UNTOUCHABLE?:
A CANADIAN PERSPECTIVE ON THE ANTI-SPAM BATTLE

Michael Geist·

Version 3.0

Forthcoming 3:1 University of Ottawa Law and Technology Journal (2005)

· Canada Research Chair in Internet and E-commerce Law, University of Ottawa, Faculty of Law. The author is a member of the Minister of Industry's National Task Force on Spam. The opinions expressed herein are personal and do not necessarily reflect the views of the University of Ottawa, the Task Force, nor the Government of Canada. The author would like to thank Milana Homsi, Warren Yeung, Sukesh Kamra, Candice Teitlebaum, and Dahlia Tessler for their research assistance, two anonymous reviewers for their suggestions, Rene Geist for her editorial comments, and the participants at the February 2004 OECD Workshop on Spam and the 12th Annual Law Society of Upper Canada's Communications Law conference for the terrific insights into spam-related issues. The author gratefully acknowledges the financial support of the Canada Research Chair program, the Social Sciences and Humanities Research Council of Canada Initiative on the New Economy, and the Ontario Premier's Research Excellence Award program.

On April 12, 1994, Laurence Canter, an Arizona immigration lawyer, wrote a small computer program that sent thousands of messages to online message boards advertising his law firm's services. The burgeoning Internet community immediately registered its disapproval of the practice and the ensuing discussion adopted the term "spam" to describe the unsolicited, commercial email. The negative reaction notwithstanding, Canter claimed that his marketing efforts were successful, generating thousands of dollars in new business.[1]

More than ten years later, it would appear that only the names and numbers have changed. Spam has moved to the forefront of Internet policy as millions of Internet users, now overwhelmed with the billions of spam messages sent daily, begin to question the reliability of email. Spamming organizations, meanwhile, continue to push the envelope, unveiling ever more creative ways to send spam in the hope of generating the tiny positive response rate needed to profit from this dubious side of Internet business. The result is a troubling conundrum for policy makers, Internet service providers, e-commerce companies, and Internet users grappling with the by-products (such as lost confidence, frustration, and fraud) of a spam epidemic that reportedly brings $250 million in income to spamming organization yet costs society as much as $87 billion in lost productivity and associated expenses.[2]

According to Brightmail, an anti-spam service provider, spam accounted for eight percent of all U.S. e-mail traffic in 2001, 36 percent in 2002[3] and 60 percent of all email in January 2004.[4] Some estimate that by 2006, spam will be responsible for 95 percent of all

---

[1] Paul Festa & Evan Hansen, "Happy Spamiversary", (12 April 2004), online at http://www.zdnet.com.au/news/security/0,2000061744,39144765,00.htm (last visited 12 April 2004).

[2] United States Telecom Association, Unsolicited Commercial Email, online: http://www.usta.org/index.php?urh=home.advocacy.industry_issues.ii_spam, (last visited 12 April 2004).

[3] "One-third of e-mails are spam" CBC News (30 Aug 2002), online: CBC News <http://www.cbc.ca/storyview/CBC/2002/08/30/Consumers/spamstats_020830> (last visited: 1 July 2003).

[4] S. Olsen, "Study: Spammers Turning Blind Eye To The Law" (10 February 2004), online: CNET < http://news.com.com/2100-1032-5156629.html> (last visited: 11 April 2004) (herinafter Olsen).

email traffic.[5] In 1999, the average e-mail user received 40 spam messages per annum; in 2004 that number surpassed 2,500.[6]

Public annoyance with spam is also on the rise. According to a poll of 2,200 U.S. adults conducted by Harris Interactive in 2003, 80 percent thought that spam was "very annoying", an increase from 49 percent who responded that way in 2000. Seventy-four percent believed that mass spamming should be made illegal. The poll showed that the most annoying spam messages were those related to pornography (91 percent), followed by mortgage and loan offers (79 percent), investments (68 percent) and real estate (61 percent). There was broad support for taking legal action to stop spamming, with between 70 – 80 percent support from respondents in all age groups, income brackets, sexes, races and political parties.[7]

Many ISPs are attempting to block spam from reaching their users' mailboxes. AOL claims to have blocked 1.2 billion spam e-mails per day from reaching its users' inboxes in late 2004, a decline from 2.4 billion per day in the previous year.[8] Hotmail and MSN also utilize spam filters; their servers block 2.4 billion messages a day from reaching subscribers' inboxes.[9] Government departments have also received more spam complaints. The Federal Trade Commission's spam database received more than 100 million spam messages in 2004 alone.[10]

---

[5] R. Jaques, Spam Approaches 95 Percent of All Email, E-commerce Times (7 February 2005), online at < http://www.ecommercetimes.com/story/Spam-Approaches-95-Percent-of-All-E-mail-40358.html>, (last visited 11 February 2005).
[6] Olsen, supra.
[7] B. Morrissey "Spam Annoyance on the Rise" Internetnews.com (3 January 2003), online Internetnews.com <http://www.internetnews.com/IAR/article.php/1564101> (last visited: 1 July 2003).
[8] M. Musgrove, AOL Reports Decline in Spam in the Past Year, Washington Post (27 December 2004), online at < http://www.washingtonpost.com/wp-dyn/articles/A30433-2004Dec27.html> (last visited 14 February 2005).
[9] B. Gates "Why I Hate Spam" Microsoft (23 June 2003), online: Microsoft <http://www.microsoft.com/presspass/ofnote/06-23wsjspam.asp> (last visited: 1 July 2003).
[10] K.B. Vlahos, Spam Still Strong Despite Law, Fox News (11 February 2005), online:< http://www.foxnews.com/story/0,2933,147056,00.html> (last visited: 14 February 2005).

