sup>223</sup> Seventh Report on the Implementation of the Telecommunications Regulatory Package, COM(01)706 final.

<sup>224</sup> See Cramer, *supra* note 218.

<sup>225</sup> See Council Directive 2002/58, *supra* note 9.

<sup>226</sup> See *id.*

<sup>227</sup> See Cramer, *supra* note 218; see Hale and Dorr, *New E.U. "Spam" Restrictions Won't Stop U.S. Marketers* (Aug. 12, 2002), at [http://www.haledorr.com/publications/pub\\_detail.aspx?ID=1357&Type=5543](http://www.haledorr.com/publications/pub_detail.aspx?ID=1357&Type=5543).

of March 11, 2004, however, nine E.U member countries have not yet implemented the legislation,<sup>228</sup> which forced the concerned E.U. to issue a warning to those countries.<sup>229</sup> When the E.U. allows Eastern European countries to become members, implementation among all members may be even more difficult to achieve, although some harmonization is certainly better than none at all.<sup>230</sup>

The Directive establishes an “opt-in” system as the default rule for spam, requiring marketers to obtain permission from consumers before they can send them spam via e-mail, faxes or automated calling systems.<sup>231</sup> In addition, all spam must have an “opt-out” feature whereby a user can click a link in the spam e-mail to remove his or her name from a spammer’s list and avoid future spam from that sender.<sup>232</sup> Strangely, the Directive leaves it up to each country to decide whether or not to apply the opt-in framework to recipients other than “natural persons,” i.e., companies.<sup>233</sup> Apparently, this provision was an attempt to allow for unsolicited, business-to-business commercial communications.<sup>234</sup> Since spam is the most burdensome on companies, this provision makes no sense at all, and leaves the legislation much weaker than it would have been without it. Fortunately, it seems that most of the countries have applied the opt-in to companies as well.<sup>235</sup>

The Directive does, however, have an exception to its opt-in framework. Companies can send direct marketing e-mail to customers if they obtained the electronic contact information “in the context of a sale of a product or service” after giving the customer a clear and distinct opportunity to object to its use for direct marketing purposes at the time of the sale, and as long as they provide

---

<sup>228</sup> France, Germany, Belgium, Finland, Greece, Luxembourg, the Netherlands, Portugal, and Sweden. Sophos, *European Union presses for anti-spam laws, Sophos comments* (Dec. 8, 2003), at <http://www.sophos.com/spaminfo/articles/euspamlaws.html>.

<sup>229</sup> See Jucca, *supra* note 23, at [http://www.forbes.com/home\\_europe/newswire/2004/02/01/rtr1237398.html](http://www.forbes.com/home_europe/newswire/2004/02/01/rtr1237398.html); See EuroCauce, *supra* note 147, at <http://www.euro.cauce.org/en/countries/index.html>; see Paul Rubell, *supra* note 16. After the warning, Sweden finally implemented the legislation. Associated Press, *Sweden Adopts EU Ban on SPAM* (Mar. 4, 2004), at <http://www.eweek.com/article2/0,1759,1542578,00.asp>.

<sup>230</sup> John Darton, N.Y. TIMES ON THE WEB, *Union, but Not Unanimity, as Europe’s East Joins West* (Mar. 11, 2004), at <http://www.nytimes.com/2004/03/11/international/europe/11EURO.html?hp>.

<sup>231</sup> Council Directive, *supra* note 9, Art. 13.

<sup>232</sup> See Christopher Saunders, *EU Oks Spam Ban, Online Privacy Rules* (May 31, 2002), at [http://biz.yahoo.com/prnews/020909/nym065\\_1.html](http://biz.yahoo.com/prnews/020909/nym065_1.html).

<sup>233</sup> Council Directive 2002/58, *supra* note 9, Art. 13 §5.

<sup>234</sup> John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 333, 363 (2003).

<sup>235</sup> See EuroCauce, *supra* note 147, at <http://www.euro.cauce.org/en/countries/index.html>.

2004]

*SPAM IN A BOX*

an easy opt-out mechanism that is free of charge each time they send an e-mail to the customer.<sup>236</sup> The exception requires that the marketing e-mail be sent by the same entity that collected the contact information and received the recipient's consent.<sup>237</sup> In addition, the marketing e-mail that a company sends to the consenting customer must be for products or services that are "similar" to the one the customer purchased during the sale with the company.<sup>238</sup>

The Directive further requires that users give explicit permission for their data to be included in public directories.<sup>239</sup> The Directive specifies that ISPs may allow third parties to access consumers' data without the user's permission *only* for the purposes of criminal investigations or national or public security.<sup>240</sup> This clause was a compromise between Parliamentary conservatives and socialists, allowing E.U. member states to legislate their own policies on whether ISPs would be required to retain information on customers' Internet activity for future police investigations or only once an investigation begins.<sup>241</sup> The Directive also indicates that "invisible tracking devices, such as cookies, that collect information on users of the Internet may only be employed if the user is provided with adequate information about the purposes of such devices" and that the user has the option of rejecting such tracking devices.<sup>242</sup> Finally, the Directive requires cell phone users to give consent to marketers who wish to send area or interest-specific spam using sensitive location data that would provide for the exact location of cell phones.<sup>243</sup>

## 2. Reactions to the Directive

Reactions to the new E.U. legislation vary. EuroISPA, a group representing

---

<sup>236</sup> Council Directive 2002/58, *supra* note 9, Art. 13 §2.

<sup>237</sup> *See id.*, stating that "...the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services. . ." *See id.*, at Recital 41. According to the Data Protection Working Party, the same entity does not include mother companies or subsidiaries. Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (Feb. 27, 2004), at [http://europa.eu.int/comm/internal\\_market/whatsnew\\_en.htm](http://europa.eu.int/comm/internal_market/whatsnew_en.htm).

<sup>238</sup> Art. 13 §2. "...the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services. . ."

<sup>239</sup> *See* Saunders, *supra* note 232, at [http://biz.yahoo.com/prnews/020909/nym065\\_1.html](http://biz.yahoo.com/prnews/020909/nym065_1.html).

<sup>240</sup> *See id.*, at [http://biz.yahoo.com/prnews/020909/nym065\\_1.html](http://biz.yahoo.com/prnews/020909/nym065_1.html).

<sup>241</sup> *See id.*, at [http://biz.yahoo.com/prnews/020909/nym065\\_1.html](http://biz.yahoo.com/prnews/020909/nym065_1.html).

<sup>242</sup> *See* Press Release, EU Institutions, Commission Welcomes European Parliament's Vote to Accept Directive on Data Protection Rules for Electronic Communications Sector (May 30, 2002), available at <http://www.eurunion.org/news/press/2002/2002034.htm>.

<sup>243</sup> Council Directive 2002/58, *supra* note 9.

ISPs, as well as other commentators,<sup>244</sup> supports the new legislation and believes that an opt-in is the best solution as it strikes a balance between the right of e-mail users to be free of the burdens of spam, and the legitimate interests of commercial entities to use e-mail to communicate with a receptive consumer base.<sup>245</sup>

Critics of the new E.U. legislation point out that it will have little impact on the quantity of spam Internet users receive because so much spam originates outside the E.U.<sup>246</sup> Even after the legislation, E.U. estimates show that spam makes up more than half of all e-mail and costs European businesses more than 2.5 billion Euros (\$3.1 billion) a year in lost productivity,<sup>247</sup> certainly not showing any improvement in the numbers on spam. First, not all the member countries have yet implemented the legislation. Even if every E.U. country had implemented the legislation, the amount of spam originating in the E.U., possibly less than ten percent total, pales compared to the almost sixty percent originating in the U.S.<sup>248</sup> Brightmail, one anti-spam group, found that nine out of ten spam e-mails are either untraceable or come from outside the E.U.<sup>249</sup>

Critics who argue that this proves the E.U. framework will not work, however, are simply not seeing the whole picture. As Joe McNamee of EuroISPA suggests, this kind of thinking is a classic case of false logic, similar in nature to saying that there should be no copyright law in Europe because those outside Europe will continue to use the Internet to violate copyrights.<sup>250</sup> The E.U. law should be construed, therefore, as a first step in the European framework of anti-spam law in that it should at least help reduce the number of spam that originates in Europe. If such strong legislation does not attain the success it should, then one can only conclude that stronger anti-spam commitments are needed from other parts of the world. The E.U.'s law is still much stronger than other anti-spam laws, like CAN-SPAM, and should be held out as an example of the type of anti-spam law that, if passed everywhere, or at least in the U.S., would significantly decrease the amount of spam flowing through the system.

---

<sup>244</sup> See Magee, *supra* note 234.

<sup>245</sup> See Tim Richardson, *Europe Bans Spam* (May 30, 2002), at <http://www.theregister.co.uk/content/archive/25515.html>.

<sup>246</sup> See *id.*, at <http://www.theregister.co.uk/content/archive/25515.html>; see also Magee, *supra* note 234.

<sup>247</sup> Associated Press, *Tech Brief: EU Readies Spam Fight* (Jan. 28, 2004), at <http://www.iht.com/articles/126894.html>.

<sup>248</sup> Sophos, *Sophos outs 'dirty dozen' spam producing countries* (Feb. 6, 2004), at <http://www.sophos.com/spaminfo/articles/dirtydozen.html>.

<sup>249</sup> See Richardson, *supra* note 245, at <http://www.theregister.co.uk/content/archive/25515.html>.

<sup>250</sup> See McCarthy, *supra* note 70, at <http://www.theregister.co.uk/content/archive/22387.html>.

### 3. Feasibility of Integrating E.U. Provisions into CAN-SPAM

The actual effect of this law for Europeans is much less important than the directive's ability to serve as a template for anti-spam laws being created in other parts of the world, or for a future international anti-spam law. If the E.U. legislation is to serve as a model for a future version of CAN-SPAM, an examination of the Directive's strongest features is necessary.

First and foremost, the E.U. law takes a very strong stance against spam by recognizing that a simple opt-out feature is not sufficient and that, in order to effectively combat spam, an opt-in requirement will be the most powerful weapon.<sup>251</sup> Even though the Directive uses the opt-in system, it works to protect legitimate non-spam business messages between employers and customers as well.<sup>252</sup> To do this, the Directive requires that a company can send e-mail to its customers regarding its own similar products.<sup>253</sup> A company must give its customers a chance at the time of sale to object to such e-mail and an opt-out in each e-mail.<sup>254</sup> Certainly these provisions will serve to let users know who is sending them commercial e-mail and why.

The provisions for companies who send their customers e-mail are exceedingly narrow, and an even broader allowance might help balance the system. Obviously illegal would be e-mail that marketers sent out en masse asking potential customers to "opt-in." Allowing this would defeat the purpose of the system. However, companies, at least to some degree, should be able to contact potential customers. Perhaps a broader category, such as one that includes business relationships stemming from a transaction other than a sale of a product or service, like e-mail sent to potential customers who attended a company event, or one that advertises a non-similar product, would add balance to the system.

Further, the similar product or service provision creates ambiguity, and a lot of room for debate over what counts as "similar."<sup>255</sup> If the customer has already agreed to receive marketing e-mail from the company, which they indeed must do, then it is difficult to see why a company cannot advertise by e-mail any of its own products or services, or send company-related informational or event e-mails to that customer. It seems an unnecessary restraint on advertising to order the company by law to only advertise one line of products, and it would do nothing to reduce the amount of spam in users' inboxes.

Instead, it would only serve to make the advertiser's e-mails less effective. A broader category of marketing e-mail that originates from a more generally

---

<sup>251</sup> Council Directive 2002/58, *supra* note 9, Art. 13.

<sup>252</sup> *Id.*

<sup>253</sup> *See id.*, Art. 13 §2.

<sup>254</sup> *See id.*

<sup>255</sup> *See id.*

defined recent business transaction is more desirable for all parties involved, since users will still recognize the sender as an entity with whom they have done business in the past and to whom they consented to receive marketing e-mails, making it more likely that the message will be desired, viewed and responded to. Moreover, without a restraint on the type of transaction and the type of marketing e-mail the company must send, companies will be able to more effectively do e-business. Further, deleting the similar products or services requirement will not lessen the fairness to recipients, as they had to indicate a desire to receive that commercial e-mail from that company in the first place. If a company were wise, it would, after making clear the company is free to send any kind of marketing e-mail if the customer agrees, offer the customer a list of products or services or other categories, so its marketers could send that type of e-mail to the customer, achieving the best marketing results and creating the least amount of annoyance to the customer.

Second, several features of the E.U. legislation, besides the opt-in, are important to note. First, the Directive protects the privacy of users<sup>256</sup> by creating a complete prohibition on harvesting and allowing users to determine where and to whom personal information flows.<sup>257</sup> Since most users, if given the option, would probably not agree to accept invisible tracking devices like cookies<sup>258</sup> and would not list their own addresses in directories, users have one more method by which to combat spammers who use these tools.

Third, the Directive prescribes an opt-in system for cellular phone spam as well as for e-mail, creating uniformity among the laws surrounding similar technologies.<sup>259</sup> This is especially important since most cell phones in Europe today are Internet capable.<sup>260</sup> In Europe, cell phone spam is currently less of a problem than in Japan,<sup>261</sup> but still much more of a problem than in the U.S., forcing Europe ahead of the U.S. in its legislative response to cellular spam. An opt-in system allows only those users who think they might actually use their cell phones to obtain location specific information to choose to receive it, creating a more effective market for advertisers while allowing users to benefit from today's technology.<sup>262</sup>

---

<sup>256</sup> *See id.*, at Art. 12. ISPs may allow third parties to access consumers' data without the user's permission *only* for the purposes of criminal investigations or national or public security.

<sup>257</sup> *See id.*

<sup>258</sup> Web servers sometimes store cookies, or pieces of text, on a user's hard disk, which allow a Web site to store information on a user's machine for later retrieval. Among other functions, cookies can serve to identify prior users of a Web site. *See* Marshall Brain, *How Internet Cookies Work* (Sept. 7, 2003), at <http://computer.howstuffworks.com/cookie1.htm>.

<sup>259</sup> Council Directive 2002/58, *supra* note 9, at Art 13.

<sup>260</sup> *See* Cramer, *supra* note 218.

<sup>261</sup> *See id.*

<sup>262</sup> Council Directive 2002/58, *supra* note 9.

2004]

SPAM IN A BOX

Finally, the provision of the Directive that allows each country to decide whether or not to apply the opt-in framework to recipients other than “natural persons, “ i.e., companies,<sup>263</sup> should not be included in the model. Although this provision was an attempt to allow for unsolicited, business-to-business commercial communications, there is no reason to think that business-to-business spam is desirable, or that businesses should not be subject to the general opt-in framework with a customer exemption.<sup>264</sup> At the risk of sounding redundant, estimates show that fifteen to twenty percent of corporate e-mail consists of spam.<sup>265</sup> This means thousands of hours of wasted employee time, at a high overall cost. One can easily see that spam is certainly the most burdensome for companies. This provision, therefore, makes no sense at all, and leaves the legislation much weaker than it would have been without it. Although most of the countries have applied the opt-in to companies as well,<sup>266</sup> some, most notably the U.K, have chosen not to.<sup>267</sup>

Altogether, the first three features of the new E.U. legislation would generally serve to strengthen and enhance CAN-SPAM. In light of the E.U. legislation, the U.S. should consider an opt-in structure with a modified version of the E.U. business customer exception, a complete prohibition on harvesting and directory listings without consent, and an opt-in framework for cellular spam. The U.S. should not, however, exempt business-to-business spam from the opt-in framework. Modifying CAN-SPAM in this way would create a fair, yet strong anti-spam law that has the actual potential to decrease spam. Though the E.U. law is limited by its geographic scope, if more and more countries adopt such strong measures and successfully coordinate enforcement measures, the feasibility of which will be discussed later, positive results will ensue.

*B. Japan and Cellular Spam*

1. History Leading to Legislation

By the end of 2001, almost seventy million Japanese, more than half the population, were using *keitai* (cell phones) – so many, in fact, that the Japanese cellular phone market was said to have possibly reached its saturation point.<sup>268</sup>

<sup>263</sup> See *id.*

<sup>264</sup> See Magee, *supra* note 234.

<sup>265</sup> *Spam Filter Review 2004*, *supra* note 6, at <http://www.spamfilterreview.com/spam-statistics.html>.

<sup>266</sup> See EuroCauce, *supra* note 147, at <http://www.euro.cauce.org/en/countries/index.html>.

<sup>267</sup> Vircom, *supra* note 151, at <http://www.vircom.com/Products/Modus3/Whitepapers.asp>.

<sup>268</sup> See *Japan's Cell Phone Penetration to Grow Slowly*, APPLIANCE MAGAZINE.COM. (May 16, 2002), at

Studies estimate that around ninety percent of Internet-using Japanese go online using a cellular phone.<sup>269</sup> Along with the widespread use of cell phones and wireless Internet,<sup>270</sup> however, comes an unwanted familiarity with unsolicited wireless advertising, or cellular spam.<sup>271</sup> Spam in Japan, therefore, often means unsolicited commercial e-mail downloaded to cell phones.<sup>272</sup>

Several years ago, cellular subscribers in Japan did not perhaps consider the possible negative effects spam could have. In 2000, NTT Docomo (“Docomo”), Japan’s largest service provider, still regarded cell phone spam e-mail as the key to a new age of commerce.<sup>273</sup> Many believed that time and location specific advertisements would benefit cellular subscribers and increase user subscription.<sup>274</sup> Of course, like everywhere else in the world, Japanese consumers soon confronted the spam monster face-to-face. By 2002, cellular subscribers had grown to view spam not as useful, but as nothing more than a burden.<sup>275</sup> Cellular spam demanded increased bandwidth and a more extensive customer service and administrative system.<sup>276</sup> According to Docomo, estimates from the beginning of 2002 showed that ninety-eight percent of all e-mail messages that went through Docomo’s servers were spam, and that eighty-five percent of the spam was sent to non-existent Docomo

---

<http://www.appliancemagazine.com/news.cfm?newsid=1919>.

<sup>269</sup> See Kenji Hall, *Pesky Spammers Sneer at the Law*, JAPAN TIMES ONLINE (Oct. 9, 2003), at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20031009b1.htm>.

<sup>270</sup> See Cramer, *supra* note 218. Japanese cell phones allow users to have high-speed mobile Internet access.

<sup>271</sup> See *id.*

<sup>272</sup> See *id.* These e-mails usually contain some type of time or location-relevant information.

<sup>273</sup> See *id.* (citing Michele M. Yamada, *Japan Deal to Put Ads on Cell Phones* (June 2, 2000), at <http://www.thestandard.com/article/display/0,1151,15659,00.html>).

<sup>274</sup> See *id.*

<sup>275</sup> See *id.* In fact, Japanese users now hate spam so much, they spend their time online playing games like “Torture a Spammer.” Marketing Sherpa of Rhode Island created the game, which was located at [www.torturespammer.com](http://www.torturespammer.com), after a former subsidiary company, SparkLIST.com, allegedly stole ten million of its customers’ e-mail addresses and sold them to spammers. Marketing Sherpa hired Cyber NY to create this game in which various icons represent spammers: a blond in a red bikini (pornographic solicitations), a purple and white pill (“Viagra”), a man in a trenchcoat (spam-list salesman) and a house with dollar bills (mortgage offers). Players of the game could use a variety of punishments with sound effects (spamalanche, boiling oil and virtual death by flying monkeys) to torture these characters. Apparently, around fourteen thousand Internet users played the “Torture a Spammer” interactive Web site game in its first two weeks. See Lee, *supra* note 78.

<sup>276</sup> See Cramer, *supra* note 218 (citing Brandon Mitchener, *All Spam, All the Time*, WALL ST. J., Oct. 29, 2001, available at <http://interactive.wsj.com/archive/retrieve.cgi?id=SB1004116795770194080.djm>).