The growth of spam comes at an increasing cost as the annual expense associated with managing spam have risen 500-700 percent over the last three years with annual ISP costs per customer averaging between US$3-$5. This cost includes system overhead, anti-spam software, personnel, educational materials, and customer support.[11] A representative from Nortel Networks states that while one might expect a company such as Nortel to benefit from spam by selling more hardware and equipment to deal with the increased bandwidth, spam instead has a chilling effect on the industry as a whole.[12]

John Levine, an Internet expert and chair of the Internet Engineering Task Force's Working Group on Spam, succinctly summarizes the problems associated with spam in the following manner:

1) The recipient [and ISP] pays far more, in time and trouble as well as money, than the sender does, unlike advertising through the postal service;
2) The recipient must take the time to request removal from the mailing list, and most spammers claim to remove names on request but rarely do so [violation of privacy];
3) Many spammers use intermediate systems without authorization to avoid blocks set up to avoid spam;
4) Many spam messages are deceptive and partially or entirely fraudulent [criminal or quasi-criminal in nature];
5) Spammers often use false return addresses to avoid the cost of receiving responses;
6) Some forms of spam are already illegal in various jurisdictions in the United States (http://spam.abuse.net/spambad.html). [13]

[11] D. Malik "Notes for 'Economics of Spam' Panel" BellSouth (30 April 2003), online: Federal Trade Commission < http://www.ftc.gov/bcp/workshops/spam/Presentations/malik.pdf> (last visited: 1 July 2003).
[12] FTC Spam Forum, Day 2, online: Federal Trade Commission <http://www.ftc.gov/bcp/workshops/spam/> at pg. 74 (last visited: 1 July 2003).
[13] As quoted in 1267623 Ontario Inc. v. Nexx Online Inc., [1999] O.J. No. 2246 (Sup. Ct).

The exponential growth of the spam problem in recent years has been accompanied by an urgent desire to identify global solutions to stem the tide. Where once industry and many policy makers opposed governmental intervention, today there is near-unanimous support among key stakeholders for a private-public anti-spam partnership that includes legal measures as an essential part of the response.

This paper argues that the emerging global anti-spam law and policy framework can be traced through three phases. The first phase, which began with the Canter email and continued until early 2000, was marked by both a relatively limited concern for the impact of spam and a perception that the marketplace could successfully address the issue.

The second phase, which began by taking the first steps toward more aggressive anti-spam solutions in early 2000 and continued until late 2003, saw the widespread adherence to a three-part anti-spam solution comprised of education, technology, and legal solutions. This phase acknowledged that government had a role to play in combating spam but was careful to assert that the private sector should continue to maintain the lead on the issue.

The third phase, which began in 2004, continues to shift toward greater governmental involvement as the weaknesses of the education, technology, and law strategy emerge and the dangers associated with spam increase. The paper concludes that the unfolding anti-spam strategy will see the anti-spam issue for what it is – an enforcement problem that requires significant governmental involvement at both the national and international levels.

Phase One – Spam as an Annoyance

Although anti-spam groups began forming as early as 1995,[14] the issue did not attract significant policy attention until several years later. U.S. Congressional attempts to introduce anti-spam legislation in 1998 and 1999 with such laws as the Inbox Privacy Act failed to garner significant support, as critics argued that the bills constituted a significant incursion into free speech rights.[15] Anti-spam legislative advocates enjoyed greater success at the U.S. state level where states such as Washington and California became early adopters of anti-spam legislation.[16]

Canada was even slower to get off the mark on the spam issue as Industry Canada waited until July 1999 to release its first policy position paper on spam.[17] The paper canvassed the legal and marketplace framework, including consumer choices amongst a competitive ISP market, privacy legislation, civil remedies, and the applicability of the criminal code, and concluded that:

> The federal government believes that its current policy and legal frameworks will continue to foster strong Internet growth and development in Canada while at the same time dealing adequately with computer abuse and criminal activity. Spam is but one of the new elements emerging from increased Internet growth and development. The government believes that an appropriate mix of policies and laws, consumer awareness, responsible Internet industry stakeholders and technological solutions is the best and most appropriate way to deal with behaviour in the new and evolving on-line environment. The government believes that Canada has this right mix today but will continue to monitor developments and consider changes if they are required.

The Canadian government's perspective on spam was consistent with its broader policy approach of minimal government intervention into Internet matters. It preferred instead

---

[14] The Coalition Against Unsolicited Commercial Email (CAUCE), a leading grassroots anti-spam group, has its origins in SPAM-L, an anti-spam mailing list that was formed in 1995. See >http://www.claws-and-paws.com/spam-l/spam-l.html> (last visited: 11 April 2004).
[15] C. Macavinta, Lawmakers Try New Spam Bill, CNET (31 March 1999), online at http://news.com.com/2100-1023-223735.html , (last visited 11 April 2004).
[16] J. Kornblum, Washington State Joins Spam War, CNET (25 March 1998), online at < http://news.com.com/2100-1033-209532.html>, (last visited 11 April 2004).
[17] Internet and Bulk Unsolicited Electronic Mail, online at http://e-com.ic.gc.ca/english/strat/spam.html (last visited: 9 August 2003).

to allow the private sector to take the lead. Buoyed by the perceived potential of e-commerce and claims that governmental intervention would serve only to stifle the development of the Internet, governments were generally only too happy to defer to self-regulatory frameworks that left policy leadership to the private sector.