2004]

SPAM IN A BOX

addresses, with around thirteen percent making it through to actual users.<sup>277</sup> Overwhelmed with spam, Docomo's network was carrying a very heavy burden, as each spam sent to a non-existent address results in four tasks for the server: three attempts to send the e-mail and then one rejection notice to the sender.<sup>278</sup> Docomo and other providers, therefore, had to pay higher customer service and system administration costs to fight spam in order to maintain their customer base. In addition, since Docomo assesses a fee for every e-mail that users receive and download,<sup>279</sup> users ended up paying directly for spam.<sup>280</sup>

Docomo tried to stop spam through legal action against spammers, more filtering at the server, and giving users the ability to limit domain names from which they receive e-mail, but all of Docomo's efforts were in vain.<sup>281</sup> Docomo and other providers still had to deal with the hassles of overflowing inboxes and the high cost of handling all the spam, in addition to the burden of taking legal action<sup>282</sup> and the unpredictable outcome of such legal action in light of the unfavorable spam laws.

By November 2001, after many complaints from cellular subscribers, Docomo requested and gained approval of the Ministry of Public Management, Home Affairs, Posts and Telecommunications (the "Ministry") to use its own tactics to fight spam.<sup>283</sup> One such tactic was to prevent advertisers from creating accurate lists by blocking spam sent to large numbers of invalid addresses<sup>284</sup> randomly generated by spammers searching for valid addresses.<sup>285</sup> Docomo also provided its users with options to block e-mails from unknown addresses or change their own address, but these options were too imprecise and often blocked messages users wanted to receive.<sup>286</sup> Moreover, if users have to change their addresses all the time, then they have to go to all the trouble of informing those with whom they exchange e-mail of the new address. In the end, Docomo's tactics did not sufficiently eliminate spam,

---

<sup>277</sup> See Kanabo Consulting, *Market Snapshot – Japan, Spam in Japan: Scourge of the Mobile Phone*, THE JAPANALYZER, at <http://www.kanaboconsulting.com/newsletter702.htm> (July 2002).

<sup>278</sup> See *id.*, at <http://www.kanaboconsulting.com/newsletter702.htm>.

<sup>279</sup> See Cramer, *supra* note 218.

<sup>280</sup> See Sorkin, *supra* note 3, at 337.

<sup>281</sup> See Kanabo Consulting, *supra* note 277, at <http://www.kanaboconsulting.com/newsletter702.htm>.

<sup>282</sup> See *Court issues injunction on DoCoMo spammer*, *supra* note 60, at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20011031a4.htm>.

<sup>283</sup> See *id.*

<sup>284</sup> See Cramer, *supra* note 218 (citing ADLAW, *Wireless Spam A Problem in Japan* (Nov. 19, 2001), at <http://www.adlawbyrequest.com/international/DoCoMo111901.shtml>).

<sup>285</sup> See *id.*

<sup>286</sup> See *id.*

leaving behind many unsatisfied customers.<sup>287</sup> After this attempt at regulation by Docomo, eighty-four percent of the nine hundred and fifty million daily e-mails in Japan were still spam, costing Docomo over two hundred million dollars.<sup>288</sup> Docomo's methods of self-help, therefore, failed to meet both the customers' expectations as well as Docomo's business expectations.

## 2. Japan's Spam Legislation

Docomo, with the failure of its attempt at self-help clearly in mind, decided to turn its attention to the law. With encouragement from Docomo, Japan's Liberal Democratic Party sought limitations on all spam, while the Ministry of Economy, Trade and Industry (METI) tried to create limitations only on pornographic and adult service spam.<sup>289</sup> In April 2002, in reaction to Docomo's attempt at self-help and party and ministry efforts, the Japanese Diet enacted two anti-spam bills: the Law for Appropriate Transmission of Specified Emails<sup>290</sup> ("LATSE"), which was proposed by the three major parties,<sup>291</sup> and an amendment to update the 1976 Specific Transactions Law, proposed by METI<sup>292</sup> as a compromise with the Liberal Democratic Party.<sup>293</sup> After the House of Councilors approved LATSE, the House of Representatives passed LATSE and the amendment into law on April 11<sup>th</sup> and 12<sup>th</sup>, 2002,<sup>294</sup> respectively, and both went into effect on July 1, 2002.<sup>295</sup>

LATSE regulates spammers under the Ministry's jurisdiction, which covers the whole of Japan.<sup>296</sup> LATSE obligates spammers to display their name and

<sup>287</sup> *See id.*

<sup>288</sup> *See id.* (citing Toru Takahashi, *Two New Laws Aimed At Cutting Spam*, YOMIURI SHIMBUN, July 1, 2002, available at 2002 WL 19074087).

<sup>289</sup> *See* Christopher Saunders, *Japan Takes Anti-Spam Steps* (July 11, 2002), at <http://www.internetnews.com/IAR/article.php/1402331>.

<sup>290</sup> *See id.*, at <http://www.internetnews.com/IAR/article.php/1402331>. The name of the law in Japanese is: *Tokutei denshimeru no soushin no tekiseikatou ni kansuru houritsu*. Law regarding the sending of certain electronic mail], Law No. 26 of 2002, available at, [http://law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX\\_OPT=1&H\\_NAME=%93%e8%92%e8%93%64%8e%71%83%81%81%5b%83%8b&H\\_NAME\\_YOMI=%82%a0&H\\_NO\\_GENGO=H&H\\_NO\\_YEAR=&H\\_NO\\_TYPE=2&H\\_NO\\_NO=&H\\_FILE\\_NAME=H14HO026&H\\_RYAKU=1&H\\_CTG=1&H\\_YOMI\\_GUN=1&H\\_CTG\\_GUN=1](http://law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=1&H_NAME=%93%e8%92%e8%93%64%8e%71%83%81%81%5b%83%8b&H_NAME_YOMI=%82%a0&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=H14HO026&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1).

<sup>291</sup> *See Law on Unsolicited E-mail Takes Effect*, JAPAN TODAY, July 1, 2002, at <http://www.japantoday.com/gidx/news221054.html>.

<sup>292</sup> *See id.*, at <http://www.japantoday.com/e/?content=news&cat=2&id=221054>.

<sup>293</sup> Amendment to 1976 Specific Transactions Law, Law No. 28 of 2002. *See* Saunders, *supra* note 289, at <http://www.internetnews.com/IAR/article.php/1402331>; *see* Cramer, *supra* note 218.

<sup>294</sup> *See* Cramer, *supra* note 218 (citing *Law Enacted to Regulate Unsolicited E-mail Ads*, JAPAN COMPUTER INDUSTRY SCAN, Apr. 15, 2002, at LEXIS, IAC Japan).

<sup>295</sup> *See id.*

<sup>296</sup> *See id.* (citing Takahashi, *supra* note 288).

2004]

SPAM IN A BOX

contact information in the subject line of e-mails so that a user will know the message is spam before downloading the body of the e-mail to their cell phones.<sup>297</sup> Specifically, the subject line of spam e-mail must contain the Japanese phrase “*mishoudaku koukoku*”, meaning unsolicited advertisement, along with a special mark.<sup>298</sup> Users can choose to block any e-mail designated as spam by its subject line.<sup>299</sup> The new law prohibits spammers from using randomly generated addresses and requires them to adhere to users’ opt-out requests, whether made by a phone call or an email.<sup>300</sup> Finally, the law allows telecommunications carriers to refuse e-mail from known spammers if it creates system problems.<sup>301</sup> The new law imposes a five hundred thousand yen (approximately four thousand one hundred eighty U.S. dollars) fine for non-compliance with opt-out requests.<sup>302</sup> Businesses can face up to two million five hundred and sixty thousand dollars in fines.<sup>303</sup> Altogether, LATSE presents one method for dealing with cellular spam.

On April 12, 2002, the House of Councilors enacted the amendment to the 1976 Specific Commercial Transactions Law, which governs mail-order businesses for the purpose of protecting consumers via exploitative marketing techniques, such as direct marketing.<sup>304</sup> The amendment is narrower than LATSE in that it only applies to products and services.<sup>305</sup> Its aim is to avoid excessive burdens on the free market.<sup>306</sup> The amendment provides cellular users with an opt-out feature.<sup>307</sup> This law gives users the ability to report spammers to the Ministry, which can then issue cease-and-desist orders to the spammers, prohibiting them from sending future spam mail.<sup>308</sup> Spammers who do not comply face up to two years in prison or fines of up to three million yen (approximately twenty-four thousand U.S. dollars).<sup>309</sup> The Ministry issued

---

<sup>297</sup> See *id.* (citing Press Release, NTT DoCoMo, NTT DoCoMo to Offer New Anti-Spam Option (July 2, 2002), available at <http://investor.nttDoCoMo.com/ReleaseDetail.cfm?ReleaseID=83905&page=article&type=Press>).

<sup>298</sup> See NTT DoCoMo, *DoCoMo Phones to Take Advantage of New Anti-spam Legislation* (Sept. 3, 2002), at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

<sup>299</sup> See Cramer, *supra* note 218.

<sup>300</sup> See *id.*

<sup>301</sup> See *id.*

<sup>302</sup> See *id.*

<sup>303</sup> See Saunders, *supra* 289, at <http://www.internetnews.com/IAR/article.php/1402331>.

<sup>304</sup> See Cramer, *supra* note 218.

<sup>305</sup> See *id.*

<sup>306</sup> See *id.* (citing *Ministry LDP Split Over Spam*, ASAHI SHIMBUN, Apr. 20, 2002, at <http://www.asahi.com/english/business/K2002020200259>).

<sup>307</sup> See Cramer, *supra* note 218.

<sup>308</sup> See *id.*

<sup>309</sup> See *id.*

warnings based on the new law on November 11, 2003 against a company based in Nakano-ku, Tokyo, which had violated LATSE by sending spam to mobile phones without the proper labels, requesting that it conform to LATSE requirements.<sup>310</sup>

Perhaps those who drafted Japan's new anti-spam legislation realized it would be too weak to fight spam on its own, and so they required carriers like Docomo and rivals like KDDI to develop ways to reduce spam.<sup>311</sup> According to a Docomo survey conducted in August 2002 on two hundred and seventy mobile phones, the ratio of legal spam to illegal spam (i.e. following the guidelines of the new laws or not) remained unchanged in September.<sup>312</sup> The imperceptible effect of the new law led Docomo to implement a series of technological spam defenses. In late September 2002, Docomo announced that it would begin blocking all e-mails containing a spam subject line on October 1, 2002.<sup>313</sup> Docomo would first focus on e-mail sent to large numbers of invalid Docomo addresses.<sup>314</sup> Docomo further announced that if users wish to receive these e-mails, they can go to their iMenu, the official i-mode portal site, and change the setting at no cost.<sup>315</sup> In addition, Docomo will allow its PDC-based i-mode users to block, or exclusively receive spam from up to twenty spammers whom they choose.<sup>316</sup> This tactic implemented a technology-based opt-in system, which relied completely on spammers' compliance with labeling requirements.

In 2003, Docomo continued using more technological methods to block spam. Docomo started suspending or rescinding known spammer's subscriptions for registered phones, and, as of August 19, Docomo had

---

<sup>310</sup> See *MPHPT Implements Orders of Measures Against Violators of the Anti-Spam Law* (Nov. 13, 2003), at [http://www.soumu.go.jp/joho\\_tsusin/eng/Releases/Telecommunications/news031113\\_1.html](http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news031113_1.html).

<sup>311</sup> See Saunders, *supra* note 289, at <http://www.internetnews.com/IAR/article.php/1402331>. See also *MPHPT announces defensive measures against spam sent to mobiles* (Jan. 19, 2004), at [http://www.soumu.go.jp/joho\\_tsusin/eng/Releases/Telecommunications/news040119\\_2.html](http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news040119_2.html) (suggesting that, among other things, users use long and complicated e-mail addresses and not give out their addresses to avoid spam).

<sup>312</sup> See *14% of Cell Phone Ads Illegal, DoCoMo Says*, JAPAN TIMES, Sept. 25, 2002.

<sup>313</sup> See NTT DoCoMo, *supra* note 198, at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

<sup>314</sup> See ADLAW, *supra* note 284, at <http://www.adlawbyrequest.com/international/DoCoMo111901.shtml>.

<sup>315</sup> See NTT DoCoMo, *supra* note 198, at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

<sup>316</sup> See *id.*, at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

2004]

*SPAM IN A BOX*

suspended contracts with six hundred and two spammers.<sup>317</sup> In October 2003, Docomo began to limit the quantity of e-mail users could send out to one thousand e-mails per day under the assumption that the users who sent more than this would most likely be spammers.<sup>318</sup> In addition, as of January 1, 2003, Docomo users gained the ability to automatically reject e-mail from any i-mode phone that sends two hundred or more e-mails per day.<sup>319</sup> This e-mail blocking feature would be the default setting on these phones.

This technology-based system is in effect for Japan's Docomo subscribers, which, because Docomo is the world's leading mobile communications company, number more than forty million customers around the world, thirty-three million of whom receive e-mail and Internet access via the i-mode function.<sup>320</sup> Docomo's efforts alleviated some businesses' concerns about the onslaught of spam coming from Asia and, more specifically, from Japan.<sup>321</sup> Some of these businesses had even started blocking out en masse all Japanese e-mails.<sup>322</sup> METI however, may still push for stronger legislative action in the future,<sup>323</sup> especially in light of the new and strong E.U. legislation.<sup>324</sup> It is likely that further legislative efforts will be made in the future because the current system is lacking in several ways.

3. Feasibility of Integrating Japan's Legislation into CAN-SPAM

CAN-SPAM contains a provision that requires study for a future determination on how it should deal with cellular spam.<sup>325</sup> The F.C.C. has two hundred seventy days to make rules "to protect consumers from unwanted

---

<sup>317</sup> Press Release, NTT DoCoMo, NTT DoCoMo Sets Daily E-mail Limit as Part of Ongoing Measures to Counter Spam (Aug. 21, 2003), available at <http://www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param%5Bno%5D=263>.

<sup>318</sup> See id.

<sup>319</sup> Press Release, NTT DoCoMo, NTT DoCoMo Announces Latest Anti-Spam Measure (Nov. 5, 2002), available at <http://www.nttdocomo.com/presscenter/pressreleases/press/pressrelease.html?param%5Bno%5D=390>.

<sup>320</sup> See NTT DoCoMo, *supra* note 198, at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

<sup>321</sup> See ISP-Planets, *Cut Off Asia!* (Jan. 18, 2002), at [http://www.isp-planet.com/technology/2002/asia\\_bol.html](http://www.isp-planet.com/technology/2002/asia_bol.html).

<sup>322</sup> See id., at [http://www.isp-planet.com/technology/2002/asia\\_bol.html](http://www.isp-planet.com/technology/2002/asia_bol.html).

<sup>323</sup> See *Court Issues Injunction on DoCoMo Spammer*, *supra* note 60, at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20011031a4.htm>. One telecom ministry official stated, "We need to take substantial action against malicious businesses that repeatedly send illegal e-mail ads, even after they receive warnings."

<sup>324</sup> Council Directive 2002/58, *supra* note 9.

<sup>325</sup> See Kennedy & Lyon, *supra* note 4.

mobile service commercial messages.”<sup>326</sup> CAN-SPAM does not rule out the possibility of an opt-in system for cellular phone messages.<sup>327</sup> The F.C.C. “shall . . . provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender.”<sup>328</sup> In deciding whether to require this of mobile service providers, the F.C.C. must consider the relationship that exists between mobile service providers and their subscribers.

Whatever decision the F.C.C. makes, recipients should also be able to indicate electronically a desire not to receive future spam from the sender.<sup>329</sup> If the F.C.C. decides not to require express prior authorization, then the mobile service providers must not only comply with other provisions of the Act, but they must allow subscribers to indicate a desire not to receive future commercial messages from the provider at the time of subscription to the service, and at the time of any billing.<sup>330</sup> Of course, all this is subject to technological capability. Japan’s legislation and the actions that Docomo has taken are indicative of what works, what is possible, and what is, or rather, what is not, a desirable method by which to regulate cellular spam.

First and foremost, Japan’s legislation regarding cellular spam is indicative that an opt-out procedure alone, like the one CAN-SPAM prescribes for computer e-mail, is not enough to solve the problem of cellular spam. Japan’s opt-out legislation was not completely without merit, as it provided a cause of action against the most egregious violations, such as crashing servers with a deluge of cellular spam.<sup>331</sup> Almost immediately after the legislation passed, however, an unsatisfied Docomo began taking technology-based steps to fight spam, showing that a pure opt-out system will not be effective in the cellular context.

In addition, Docomo’s technological moves have many hidden negatives. Docomo’s first step consists of a block on all e-mails containing a spam subject line, along with the ability of a user to choose to receive e-mails with a spam subject line from up to a certain number of spammers in regard to certain desired subject matter.<sup>332</sup> Under this possible framework, all cellular spam must include a spam label. A subscriber could choose to receive a certain number and subject matter of e-mails with this label, or they could choose to receive none with this label. This system faces the obvious problem that

---

<sup>326</sup> 15 U.S.C. § 7712(b).

<sup>327</sup> 15 U.S.C. § 7712(b)(1).

<sup>328</sup> *Id.*

<sup>329</sup> 15 U.S.C. § 7712(b)(2).

<sup>330</sup> 15 U.S.C. § 7712(b)(3).

<sup>331</sup> See Kenji Hall, *supra* note 269, at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20031009b1.htm>.

<sup>332</sup> See NTT DoCoMo, *supra* note 198, at [http://www.japancorp.net/Article.Asp?Art\\_ID=3724](http://www.japancorp.net/Article.Asp?Art_ID=3724).

2004]

*SPAM IN A BOX*

spammers will simply not include the label, thus nullifying this system, even when doing this puts them in violation of LATSE since they do not fear prosecution.

The other Docomo spam-defense tactics are also not very useful, and some even present a significant threat to the legitimate e-business community. Docomo started suspending or rescinding spammer's subscriptions for registered phones. This is the least major self-regulation of the bunch, but it could create problems. One problem is that this step may not be very effective because spammers are innovative and often sneaky, so they may be able to switch to new accounts and contracts fairly easily. Another, bigger problem is that, if Docomo is not careful, it may end up blocking companies who send out large quantities of e-mails to customers.

Docomo's strategy of limiting the quantity of e-mail that users can send to one thousand e-mails per day, however, is much more dangerous. Many big companies, or even smaller companies who are sending customers non-spam e-mail could easily send more than a thousand e-mails a day. Further, if users choose to receive marketing e-mail from a certain spammer, which they indeed can do under Docomo's system, then that spammer may be a very successful marketer who should be able to send out as many e-mails as are requested. In addition, giving Docomo users the ability to automatically reject e-mail from any i-mode phone that sends two hundred or more e-mails per day may also block a business trying to send e-mail to customers or certain marketers from sending commercial e-mail to a subscriber who requested it to do so. These dangers threaten the utility of e-mail as a communication tool.

In addition, another problem stems from the fact that Docomo is not the only provider in Japan. A question arises as to whether other providers will be able to bear the same financial burden as Docomo, or be able to implement the same system in order to block out such large quantities of spam. Of course, Docomo's competitors are not tiny startups. J-Phone (thirteen million subscribers) and KDDI (thirteen million subscribers),<sup>333</sup> and most likely are financially and technologically capable of providing the same spam filter service as Docomo. New companies, however, may always emerge, unless of course they are constrained by the large filtering burden they would have to bear to compete. The real question, then, becomes whether a system that requires such a large commitment by a service provider would work as well in places, like the U.S., where there are still many smaller mobile service startups who could not perhaps implement the same filtering systems as the larger

---

<sup>333</sup> See Press Release, Telecommunication Carriers Association, The number of subscribers of Mobile Telephone, PHS (Personal Handy-phone System), Internet Provider Services and Radio Paging (Dec. 31, 2002), at <http://www.tca.or.jp/index-e.html>.

providers,<sup>334</sup> leading to a lack of predictability and uniformity, and an unnecessary restraint on competition.