In July 1997, for example, President Clinton released a report entitled Framework for Global Electronic Commerce, articulating guiding policy principles, including private sector leadership; avoidance of undue governmental restrictions on e- commerce; the enforcement of a predictable, minimalist, consistent, and simple legal environment for commerce; the recognition of the unique qualities of the Internet; and the facilitation of electronic commerce on a global basis.[18] The European Union declaration, released one week after the U.S. framework, followed the United States' lead and called for, among other things, a key role for the private sector, the development of a clear and predictable regulatory framework, and the recognition of the special characteristics and fundamentally transnational nature of the Internet.[19]

Not surprisingly, global corporations encouraged the self-regulatory approach. For example, the Global Business Dialogue on E-Commerce (GBDe), an e- commerce corporate policy and lobbying group with dozens of multinational corporations among its membership, maintained,

> [T]he pace and scope of change requires business to play a leadership role in working with governments, governmental organizations, business groups, consumer organizations and other stakeholders to develop an effective e-commerce framework that is global, market-driven and flexible .... [E]-commerce policy solutions should be market-driven and based on industry self-regulation wherever possible.

---

[18] President William J. Clinton & Vice President Albert Gore, Jr., Framework for Global Electronic Commerce (July 1, 1997), at http:// www.ta.doc.gov/digeconomy/framewrk.htm (last visited Feb. 3, 2003); see Memorandum on Electronic Commerce, 2 PUB. PAPERS 898, 899 (1997); see also U.S. INFO. AGENCY, A Framework for Global Electronic Commerce, GLOBAL ISSUES, Oct. 1997, at 33, 34 (summarizing principles outlined in the Framework), available at http://usinfo.state.gov/journals/itgic/1097/ijge/ijge1097.pdf.

[19] See Ministerial Declaration from European Ministerial Conference (Bonn, Germany), Global Information Networks: Realising the Potential (July 6- 8, 1997) [hereinafter Ministerial Declaration], at http:// europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html.

> ... Conventional regulatory structures seem to be less capable of coping with the challenges of converging markets. The GBDe believes priority must be given to self-regulation and policy cooperation rather than over- regulation. Only in providing for continued market dynamism will a policy framework enable the converging process to realize its full potential, as well as allowing electronic commerce to reap the largest benefit from the convergence melting pot.[20]

The private sector, particularly ISPs, did indeed take the lead on the anti-spam front by deploying both technological solutions and launching legal actions. On the technological front, ISPs such as Compuserve began installing anti-spam filters in 1997 in an effort to stem the growing spam tide.[21] Anti-spam groups began developing lists of ISPs that they believed allowed spamming to originate from their systems along with the organizations responsible for sending spam. The worst ISP offenders were given the "Usenet Death Penalty" for allowing its members to send spam to newsgroups. Placement on the UDP would result in the blocking of messages from all of a given ISP's customers to Internet newsgroups, a development that ISPs took very seriously.[22] Organizations accused of sending spam were placed on "blackhole" lists. Thousands of ISPs worldwide subscribed to such lists and proceeded to block all email from servers included on the list.

Many other ISPs used legal tactics to challenge spamming activity. Trademark law was used in cases where spamming organizations used false information regarding the source, transmission path, and subject of the email message in an effort to evade ISP anti-spam filters. ISPs such as AOL successfully claimed that the unauthorized use of the AOL trademark within the email header constituted trademark infringement.[23]

---

[20] GLOBAL BUS. DIALOGUE ON ELEC. COMMERCE, GBDE 2000 BROCHURE 2, 7 [hereinafter GBDE 2000 BROCHURE] (on file with the author). Current information on the GBDe is available at http://www.gbde.org (last visited Mar. 2003).
[21] J. Kornblum, Compuserve Creates Spam Filter, CNET, online at < http://news.com.com/2100-1033-203571.html> (24 September 1997); last visited (11 April 2004).
[22] J. Kornblum, Compuserve Given Death Penalty, CNET, online at < http://news.com.com/2100-1023-205516.html> (18 November 1997); last visited (11 April 2004).
[23] AOL v. CN Productions, Civil Action No. 98-552-A (E.D. Va. 1998), online at < http://legal.web.aol.com/decisions/dljunk/cnprod.html>, (last visited: 17 January 2005).

Trespass to property was also successfully employed by ISPs, who argued that the transmission of email messages to their computer equipment, despite the existence of a contractual agreement prohibiting the practice and the installation of filters designed to block such incoming email traffic, constituted a trespass to personal property.[24]

The most egregious spamming organizations were occasionally hit with criminal actions. For example, AOL turned to the criminal provisions contained in the Computer Fraud and Abuse Act as well as the Virginia Computer Crimes Act in an action against LCGM in 1998.[25]

Canada's first criminal spam case did not commence until 2002. In R. v. Hamilton, a spammer who sent emails offering to sell documents detailing how to make homemade bombs, how to break into private homes, and how to generate credit card numbers, was charged under s. 464 of the Criminal Code, which states that it is a criminal offence to counsel indictable offences such as making explosive devices with intent to cause an explosion.