The downside, therefore, of giving mobile service providers free reign, is that they will often take steps that fail to protect the legitimate interests of the business community in order to take steps to make their customers happy. Customers may not be so happy if providers take away some of the major benefits of the Internet. Even a strong anti-spam law should allow businesses to send out e-mail en masse in appropriate circumstances: where they were requested to send it or where they sent it to former or current customers who willingly supplied their contact information. In addition, requiring big mobile service providers to take anti-spam steps will place a large burden on them, one that will leave no room for new competitors or uniformity with smaller competitors, and may even lead to antitrust problems.

The conclusion, therefore, is that a system other than Japan's current one, would better serve everyone's interests. The best option, therefore, after examining the situation in which Japan finds itself, is to create a strong opt-in system by simply making all cellular spam illegal, except for commercial messages sent by a company to a customer or to a subscriber who requested the commercial message. Docomo may be correct in being somewhat skeptical over whether the enforcement of the spam law necessary for this option would be sufficient, but as the spam legislation is made stronger and enforcement improves, spammers will grow more fearful of prosecution, and a deterrent effect will emerge.

One way by which to strengthen an opt-in system for cellular spam is to create a strong prohibition on harvesting. Japan's legislation does nothing to prevent data gathering by spammers like its EU counterpart,<sup>335</sup> except to prohibit the random generation of addresses. Docomo's new technology does this indirectly in that it will prevent spammers from receiving invalid address messages and, as a result, spammers will have more difficulty creating accurate address lists.<sup>336</sup> Without data gathering amendments to the new law, however, spammers will be able to find addresses from many other sources despite Docomo's technology. A strong prohibition on harvesting, in conjunction with an opt-in, would lead to a much stronger law, especially if the prohibition on harvesting was adequately enforced. If spammers who attempt to evade the opt-in law have only a few addresses at hand, they would be forced to break the law again by either randomly generating or harvesting the addresses. The spammers would thus face double liability, and be deterred from future violations.

---

<sup>334</sup> See Saunders, *supra* note 289, at <http://www.internetnews.com/IAR/article.php/1402331>.

<sup>335</sup> Council Directive 2002/58, *supra* note 9.

<sup>336</sup> See ADLAW, *supra* note 284, at <http://www.adlawbyrequest.com/international/DoCoMo11901.shtml>.

2004]

*SPAM IN A BOX*

Japan's cellular situation, therefore, leads one to conclude that a strong opt-in system making all cellular spam illegal, except for commercial messages sent by a company to a customer or to a subscriber who requested the commercial message, is the best option. Such a system, in combination with a strong prohibition on harvesting, some non-conflicting technological innovation and global harmonization, would be the best weapon against cellular spam and one that the U.S. should consider adopting in the next several months.

VI. COMBINING APPROACHES: AIMING FOR A GLOBAL SOLUTION

*A. Amending CAN-SPAM To Make It More Effective*

CAN-SPAM, as is, will likely accomplish very little in the fight against spam. Signs that future change is coming, however, are abundant. Not only do both political parties sense the necessity to show the public that they are working hard to fight spam,<sup>337</sup> but also CAN-SPAM itself clearly leaves rooms for change, which could easily take the form of a stronger anti-spam law in the near future. In addition, in light of the array of problems that have arrived in the wake of CAN-SPAM, Congress should conclude that the current version of the Act is mightily lacking.

Changes that should occur in order to strengthen CAN-SPAM fall under four general categories: opt-in versus opt-out, definitions and exceptions, harvesting, and wireless spam. In light of the E.U. legislation, the U.S. should consider an opt-in structure with a modified version of the E.U. exception, a complete prohibition on harvesting and directory listings without consent, and an opt-in framework for cellular spam. Japan's current system provides evidence that instead of taking a softer approach to cellular spam, the U.S. should choose a strong opt-in framework. Further, although CAN-SPAM allows for a possible future implementation of a national do-not-email registry,<sup>338</sup> doing so will likely prove counterproductive. In addition, enforcement mechanisms should be improved through increased public awareness and a more accessible violation reporting system. The following is a more detailed discussion of these suggestions for change that will serve to improve the effectiveness of CAN-SPAM.

1. Opt-In and National "Please E-mail" Registry

The E.U. law takes a very strong stance against spam by recognizing that an opt-in requirement will be the most powerful weapon against spam.<sup>339</sup> The

---

<sup>337</sup> See Pizzi & Lyons, *supra* note 112, at <http://www.cfg-lawfirm.com/articles/can-spam.html>.

<sup>338</sup> 15 U.S.C. § 7708.

<sup>339</sup> Council Directive 2002/58, *supra* note 9, at Art. 13.

U.S. has many reasons to discard the opt-out system and follow the E.U.'s lead. First, an opt-out requirement sends a message to spammers that spam is legal and, as long as spammers follow certain procedures, they will not face any penalties. The quantity of spam, therefore, will only increase with an opt-out regime even if spammers follow the law. The servers will crash, users will become irritated as they waste more and more time, and the costs that individual users and companies will have to pay will grow prohibitive.

Further, an opt-out regime allows spammers who do violate the law to use various tricks to avoid detection, and when there are many ways to make a spam e-mail appear to comply, spammers have much less fear of being caught. Spammers will thus send more spam, forcing users to spend even more time sifting through e-mail. Honest businesses claim they are scrambling to comply, while unethical marketers that engage in fraud or deception will avoid prosecution because they will not be easily detected.<sup>340</sup> However, even honest businesses can send such massive quantities of spam through the system that they crash servers and cause huge economic consequences.

Additionally, the confusion that the opt-out regime causes and the burden it imposes on businesses are unnecessary and inefficient. Under an opt-out, businesses who engage in joint marketing relationships must communicate with each other very efficiently regarding opt-outs, as they have only ten days to comply with requests, which will lead to huge and complicated lists of users who have opted-out, and even companies who attempt to comply may find themselves suddenly in violation if the lists become inaccurate.

The rationale that proponents of the opt-out system give, therefore, does not stand up in the face of reality. A system that allows for e-mail marketing generally, but that weeds out the deceptive marketing messages from the rest, cannot increase the efficiency of e-mail marketing and legitimate commercial uses of e-mail as a whole because even the so-called "legitimate" messages will cause all of the same problems, and will not be an effective method of advertising.<sup>341</sup> Only an opt-in regime, such as that of the E.U., but with a broader exception for commercial marketing, will create the proper balance between the interest in having an efficient e-mail system and the interest in allowing for effective e-mail marketing.

An opt-in regime will serve to increase the efficiency of e-mail by allowing users to much more easily identify spammers. Under an opt-in regime, if users receive commercial e-mail from someone that does not fall under the exemption, i.e., someone with whom they have not recently done business or from whom they have not requested commercial e-mail, then that user will know with certainty that the sender is in violation. Any tricks a spammer may use to appear to "comply" would not matter, for the spam would simply be illegal. As long as users understand this simple law, and there is an efficient

---

<sup>340</sup> See Kennedy & Lyon, *supra* note 4.

<sup>341</sup> See Deligiannis, *supra* note 104.

2004]

*SPAM IN A BOX*

method by which users can report the illegal spam, an opt-in regime would be much more easily enforced than an opt-out. Additionally, an opt-in will save businesses from the burden of dealing with giant lists of opted-out addresses, and the great possibility of unwitting violations. Moreover, an opt-in system will not likely violate the First Amendment, as the First Amendment protects commercial free speech, but it does not create immunity from reasonable regulation.<sup>342</sup>

If an opt-in system were implemented, therefore, a national do-not-email registry would be wholly unnecessary. This would alleviate the F.T.C.'s concerns that such a registry would be too expensive, unworkable and not a good allocation of resources.<sup>343</sup> While a Do-Not-Call registry achieved some success, there is no reason to think that a similar registry would work for e-mail. That some people even compare the two systems is surprising. Although telephones and e-mail are both communication devices, the two are very different. For one, a single e-mail can be sent to millions of users in seconds. Also, many marketers who send e-mail are not sure that the address actually belongs to a user, while those who make marketing phone calls are sure that the number exists and that, even if the person they were trying to reach is not there, somebody will be reached. These are only two of many differences between e-mail and telephones that lead many to worry that spammers would

---

<sup>342</sup> See France, *supra* note 22, at [http://biz.yahoo.com/bizwk/020927/sb200209265958\\_1.html](http://biz.yahoo.com/bizwk/020927/sb200209265958_1.html). An opt-in system would not simply block all spam as it still would provide for exceptions to the rule. Users would have the ability to make a decision as to which commercial mail they wish to receive, or if they choose to receive any at all, and a choice could have different implications than a complete ban for constitutional concerns. See [http://biz.yahoo.com/bizwk/020927/sb200209265958\\_1.html](http://biz.yahoo.com/bizwk/020927/sb200209265958_1.html) (quoting University of Southern California constitutional law professor Erwin Chemerinsky who believes that "Giving recipients a choice is different than banning spam"). In addition, the rules governing commercial speech do not take a clear position that only an opt-out system would be constitutional. The government interest that is asserted must be substantial, and the regulation must advance this government interest without being more extensive than necessary. See Magee, *supra* note 234. Instead, the First Amendment only requires a reasonable fit between the means and the goal, not the least restrictive rule possible, although the availability of less restrictive means might be considered. Even after a brief look at the financial burden and crashed servers that spam has caused, the government clearly has a substantial interest in regulating spam. Spam is likely to increase and may, without regulation, completely nullify the viability of e-mail as a communication medium. Moreover, the opt-out alternative has already begun to prove itself overwhelmingly ineffective as a regulation of spam. It is unlikely, therefore, that a more attractive alternative exists, or even an alternative that would be effective at all. An opt-in regime that allows for business exceptions, therefore, would be a regulation that reasonably fits the goal of saving the e-mail system and would likely be found constitutional.