While the Crown had little difficulty in proving that the defendant met the active element of the charge by distributing the content, it failed to prove the equally important mental element of the crime. The court ruled that merely intending to counsel an indictable offense was insufficient.[26] Rather, the law requires the intent that the offence being counseled actually be committed. In this case, the court found that the spammer did not really intend for anyone to use the information he was selling. In fact, the spammer testified that he had never even read the bomb making material. Accordingly, the court ruled that the spammer's motivation was monetary rather than criminal so therefore the requirements under the statute were not met. The Supreme Court of Canada heard an appeal of the case in January 2005.

[24] Compuserve Incorporated v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).
[25] AOL v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).
[26] R. v. Hamilton, [2002] A.J. No. 30 (Alta QB).

Using contract law was another popular avenue for ISPs to shut down spamming organizations. For example, in 1999 I.D. Internet Direct Ltd., an Ontario ISP, obtained a court order restraining Corey Altelaar, a known spammer based in Ontario, from continuing to send spam messages through its system. The court reasoned that Altelaar had breached the terms of his email use agreement with the ISP.[27]

In the United States, the private lawsuits were supplemented by the Federal Trade Commission actions against the deceptive practices of some spamming organizations. The FTC launched its first anti-spam action in 1998, successfully requesting that a court permanently prohibit the seller of an alleged fraudulent business opportunity from spamming the Internet with his scheme.[28]

Not content to serve as legal target practice, several organizations accused of spamming sought to counter the lawsuits by bringing legal actions of their own against ISPs. In a Canadian case that attracted global attention, 1267623 Ontario Inc., an Oakville, Ontario company selling home furnishings via the Internet, sued Nexx Online, a Toronto-based ISP, for deactivating its webpage after the ISP received complaints that the customer was using its account to send spam. The ISP argued that it was entitled to cancel its service contract on the grounds that the contractual provision requiring account holders to follow "generally accepted Netiquette", or Internet etiquette, had been violated.[29] The court agreed, concluding that "sending unsolicited bulk commercial e-mail is in breach of emerging principles of Netiquette, unless it is specifically permitted in the governing contract."[30]

Not surprisingly, organizations accused of spam also objected to being included on blackhole lists, such as the Mail Abuse Prevention System's Real-time Blackhole List (MAPS RBL). In several instances, organizations launched lawsuits against the groups

[27] I.D. Internet Direct Ltd. v. Altelaar [1999] O.J. No. 1804 (Sup. Ct.).
[28] J. Kornblum, FTC Takes Spammer to Court, CNET (5 March 1998), online at < http://news.com.com/2100-1023-208774.html>, (last visited 11 April 2004).
[29] 1267623 Ontario Inc. v. Nexx Online Inc., [1999] O.J. No. 2246 (Sup. Ct).
[30] Id.

who maintained the lists citing unfair business practices and defamation as the grounds for the actions. The suits met with mixed success with some organizations, including YesMail and Harris Interactive,[31] obtaining court orders requiring MAPS to remove them from the RBL, while others failed to convince the courts that such an order was warranted.[32]

Phase Two – The Three Anti-Spam Pillars

Notwithstanding the efforts of ISPs, the FTC, and some U.S. state governments, the spam problem continued to mushroom as the individual actions did little to deter the largest spamming organizations from plying their trade. As both the volume of spam and its associated costs increased, a global consensus gradually emerged on the need to address the spam issue through three mechanisms – technology, consumer education, and legal solutions.

i. Technological Solutions

Technological solutions initially focused chiefly on developing improved tools for filtering out spam messages. Spam filtering systems, which are commonly used today, seek to identify spam messages at one of three levels. First, some ISPs install filtering systems that block purported spam messages at the mail server level, thereby stopping the spam from leaving their systems. This approach is particularly popular with web-based email systems such as Hotmail.[33] Second, many ISPs install filtering systems designed to block messages at the time of receipt, thereby stopping the message from entering the user's email inbox.[34] Third, ISPs often encourage users to install spam filtering systems

[31] G. Mariano, Anti-spam Group Makes Up With Pollster, CNET (22 August 2001), online at <http://news.com.com/2100-1023-943349.html> , (last visited: 11 April 2004).
[32] Media3 Technologies, LLC v. Mail Abuse Prevention System, LLC, 2001 WL 92389 (D. Mass. 2001).
[33] L. Bowman, Hotmail Spam Filters Block Outgoing E-mail, CNET (18 January 2001), online at <http://news.com.com/2009-1023-251171.html>, (last visited: 11 April 2004).
[34] J. Evers, Gates Attacks Spam in E-Mail Message, Infoworld (24 June 2003), online at http://www.infoworld.com/article/03/06/24/HNgatesspam_1.html, (last visited: 12 December 2003).

on their personal computers and to use the filters to sort through email already in found in their inbox.

Spam filtering systems adopt a wide range of approaches to identify spam messages. Some search for commonly found spam markers such as common spam subjects or phrases, known spammer addresses, or frequently used spammer email servers. More sophisticated anti-spam tools use machine learning techniques, particularly bayesian filtering which seeks to calculate the probability of a message being spam, to identify spam messages.[35]

Although spam filters unquestionably have the potential to reduce the amount of spam that enters into users' in-boxes, they at best represent only a partial solution. Spam filtering techniques, no matter how sophisticated, are unable to block all spam. In fact, initial version of spam filters found that some caught less than half of all spam messages examined.[36] While the technology has improved in recent years, spamming organizations have also become increasingly sophisticated in their attempts to evade spam filtering technology.

The serious deficiency of spam filtering technology is even more pronounced when spam filters block non-spam messages, creating what is known as a false positive problem. When filters block non-spam messages, confidence in electronic communications diminishes since users can no longer rely with any degree of certainty that their email communication will reach the intended recipient.[37] Furthermore, spam filtering technology, with all its imperfections, still requires significant capital investments from ISPs, businesses, and occasionally from users.

---

[35] S. Holden, Spam Filters, Online at http://freshmeat.net/articles/view/964/, (last visited: 17 April 2004).
[36] G. Mariano, Study Finds Filters Catch Only Fraction of Spam, CNET (15 June 2000), online at http://news.com.com/2100-1023-241997.html, (last visited: 12 December 2003).
[37] M. Delio, Spam Filters Grab Good With The Bad, Wired News (19 January 2004), online at < http://www.wired.com/news/infostructure/0,1377,61945-2,00.html>, (last visited: 12 April 2004).

In light of the deficiencies, alternative technological solutions have started to emerge. The most popular proposed solution is the development of sender authentication systems. Such systems provide a method of authenticating an e-mail sender's IP address and block all e-mails that are not successfully authenticated. While authentication has generated considerable interest from the technical and ISP communities, the leading technology providers have thus far been unable to reach agreement on a common standard for authenticating email. While each provider has expressed support for authenticated email, all proposed solutions, whether Yahoo!'s Domain Keys, AOL's Sender Policy Framework (SPF), or Microsoft's Caller ID for E-mail, embrace slightly different technological approaches to the degree that the authenticated email initiative has been unable to coalesce around a single standard.[38] Moreover, work toward a single standard has been beset by concerns over proprietary intellectual property, with the International Engineering Internet Task Force Working Group focused on email authentication collapsing in September 2004 under the weight of fears of overlap with Microsoft patents applicable to an emerging standard.[39]

While technology does hold some promise in battling spam, it is apparent that technology alone cannot solve the problem. First, spamming organizations have proven adept at overcoming new technological solutions, creating a spam filtering cat-and-mouse game in which spam filtering providers devise new methods to block spam only to find that spamming organizations quickly respond by identifying new methods to deliver their mail. Second, costs are significant both with respect to the diversion of funds needed to purchase, implement, and maintain technological solutions (costs that are ultimately borne by the consumer) as well as with regard to the false positive problem which decreases the reliability of email as a critical communication system. Third, technological standardization has proved elusive, thereby further increasing costs and delaying the implementation of a widely supported solution.

---

[38] S. Olsen, Technology Solution to Slicing Spam Lags, CNET (22 March 2004), online at < http://news.com.com/2100-7349-5176415.html> (last visited: 18 April 2004).

[39] S. Olsen, Microsoft-Backed Antispam Spec Filtered out, CNET (23 September 2004), online at < http://news.com.com /2100-1032_3-5380029.html>, (last visited: 5 October 2004).

ii. Education

Educating both businesses and consumers was (and remains) widely regarded as a second essential element in the battle against spam. Although most businesses and consumers need only look at their email in-boxes to realize that there is a spam problem, the evidence suggests that many people are still unfamiliar with anti-spam practices.

On the business front, education has come largely in the form of advocating industry best practices or codes of conduct. For example, the Canadian Marketing Association has emerged as an aggressive advocate against spam, noting that the diminishing confidence in both e-mail and e-commerce adversely affects its members who wish to engage in legitimate email marketing.[40] The CMA has supported an opt-in approach to anti-spam legislation and has developed tough email marketing codes of conduct for its members. Interestingly, the CMA position can be contrasted with the U.S. Direct Marketing Association, which, after long opposing anti-spam legislation, recently switched its position to support the enactment of an opt-out system.[41]

In some countries, most notably Australia, anti-spam business codes of conduct have risen above private sector voluntary codes to the level of legal obligations. Australia established an enforceable code of conduct governing spam delivered to mobile phones, known as wireless spam.[42] This anti-spam code, written by the Australian Communications Industry Forum, is legally enforced by the Australian Communications

[40] CMA Responds to Industry Canada Discussion Paper on Spam E-mail, (27 March 2003), online at < http://www.the-cma.org/media/downloads/March%2027%20submission.pdf>, (last visited: 12 April 2004).
[41] D. McCullagh, Spammers Slam Anti-Spam Proposals, Wired News (28 March 2002), online at < http://www.wired.com/news/politics/0,1283,51370,00.html>, (last visited: 12 April 2004); The DMA Announces Support For Spam Legislation, (20 October 2002), online at < http://www.the-dma.org/cgi/disppressrelease?article=354>, (last visited: 12 April 2004).
[42] M. Hollands, Strict Conduct Code Curbs SMS Spam, Australian IT (17 February 2004), online at < http://australianit.news.com.au/articles/0,7204,8679027%5e16681%5e%5enbv%5e,00.html>, (last visited: 12 April 2004).

Authority, which has the power to impose fines of up to $10 million on companies that run afoul of the code.[43]

Consumer education, a critical part of most anti-spam strategies,[44] typically involves educating the public on the desirability of installing anti-spam filtering technology and raising awareness of fraudulent spam, such as the "Nigerian bank scam", an offline scam that has gravitated online and has victimized thousands of people,[45] as well as the recent proliferation of phishing scams which combine email and World Wide Web fraud to obtain personal financial information that can be used to support identity theft crimes.[46]

Consumer education has also focused on how best to respond to spam messages. The FTC created a "spam refrigerator" in 1998, encouraging consumers to send their spam messages to the enforcement agency for future data mining and analysis. Years later, the FTC has received millions of spam messages which can be used to assist in enforcement actions.[47] Canadian enforcement agencies, however, have yet to introduce a similar service, though a Canadian equivalent has been discussed as part of a national anti-spam strategy.