<sup>343</sup> See Deligiannis, *supra* note 104.

either completely ignore such a registry, or would use the list for all of the wrong reasons. It seems fairly certain that spammers, who go through great trouble to develop accurate lists of real e-mail addresses, would see such a registry as the first freely compiled and accurate database of working e-mail addresses, and proceed to send out spam in great masses to those addresses. Under an opt-in regime, a do-not-email registry is clearly unnecessary. If those who support a national registry still cling to the idea, then perhaps they should instead consider taking up the cause for an opt-in regime using a national “please e-mail” registry.

## 2. Definitions and Exemptions Revised

The Act first confines its application to a “commercial electronic mail message,” which does not include a “transactional or relationship message.”<sup>344</sup> The Act then proceeds to define a “transactional or relationship message.”<sup>345</sup> The categories under this definition are referred to as the Act’s “exemption” provision in that the instances listed in the categories will not fall within the sphere of the Act. Notably, CAN-SPAM does not omit e-mail sent to recipients with whom the sender has an ongoing business relationship. CAN-SPAM, therefore, requires businesses that contact their customers not regarding a specific “transaction” to observe all the restrictions that apply to emails that CAN-SPAM covers. This set-up, which provides spammers with loopholes by which to evade the law, has received criticism due to the fact that key words within the definition are not clearly defined.<sup>346</sup> The CAN-SPAM Act does, however, authorize the F.T.C. to modify the above as needed to accommodate changes in technology and email practices and to accomplish the

---

<sup>344</sup> 15 U.S.C. § 7702(2)(B); §7702(17).

<sup>345</sup> A “transactional or relationship message is “a message the primary purpose of which is (i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient; (iii) to provide (I) notification concerning a change in the terms or features of; (II) notification of a change in the recipient’s standing or status with respect to; or (III) at regular periodic intervals, account balance information or other type of account statement with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; (iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating or enrolled; or (v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.” 15 U.S.C. § 7702(17).

<sup>346</sup> The terms “advertisement,” “promotion” and “primary purpose” are not defined. See Kennedy & Lyon, *supra* note 4.

2004]

SPAM IN A BOX

purpose of the Act.<sup>347</sup>

Under an opt-in regime, however, there are no exemptions, only exceptions. The E.U. Directive creates one main exception to the prohibition on spam besides prior user consent. Companies can send direct marketing e-mail to *customers* if they obtained the electronic contact information “in the context of a sale of a product or service” after giving the customer a clear and distinct opportunity to object to its use for direct marketing purposes at the time of the sale, and as long as they provide an easy opt-out mechanism that is free of charge each time they send an e-mail to the customer.<sup>348</sup> In addition, the marketing e-mail that a company sends to the consenting customer must be for *its own* products or services that are *similar* to the one the customer purchased during the sale with that company.<sup>349</sup> The words “its own” require that the marketing e-mail be sent by the same entity that collected the contact information and received the recipient’s consent.<sup>350</sup>

The E.U.’s exception is very narrow, however, and if the U.S. were to implement an opt-in, it could create a much broader exception based on the categories in its exemption in order to protect legitimate non-spam business messages. Most of the exemption categories relate to a current or ongoing transaction.<sup>351</sup> All of the Act’s categories would become opt-in exceptions under an opt-in regime, meaning that spam would be prohibited, except for the instances described in the categories. As in the E.U., however, companies should only be able to send e-mail in such instances if they obtained the electronic contact information after giving the customer a clear and distinct opportunity to object to its use for direct marketing purposes at the time of the sale, and as long as they provide an easy opt-out mechanism that is free of charge each time they send an e-mail to the customer.<sup>352</sup>

Unlike the E.U. framework, however, the Act should include other categories besides business relationships stemming from previous transactions involving the sale of products and services. The current Act excludes at least one type of business relationship that does not stem directly from a sale of a product or service by allowing employers to send messages to their employees that provide information regarding employment relationships or benefit plans. It could also make exceptions for other categories, such as e-mail sent to potential customers who attended a company event. Any categories relating to potential customers, however, would have to be based on some point of contact or relationship brought on by the recipient, such as the voluntary attendance at an event, in order to prevent the opt-in mechanism from losing its bite.

---

<sup>347</sup> 15 U.S.C. § 7702(17)(B).

<sup>348</sup> Council Directive 2002/58, *supra* note 9, at Art. 13 §2.

<sup>349</sup> *See id.*

<sup>350</sup> *See id.*

<sup>351</sup> 15 U.S.C. § 7702(17)(A).

<sup>352</sup> Council Directive 2002/58, *supra* note 9, Art. 13 §2.

Further, while the Act should require that only the company that collected the information could send e-mail, it should not require that the e-mail relate to products or services that are similar to the one the customer purchased in past transactions. Even if the e-mail is sent to a potential customer who consented to receive marketing e-mail, there should be no restriction on the type of products or services the company can promote, as long as they are that company's products and services.

This broadening of the E.U. exception makes sense since the customer will have to permit the company to send it marketing e-mail in the first place. Doing otherwise would be an unnecessary restraint on legitimate advertising. This way, users will still recognize the sender as an entity with whom they have done business in the past and to whom they consented to receive marketing e-mails, making it more likely that the message will be desired, viewed and responded to. Moreover, with less restraint on the type of transaction and the type of marketing e-mail the company must send, companies will be able to more effectively do e-business. Business-savvy companies may choose to allow customers or potential customers to select the kind of marketing e-mail they wish to receive by offering the customer a list of products or services, and offering to limit the recipient's consent to that category, so that the company can take the most advantage of the customer's consent while ensuring that customer does not receive undesired e-mail.

### 3. Harvesting

The current version of CAN-SPAM contains only a weak prohibition on harvesting, contingent on violations of other parts of the anti-spam law.<sup>353</sup> This weak provision neither prohibits automated alphanumeric creation of addresses and harvesting, nor requires harvesting consent from users. Instead, the prohibition only holds in cases where either the address was used to send spam that violated the Act to addresses that were alphanumerically created by automated means or the website or service from which the information was taken posted a notice prohibiting the harvesting of the addresses. These requirements place a significant burden on both individual web-site creators and ISPs to place notices on all websites that contain e-mail addresses, a burden that is counter-productive and wholly unnecessary.

The law should instead prohibit harvesting altogether, or at the very least, prohibit harvesting if the spammer used the address to send commercial e-mail that violated the opt-out rules of the current Act without the notice or address creation conditions mentioned above. In any case, website notices should play no role in the rules on harvesting. There is no reason for this additional complexity, which can only serve to create confusion.

The main rule regarding harvesting should instead relate to the exception to the opt-in rule. The only legitimate way for companies to acquire e-mail

---

<sup>353</sup> 15 U.S.C. § 7704(b)(1)(A).

2004]

*SPAM IN A BOX*

contact information should be when dealing with a customer or a potential customer (in the situations described in the exception), if the recipient has the clear and distinct opportunity to object to use of the contact information for direct marketing purposes at the time of the sale, and as long as an easy opt-out mechanism that is free of charge is available each time e-mail is sent to the recipient.<sup>354</sup> Such a strong prohibition on harvesting is desirable because spammers who attempt to evade the opt-in law but who have only a few addresses at hand, would be forced to break the law again by either randomly generating or harvesting the addresses. The spammers would thus face double liability and hopefully be more heavily deterred from future violations. The U.S. should, therefore, implement a rule on harvesting similar to that in the E.U., and users should be able to determine where and to whom personal information flows.<sup>355</sup>

4. Wireless

The F.C.C. must decide on rules to protect the public from unwanted cellular spam.<sup>356</sup> An opt-out mechanism would not stop the flood of spam that is ever increasing in the cellular phone context, while some worry that a complete opt-in system would prevent subscribers' ability to receive commercial area-sensitive information. In deciding whether to require this of mobile service providers, the F.C.C. must consider the relationship that exists between mobile service providers and their subscribers.<sup>357</sup> Because Docomo was forced to take technology-based steps immediately after the Japanese opt-out legislation went into effect, an opt-out procedure alone is clearly not enough to solve the problem of cellular spam. This suggests that an opt-out system will not be effective.

Although a mobile service provider's technology, in combination with legislation, has at least some possibility of being fair and effective, the steps Docomo has taken failed to protect the legitimate interests of the business community. Even a strong anti-spam law should allow businesses to send e-mail in legitimate circumstances: where they were requested to send it or where they sent it to potential (in certain cases) or former customers who willingly supplied their contact information. In addition, requiring big mobile service providers to take anti-spam steps will place a large burden on them, one that will leave no room for new competitors or uniformity with smaller competitors, and possibly even antitrust problems.

The conclusion, therefore, is that the best option is to create a strong opt-in system by simply making all cellular spam illegal, except for commercial

---

<sup>354</sup> Council Directive 2002/58, *supra* note 9, Art. 13 §2.

<sup>355</sup> *See id.*

<sup>356</sup> 15 U.S.C. § 7712(b).

<sup>357</sup> 15 U.S.C. § 7712(b)(2).

messages that fit the exception categories. Although some worry about the effect of preventing the ability to receive commercial area-sensitive information, subscribers who desire such information can still request it under an opt-in regime. An opt-in regime would be the best weapon against cellular spam and one that the U.S. should consider adopting in the next several months.

#### 5. Enforcement

The law can only work when enforcement is thorough and quick. If it is easier to identify e-mail that does not comply, then enforcement will also be easier. Under the current law, many spammers are not convinced that they will be caught and prosecuted. Many use “compliance” mechanisms that will evade detection in the first place.<sup>358</sup> Since many never test the opt-out mechanism for fear of confirming the existence of their e-mail address and adding to spammers’ database of usable addresses, often spammers who do not comply are never discovered.<sup>359</sup> Under an opt-in system, however, many of these problems disappear. Users will recognize any deviant commercial e-mail more easily because they will not recognize the sender company, whether it is labeled as spam or not.