Anti-spam advocates have long cautioned consumers against responding directly to spamming organizations, even if only to "opt-out" of future spam messages. Advocates believe that spamming organizations use the opt-out message to verify the particular email address, thereby leading to even more spam. Interestingly, today there is some disagreement over whether opting-out of spam messages is likely to have any effect on future spam volume, as more sophisticated spamming organizations have developed alternative means to verify recipient addresses. The advice over opt-out has become

---

[43] Id.
[44] See, e.g., Federal Trade Commission, You've Got Spam: How To "Can" Unwanted Email, online at < http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm>, (last visited: 12 April 2004).
[45] See, Nigeria – The 419 Coalition Website, online at < http://home.rica.net/alphae/419coal/>, (last visited: 19 April 2004).
[46] See, Anti-Phishing Working Group, online at http://www.anti-phishing.org, (last visited: 19 April 2004).
[47] M. Delilo, FTC: Where Spam Goes To Die, Wired News (5 November 2002), online at < http://www.wired.com/news/politics/0,1283,55972,00.html>, (last visited: 12 April 2004).

increasingly controversial with the enactment of the U.S. CAN-Spam Act, the United States federal anti-spam law discussed below, which depends upon the opt-out approach as an essential aspect of its enforcement framework.

More fundamentally, anti-spam advocates have struggled to convince consumers to simply delete or ignore spam. Evidence suggests that a sizable percentage still respond on occasion to the commercial message found in the email. At an FTC workshop on spam held in April 2003, it was reported that eight percent Internet users have purchased goods or services as a result of reading a spam message, providing ample evidence that spam can be an effective marketing tool.[48]

Much like technology, business and consumer education may assist in the anti-spam battle, though it also does not provide a complete solution. In fact, the experience to date suggests that education has done little to alter consumer and business anti-spam practices due to inconsistent messages to consumers and an unwillingness for businesses to abide by industry codes of conduct that do not feature enforcement mechanisms.

iii. Legal Solutions

While the desire for anti-spam legislation began to surface in the late 1990s, the tactic has taken centre stage in the anti-spam battle for the past four years. Anti-spam legislation is now an accepted part of the legal landscape in most developed countries including the United States, the European Union, Australia, Japan, and South Korea.

Although Canada has proceeded cautiously, Industry Canada did follow through on its pledge to consider changes to its spam policy position by releasing a discussion paper on the subject in January 2003.[49] That paper raised, for the first time, the prospect of Canadian anti-spam legislation. In the face of mounting criticism over its hands-off spam

[48] Official Transcript Proceeding, Day Two, FTC Spam Project, p. 7, 1 May 2003, online at < http:// www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf>, (last visited 12 April 2004).
[49] E-mail marketing: Consumer choices and business opportunities, Industry Canada, online at < http://e-com.ic.gc.ca/english/strat/email_marketing.html>, (last visited 9 August 2003).

policy, along with questions about the efficacy of existing Canadian laws to combat spam, the government asked Canadians whether new laws dealing with spam should be enacted. In May 2004, the Canadian government unveiled a new anti-spam action plan.[50] The action plan featured the establishment of a national anti-spam task force that is scheduled to release its recommendations in the spring 2005.[51]

While the Canadian process continues to unfold (and is discussed in further detail below), Canada is largely playing catch-up with many jurisdictions worldwide. The United States, the European Union, South Korea, Australia, and Japan have all taken various legislative steps to combat spam. As fears grew that Canada might find itself identified as a spam haven, there was little alternative but to re-open the discussion and consider Canadian anti-spam legislation.

While a comprehensive analysis of all global anti-spam legislation is beyond the scope of this paper, a brief review of the primary anti-spam legislative techniques is discussed below. The breadth of anti-spam legislation varies, as some statutes focus exclusively on email messaging, while others cover SMS spam, mobile spam, and other forms of electronic messaging.

Virtually all anti-spam legislation features significant civil and criminal sanctions including sizable fines and possible imprisonment for repeat offenders. The civil penalties found in anti-spam legislation are particularly noteworthy since they frequently provide parties such as ISPs the right to bring private actions to obtain statutory damages. For example, the State of Washington's anti-spam law provides that recipients of e-mails that violate the law are entitled to the greater of $500 or actual damages,[52] while

---

[50] An Anti-spam Action Plan For Canada, Industry Canada, May 2004, online at < http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html>, (last visited: 5 October 2004).
[51] The author is a member of the task force. See, T. Hamilton, Ministry Appoints Anti-spam Task Force, Toronto Star, 12 May 2004 (online at: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1084313410608&call_pageid=968350072197&col=969048863851>, last visited: 5 October 2004).
[52] Revised Code of Washington s. 19.190.040(1).

interactive computer services such ISPs that suffer damages due to violations of this law are entitled to the greater of $1000 or actual damages.[53]

Some statutes also contain increased damages for aggravated violations. The U.S. CAN-Spam Act provides for trebled damages for the violation of any of its anti-spam prohibitions where the violation was (i) done knowingly and willfully, (ii) used email addresses obtained through harvesting, (iii) engaged in a dictionary attack, (iv) used automated services to register for multiple email addresses, or (v) accessed a computer or computer network without authorization and knowingly relayed or retransmitted commercial e-mail messages from that computer without authorization.[54]

Although anti-spam legislation varies as between jurisdiction, a core group of provisions have emerged in many statutes. These include:

a. Labeling Requirements

Labeling requirements, which obligate email senders to accurately label their email messages within the headers of their email is a common legislative tool since accurate header information is viewed as one method to both simplify and increase the accuracy of spam filtering. For example, the State of Arizona's anti-spam law, which, like most U.S. state anti-spam statutes has been pre-empted by the CAN-Spam Act, required that "ADV", short for advertisement, be the first three characters in the subject line of any unsolicited commercial e-mail.[55]

Many countries and states have also moved to require that the content of particular commercial email contain accurate labeling. South Korea, which has introduced several anti-spam statutes, required in 2001 that all commercial email be marked appropriately on the subject line such that where the message is a commercial advertisement, the word

[53] Revised Code of Washington s. 19.190.040(2).
[54] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, § 5(b) [hereinafter CAN-Spam].
[55] Arizona Revised Statutes, s. 44-1372.01(B)(1).

"Advertisement" must be placed in the subject line, if the email includes non-profit information the word "Information" must be included, and if the email contains adult content the word "Adult" must be included.[56]

The U.S. CAN-Spam Act contains specific labeling requirements for adult content.[57] The law requires initiators of commercial e-mail that features sexually oriented material to either include in the subject heading specific marks or notices to be created by the FTC, or to ensure that the material in the message that is initially viewable to the recipient when the message is opened include only the mark or notice indicating that the message is a sexually oriented one.

b. Prohibition on False Header Information

Spamming organizations seeking to gain access to open mail servers or to evade spam filtering technologies often resort to the use of false header information. This often includes the falsification of information in respect to the sender of the email, its originating server, or the subject of the email itself. Legislation prohibiting this deceptive practice has been widely introduced, though such measures are likely caught by most existing anti-deceptive practice legislation.

For example, the U.S. CAN-Spam Act contains civil prohibitions against the use of false or misleading header or transmission information in a commercial e-mail message, the use of another computer to relay or retransmit commercial e-mail for the purpose of disguising its origin, and the sending of commercial e-mail that includes an originating e-mail address, domain name, or Internet protocol address that was obtained by means of false pretenses or representations.

c. Prohibition on Email "Dictionary Attacks"

[56] DC Kang, "Anti-spam regulations in Korea" Korea Information Security Agency (February 2003).
[57] CAN-Spam, supra, § 5(d).

An email "dictionary attack" occurs when spamming organizations use machine generated email addresses at popular email providers to query the validity of those addresses. The information is then used to either send spam messages or can be sold to other spamming organizations. For example, a common dictionary attack involves the sending of millions of machine generated email addresses to users at hotmail.com or aol.com. Japan's Law on the Regulation of Transmission of Specified Electronic Mail prohibits the use of email dictionary attacks by banning the transmission of emails to randomly generated email addresses.[58]

d. Prohibition on Email Address Harvesting

Spamming organizations may also obtain email addresses by harvesting email addresses from websites, listserves, newsgroups, and any other source known to feature live email addresses. South Korea is one of several jurisdictions that has banned the practice of harvesting email addresses from online sources.[59] Its legislation provides that the use of a program for the collection of email addresses through technical means is prohibited. Moreover, the legislation seeks to stop the sale of email addresses between spamming organizations, by prohibiting the act of sharing, selling, exchanging or providing others with a list of email addresses harvested from Internet bulletin boards.

e. Prohibition on Email Harvesting Software

In addition to a prohibition on email harvesting, Australia's Spam Act 2003 features a ban on software tools that can be used to harvest email addresses. The provision stipulates that a person in Australia may not acquire nor use address harvesting software,[60] defined to include software that is specifically designed or marketed for use for (a) searching the Internet for electronic addresses and (b) collecting, compiling, capturing or otherwise harvesting those electronic addresses.[61]

---

[58] Law No. 26 of 2002.
[59] Act on Information Network and Protection, July 2001.
[60] Spam Act 2003, S. 20 and 21.
[61] Spam Act 2003, S. 4.

f. ISP Immunity for Good Faith Actions

Given the important role ISPs have played in combating spam, many states and countries have granted them statutory immunity for the actions they take against spamming organizations. For example, the State of Indiana's anti-spam law grants an ISP the right to block the receipt or transmission of messages it reasonably believes to be in violation of the state anti-spam statute[62] and provides that the ISP not be held liable for such action if it is taken in good faith.[63] Similarly, South Korea's anti-spam legislation specifies that ISPs can deny services for transmitting information on the condition that there is concern about potential obstruction due to large influxes of spam.[64]

g. Do Not Spam Lists

In light of the popularity of the U.S. do-not-call list, which has registered more than 85 million numbers in less than two years,[65] there is some support for the establishment of a similar do-not-email list. Under the U.S. CAN-Spam Act, the FTC was required to establish a plan and timetable for establishing a do-not-email list. The plan was required to include any practical, technical, security, privacy, enforceability, or other concerns that the FTC has regarding such a registry.[66] In June 2004, the FTC released its report, concluding that such a list would be ineffective and burdensome to consumers.[67]