Of course, in order for users to recognize that this spam is illegal, they must be familiar with and properly informed of the law. The F.T.C., along with ISPs, therefore, should work to inform users of the law through media coverage, press releases, and postings on e-mail services. ISPs or e-mail services especially have a responsibility to make every user aware of what exactly is illegal and subject to penalty. This information should be available on one of the main e-mail web pages that users must view in order to use their e-mail accounts. All of the rules should be in laymen’s terms so that a quick scan will let a user know what is illegal and how to respond.

In addition, although a private right of action would flood the courts with litigation, users should be provided with a quick and easy way of reporting spam that violates the law so either ISPs, the F.T.C. or state attorneys generals can sue on their behalf. ISPs should add a link so that users can access the reporting system via an easy click, or simply check a box next to the spam e-mail. It would also be a good idea to inform users of court cases against spammers and their outcomes in a simple scrolling text across the top of e-mail pages. Further, all commercial e-mail that is sent under an exception should have a label so it could be sent to a “commercial e-mail in-box.” Although users may still end up sorting through spam for a while, if the reporting system is used, and quick and strong enforcement with civil and criminal liability

---

<sup>358</sup> See Press Release, *supra* note 21, at [http://biz.yahoo.com/prnews/040202/sfm067\\_1.html](http://biz.yahoo.com/prnews/040202/sfm067_1.html).

<sup>359</sup> See Rollins, *supra* note 179, at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nc20030327mr.htm>.

2004]

SPAM IN A BOX

follows, then eventually fear will be instilled in spammers and the quantity of spam will decrease.

*B. Global Harmonization and Technological Innovation*

1. Pursuing Global Harmony

One of the major problems relating to anti-spam legislation is that the Internet is global, while the spam laws are local.<sup>360</sup> Finding Twelve of the current Act points to the necessity of an international solution, or at least “cooperative efforts with other countries,” and that is indeed necessary for strong anti-spam legislation to have any real effect.<sup>361</sup> No matter how strict the spam laws of one country appear, they can never completely eliminate spam without global cooperation. Indeed, Internet access is now available in two hundred countries and likely to spread.<sup>362</sup> While February 2004 statistics show that the U.S. is by far the biggest source of spam,<sup>363</sup> spam can and does come from other countries as well, or is rerouted through other countries from U.S. sources.<sup>364</sup> In fact, many spammers have set up shop recently in China,<sup>365</sup> Thailand and other foreign countries in order to avoid CAN-SPAM.<sup>366</sup> Because of the lack of uniformity, spammers often send from the location with the most favorable laws, creating a spammer “haven.”<sup>367</sup> The lack of uniformity makes enforceability not only difficult, but also confusing.

Indeed, there has been little uniformity of laws among the top spammers in

<sup>360</sup> *But see, e.g.,* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001).

<sup>361</sup> 15 U.S.C. § 7701(a).

<sup>362</sup> OECD, *OECD Calls on Governments to Step Up Their Fight Against Spam* (Feb. 2, 2004), [at](http://www.oecd.org/document/17/0,2340,en_2649_201185_26198225_1_1_1_1,00.html) [http://www.oecd.org/document/17/0,2340,en\\_2649\\_201185\\_26198225\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/17/0,2340,en_2649_201185_26198225_1_1_1_1,00.html).

<sup>363</sup> United States, 56.74%; Canada, 6.80%; China (including Hong Kong), 6.24%; South Korea, 5.77%; TechWeb, *supra* note 163, *at* [http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040227/tc\\_cmp/18200812](http://story.news.yahoo.com/news?tmpl=story&u=/cmp/20040227/tc_cmp/18200812).

<sup>364</sup> *See* Wright, *supra* note 51, *at* [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>365</sup> *See* news24.com, *supra* note 166, *at* [http://www.news24.com/News24/Technology/News/0,,2-13-1443\\_1486065,00.html](http://www.news24.com/News24/Technology/News/0,,2-13-1443_1486065,00.html). The Chinese government, confronted with over seventy million pieces of spam getting through to the country’s users, now sees spam as a political threat. *See* Associated Press, *China Sees Spam As Political Threat* (Feb. 5, 2004), *at* [http://www.unspam.com/fight\\_spam/articles/1283.html?ses=8Abz2-x9s1t6\\_GWUe-5HxJSB1o\\_ZWJtyj8hBEI7Wi](http://www.unspam.com/fight_spam/articles/1283.html?ses=8Abz2-x9s1t6_GWUe-5HxJSB1o_ZWJtyj8hBEI7Wi).

<sup>366</sup> *See* Wright, *supra* note 51, *at* [http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc\\_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail](http://story.news.yahoo.com/news?tmpl=story&u=/usatoday/20040225/tc_usatoday/withantispamlawineffectcompaniesworktofoiljunkemail).

<sup>367</sup> *See id.*

the world. China, a country with eighty million Internet users, the second biggest production of spam after the U.S., and users who receive more spam than e-mail, is expected to pass anti-spam legislation by the end of 2004.<sup>368</sup> Legislation efforts by China's Ministry of Public Service, which will give most of the responsibility for handling spam to ISPs and aim for new Internet security measures, began after international complaints were voiced.<sup>369</sup> Chinese government officials became frustrated because their own e-mails were blocked and they began to see some politically "reactionary" spam.<sup>370</sup> Some argue that the spam originating in China is actually originating from elsewhere because Western spammers were selling lists of Chinese vulnerabilities and systems administrators were unable or unwilling to secure the servers.<sup>371</sup> The solution, many say, will come from increased security measures and more regulation.<sup>372</sup>

Meanwhile, South Korea has taken innovative, yet questionable steps to combat spam recently. South Korea, which is the fourth biggest spam producer, has plans to invest ten billion Korean Won by 2007 to help curb the spam problem by increasing penalties and prohibiting spam that is sent at night.<sup>373</sup> South Korea's plan, however, is problematic for it fails to recognize that much of its spam comes from spammers from other parts of the world who hack into South Korean computers and who would not respect South Korea's nighttime rule.<sup>374</sup>

Australia's new Spam Act, which will come into effect on April 11, 2004, prohibits any spam via e-mail or cellular phone that contains an Australian link, and spammers will be subject to around eight hundred thousand dollars (U.S.) per day.<sup>375</sup> Australia plans to inform the public about its new legislation and about spam with a one-year campaign.<sup>376</sup> Australia's law, as well as the E.U.'s Directive, should be held out as an example of the type of anti-spam law

---

<sup>368</sup> See Rebecca Bolin, *Spam Laws Worldwide: China* (Feb. 17, 2004), at <http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1340>; *China to Issue Anti-spam Legislation in First Half of 2004* (Feb. 2, 2004), at <http://www.interfax.com/com?item=Chin&pg=0&id=5685285&req=>.

<sup>369</sup> See Bolin, *supra* note 368, at <http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=1340>.

<sup>370</sup> See *id.*

<sup>371</sup> See *id.*

<sup>372</sup> See *id.*

<sup>373</sup> Sophos, *No spam at night? South Korea Reveals Anti-spam Plan* (Feb. 27, 2004), at <http://www.sophos.com/spaminfo/articles/spamatnight.html>.

<sup>374</sup> See *id.*

<sup>375</sup> ZDNet, *Australia's Spam Act to Become Law in April*, *supra* note 9, at [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

<sup>376</sup> See *id.* See Caube.AU, *Spam Law Passes the Federal Parliament*, at <http://www.caube.org.au/> (last visited Mar. 15, 2004).

2004]

SPAM IN A BOX

that, if passed everywhere, or at least in the U.S. as it is the largest source of spam, would significantly decrease the amount of spam flowing through the system. Until the rest of the world makes stronger anti-spam legislative commitments, however, the world will not be able to defeat the spam monster.

A lack of legal uniformity among countries and an array of weak anti-spam legislation, however, are only some of the problems that must be examined on an international level. According to the Australian Minister for Information, Technology and Communications, even the strong Australian anti-spam legislation will not be effective without international cooperation and enforcement coordination.<sup>377</sup> Countries from around the world need to create a world in which spammers who do not heed the law will easily stand out as the eyes of the whole world watch out for them together.

There is a general consensus that a holistic approach to the spam problem is necessary, and that such an approach would initially require an open forum for discussion between governments, businesses and other interested parties. In addition to the global encouragement of strong anti-spam laws, goals include coordinated research efforts, end-user education, enforcement efforts, and the use of technology solutions. Even the U.S. has recognized that global efforts such as workshops are needed to win the war against spam.<sup>378</sup>

To work toward its goal of international cooperation, Australia attended the Organisation for Economic Co-operation and Development (OECD) Workshop in February 2004. The goal of this workshop was to discuss multilateral anti-spam approaches.<sup>379</sup> The OECD spam working group is one example of a way for different countries to come together to discuss cooperation in this early stage in the global spam fight. The OECD spam working group, which seeks to increase efforts to improve cross-border cooperation in order to protect the integrity of the Internet, has members from thirty developed countries, and the OECD generally has been successful in creating influential guidelines for computer security, online privacy and Internet consumer protection standards.<sup>380</sup> The OECD provides an organized forum for discussion between governments, businesses and other stakeholders, and is an ideal platform for the development of international spam policies.<sup>381</sup> The OECD would like to encourage global coordination in areas such as research and information gathering, education and awareness, self-regulation, the development of

---

<sup>377</sup> ZDNet, *Australia's Spam Act to Become Law in April*, *supra* note 9, at [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

<sup>378</sup> See Press Release, *supra* note 172, at <http://www.tmcnet.com/usubmit/2004/Jan/1022594.htm>.

<sup>379</sup> ZDNet, *Australia's Spam Act to Become Law in April*, *supra* note 9, at [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

<sup>380</sup> OECD, *supra* note 362, at [http://www.oecd.org/document/17/0,2340,en\\_2649\\_201185\\_26198225\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/17/0,2340,en_2649_201185_26198225_1_1_1_1,00.html).

<sup>381</sup> See *id.*

coordinated technical solutions, and international cooperation in enforcement of national laws.<sup>382</sup>

In addition, the European Commission, recognizing that international cooperation is necessary, organized a European workshop on spam in October 2003.<sup>383</sup> The workshop, which took place in Brussels, included discussions involving representatives from industry, consumer associations and individual Member States.<sup>384</sup> In January 2004, the E.U. revealed its new plan with which it will supplement its strong legislation.<sup>385</sup> Not only did the E.U. agree to create an agency to improve Internet security, but it intends to aim for greater enforcement, consumer information and international cooperation to combat spam.<sup>386</sup>

Workshops such as these create an appropriate forum for discussion among many groups in order to solve the spam problem. In addition to working groups and organizations that will help push for general international cooperation, however, it is important to consider more specific bilateral and multilateral methods of cooperation as well.<sup>387</sup> Even the two-year study ordered by CAN-SPAM requires an analysis of how to address the lack of uniformity problem and the problem of spam that originates in foreign countries.<sup>388</sup> The Act requires that this analysis include “initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions.”<sup>389</sup>

It is clear to many, therefore, that, in addition to an open forum for discussion, more specific bilateral and multilateral cooperation will aid in the creation of a united global effort to end the spam problem. Notably, Australia has signed an agreement with the Korean Information Security Agency to cooperate on spam-related issues.<sup>390</sup> The creation of such bilateral agreements will aid in creating global uniformity one step at a time. As more and more bilateral agreements emerge, there will be room for the negotiation of multilateral agreements. If an increasing number of bilateral agreements are entered into with the understanding that the efforts to curb the spam problem are also efforts to prevent the erosion of consumer confidence in the digital

---

<sup>382</sup> *See id.*

<sup>383</sup> Fried, *supra* note 219, *at* <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=18707>.

<sup>384</sup> *See id.*

<sup>385</sup> *See* Associated Press, *supra* note 247, *at* <http://www.iht.com/articles/126894.html>.

<sup>386</sup> *See id.*

<sup>387</sup> Fried, *supra* note 219, *at* <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=18707>.

<sup>388</sup> 15 U.S.C. § 7709(b).

<sup>389</sup> *Id.*

<sup>390</sup> ZDNet, *Australia's Spam Act to become law in April*, *supra* note 9, *at* [http://news.com.com/2100-1028\\_3-5129683.html](http://news.com.com/2100-1028_3-5129683.html).

2004]

*SPAM IN A BOX*

economy and the open character of the Internet,<sup>391</sup> then the parties that enter into bilateral agreements may soon discover that broader agreements are possible. In the future, perhaps World Trade Organization members, or even a larger set of countries will create far-reaching treaty provisions that will help end the global spam problem.

In addition, the implications of a global cooperation take on a greater importance in light of the recent war in Iraq and possible uses of spam during conflict in the future. The U.S. launched its first military spam offensive ever in order to persuade Iraqi senior officials and military to defect.<sup>392</sup> The propaganda messages, which were in Arabic and titled “Important Information,” included a guide on how to defect, an appeal to turn over any information on Iraq’s supposed chemical and biological weapons program to UN inspectors and an urge to personnel to disable any weapons of mass destruction or refuse to use them in the event of war.<sup>393</sup> In response, Iraq shut off some of its Internet gateways.<sup>394</sup> One can easily imagine how spam could be used in large quantities to force a country to shut down its Internet connections altogether, with potentially financially devastating results. Global initiatives should thus consider spam not only as a threat, but as a potential weapon, in attempting to create a global spam resolution.

2. Using New Technology to Aid in the Fight Against Spam

In addition to strong domestic legislation and global efforts, new technology solutions will also help to curb the spam problem. Finding Twelve of the current Act points to the necessity of technological mechanisms to fight spam as well as an international cooperation.<sup>395</sup> The two-year study that will take place under CAN-SPAM requires “an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act.”<sup>396</sup> Certainly, the spam problem is spreading to new devices, such as the recent instant messaging “spim” phenomenon,<sup>397</sup> and may soon spread even further. One other way that new technology can play a role, however, is either as an alternative to strong legislation, or, preferably, as a method by which to

<sup>391</sup> OECD, *supra* note 362, at [http://www.oecd.org/document/17/0,2340,en\\_2649\\_201185\\_26198225\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/17/0,2340,en_2649_201185_26198225_1_1_1_1,00.html).

<sup>392</sup> See John Leyden, *US. Mil Launches Operation Desert Spam* (Jan. 13, 2003), at <http://www.theregister.co.uk/content/6/28839.html>.

<sup>393</sup> See *id.*, at <http://www.theregister.co.uk/content/6/28839.html>.

<sup>394</sup> See *id.*, at <http://www.theregister.co.uk/content/6/28839.html>.

<sup>395</sup> 15 U.S.C. § 7701(a).

<sup>396</sup> 15 U.S.C. § 7709(b).

<sup>397</sup> Swartz, *supra* note 18, at [http://www.usatoday.com/tech/news/2004-03-01-spim\\_x.htm](http://www.usatoday.com/tech/news/2004-03-01-spim_x.htm).

supplement strong legislation to help defeat spam.

Every day, companies are developing new technologies to combat spam. For a long time, some have suggested revamping the e-mail system by charging a postage fee of a penny or less for e-mail.<sup>398</sup> At the World Economic Forum in January 2004, Microsoft chairman Bill Gates, along with his team of researchers, suggested that instead of a penny fee, senders would instead have to devote ten seconds of time to a simple math puzzle or other such activity so that the senders can show their good faith.<sup>399</sup> Companies like Goodmail Systems, along with Yahoo and some others, are still considering charging bulk mailers a penny to prevent their mail from being sent to the bulk folder.<sup>400</sup> Some even suggest allowing recipients to set the cost of e-mail that they will accept so that busy executives could choose to receive only e-mail that cost the sender a high price to send in order to avoid spam.<sup>401</sup>

Though such tactics would likely devalue the e-mail system and would be difficult to implement globally,<sup>402</sup> it is only a matter of time until a truly effective technology-based solution is discovered. One way that technology would certainly be useful as a supplement to legislation is to aid in the effort to find spammers. Recently, Bill Gates unveiled a new “caller ID for e-mail” plan.<sup>403</sup> Yahoo and America Online are also working to create a sender authentication system.<sup>404</sup> If such plans are successful, then spammers will not be able to hide from the law, and enforcement of tough anti-spam laws will become much easier.

## VII. CONCLUSION

Spam is out of control. If the U.S. fails to make changes to CAN-SPAM, spam will increase exponentially in the next decade. Legislators must find a way to prevent spammers from inundating Internet users with useless information that will deplete the Internet of its purpose. Current ISP filtering systems are only semi-effective in blocking spam and they inevitably block out legitimate business e-mail accidentally. Further, those who take spammers to court have only been successful in obtaining injunctions in very limited situations.

The burden of overflowing inboxes and the high cost of handling spam, in

---

<sup>398</sup> See Associated Press, *Gates: Buy Stamps to Send E-mail* (Mar. 5, 2004), at <http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/index.html>.

<sup>399</sup> See *id.*

<sup>400</sup> See *id.*

<sup>401</sup> See *id.*

<sup>402</sup> See *id.*

<sup>403</sup> See Mike Langberg, *supra* note 203, at [http://story.news.yahoo.com/news?tmpl=story&u=/sv/20040227/tc\\_sv/optimismgrowsinfightagainsttorrentofspam](http://story.news.yahoo.com/news?tmpl=story&u=/sv/20040227/tc_sv/optimismgrowsinfightagainsttorrentofspam).

<sup>404</sup> See *id.*

2004]

*SPAM IN A BOX*

addition to the burden of taking legal action, suggest that communication between companies alone is not enough. Spammers will find ways to avoid falling within the sphere of the case law or simply choose to ignore the law in hopes of not being brought to court. Although several companies have developed more creative strategies to curb spam, these strategies are not feasible for general use and only demonstrate that users, service providers and businesses desperately need effective legislation.

Unfortunately, the U.S. has created federal legislation that will accomplish very little if it is not changed. The array of problems that have arrived in the wake of CAN-SPAM should lead Congress to conclude that the current version of the Act is mightily lacking. An examination of legislation in the E.U. and Japan provides some guidance in ways to improve CAN-SPAM. The E.U. has developed a strong anti-spam opt-in law that has a high likelihood of decreasing spam. Japan has also passed legislation that, while not as strong on its face as its E.U. counterpart, shows why an opt-in style of regulation for wireless spam is the most effective way to curb wireless spam. The U.S. should learn from the E.U. and Japan in order to make serious changes to its law in order to help reduce spam.

In light of the E.U. legislation, the U.S. should consider an opt-in structure with a modified version of the E.U. exception, a complete prohibition on harvesting and directory listings without consent, and an opt-in framework for cellular spam. Japan's current system provides evidence that instead of taking a softer approach to cellular spam, the U.S. should choose a strong opt-in framework. Further, although CAN-SPAM allows for a possible future implementation of a national do-not-email registry,<sup>405</sup> doing so will likely prove counterproductive. In addition, enforcement mechanisms should be improved through increased public awareness and a more accessible violation reporting system.

Now, the U.S. has the perfect opportunity to join the world in the fight against spam.

The nature of spam requires that, in addition to the U.S., other countries also make stronger anti-spam legislative commitments as well, and that the whole world embark on a path of international cooperation, while remaining open to new technological solutions, in order to finally defeat the spam monster.

The creation of a strong global legal standard will create uniformity and thus help eliminate spam on a much larger scale since spammers would face the same restrictions worldwide and coordinated enforcement procedures. In addition, technical solutions may be able to aid in locating spammers and easing the burden of enforcing strong anti-spam laws. Anti-spam work groups and organizations will create an ideal platform for discussing the spam problem, and bilateral and multilateral agreements will help create a stable and uniform front. Eventually, a global resolution may emerge to help curb the

---

<sup>405</sup> 15 U.S.C. § 7708.

spam problem. A strong, global resolution that aims to protect consumers and service providers from out-of-control spammers, while allowing for companies to make legitimate use of the Internet, will be the real sword that strikes down the spam monster once and for all.