Even if Congress decides to ignore the FTC recommendation, a U.S. do-not-spam list would not be the first such list instituted by a national authority. In August 2002, South Korea launched "NoSpam", a spam blocking website. The site allowed users to register

[62] Indiana code, s. IC 24-5-22-9(a).
[63] Indiana code, s. IC 24-5-22-9(b).
[64] OECD, Background Paper for the OECD Workshop on Spam, at p. 37-8. 22 January 2004.
[65] P. Davidson, Time-Share Marketers To Pay $500,000 in Do-Not-Call Case, USA Today (16 February 2005), online at < http://www.usatoday.com/money/companies/regulation/2005-02-16-do-not-call-usat_x.htm>, last visited: 18 February 2005.
[66] CAN-Spam, supra, § 9(a).
[67] D. McCullagh, FTC: Thumbs-Down on Do-Not-Email List, CNET (15 June 2004), online at < http://news.com.com /2100-1024_3-5234480.html>, last visited: 5 October 2004.

their telephone numbers and/or e-mail addresses, and by doing so, all spam messages were to be blocked from reaching those numbers or addresses. Registering on the site was, according to government regulators, an expression by the individual of his or her desire not to receive any spam. Once enrolled, it was hoped that the users would be safe from all spam for six months, after which they would be prompted to renew.[68]

h. Commissioning Spam

Recent anti-spam legislation recognizes that many spamming organizations send spam messages on behalf of others, rather than actually selling the goods or services themselves. Australia's Spam Act 2003 broadened the scope of its coverage to include not only spamming organizations who engage in the deceptive practices discussed above, but also those parties that commission spam to be sent on their behalf.[69]

i. Opt-in vs. Opt-out

The most contentious anti-spam provisions have inevitably revolved around whether to force consumers to ask to be removed from receiving commercial marketing (an "opt-out" approach) or to force businesses to obtain consumers' positive consent before sending commercial marketing (an "opt-in" approach). The opt-out approach occurs when a person is added to a list without her permission or knowledge, and it is the recipient's responsibility to indicate that she no longer wishes to be on the list, should she want to stop receiving the messages. At the other end of the spectrum is a confirmed opt-in approach. Under this process, when a person opts-in to a list, he is sent an e-mail automatically, providing notification that the person will not be added to the list until the e-mail is confirmed that he does indeed wish to be on the list.

[68] Y. Sung-jin "Powerful Web site blocking spam" The Korea Herald (22 August 2002), online: Korea Information Security Agency < http://powerfulwebsite.notlong.com/> (last visited: 16 February 2005).
[69] Spam Act 2003, S. 8.

Several variations of both opt-out and opt-in also exist. A confirmed opt-out occurs when a person's e-mail address is added to the list and the recipient is sent an e-mail stating that she was added to the list and given instructions on how she can opt-out if desired. A non-confirmed opt-in approach only adds a person to the list when they have so requested, but no confirming email is sent to ensure that it is a legitimate opt-in.

U.S. legislation, at both the federal and state levels, have adopted, with near uniformity, an opt-out approach supplemented by penalties for failing to abide by opt-requests.[70] Although there are various forms of opt-out legislation, most provide that all unsolicited commercial email must include explicit opt-out language. Moreover, statutes often require senders to provide clear and genuine identification, including name, telephone number, valid opt-out email address, postal address, and an easy mechanism for opting out of a list. Senders are typically required to implement opt-out requests within a short time frame (for example, the CAN-Spam Act establishes a ten business day requirement).[71] Failure to abide by any of the opt-out legislative provisions may result in significant fines or other penalties.

By contrast, the European Union Directive on Privacy and Electronic Communications, which forms the basis for most European anti-spam legislation, adopts an opt-in approach with a limited pre-existing business relationship exception (typically referred to as a "soft opt-in approach").[72] The Directive requires member states to prohibit the sending of unsolicited commercial email unless the prior consent of the person has been obtained.[73] The limited exception allows for the use of personal information obtained from customers in the context of a sale, but that information may only be used by the same legal person that originally collected the data. Moreover, the personal information may only be used to market similar products and services and an explicit opt-out option must be offered at

[70] The single, noteworthy exception was a State of California opt-in bill that was pre-empted by the federal CAN-Spam Act.
[71] CAN-Spam, supra, § 5(a)(4)(A).
[72] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[73] Id. Article 13(1).

the time of collection and with each subsequent message.[74] The E.U. is not alone in adopting an opt-in approach as other countries, including Australia, have implemented legislation featuring opt-in approaches. As of January 2005, however, several European Union member states had yet to implement the anti-spam directive.[75]

j. Canada

While Canada has yet to enact anti-spam legislation,[76] anti-spam advocates and enforcement agencies do have several legal tools at their disposal that provide similar powers. These include the use of private sector privacy legislation, deceptive practices legislation administered by the Competition Bureau's Fair Business Practices Branch, the application of the Criminal Code, and enforcement of section 41 of the Telecommunications Act. Viewed in combination, the Canadian legal options would allow for enforcement actions against many of the kinds of conduct identified by current global anti-spam legislation including the use of deceptive headers, failure to honour opt-out requests, limitations on email address harvesting and sales, and the unauthorized use of computing equipment to send spam.

1. PIPEDA

[74] Id. Article 13(2).
[75] P. Meller, EU Pressures Member States to Implement Spam Law, IDG News Service (1 April 2004), online at < http://www.infoworld.com/article/04/04/01/HNeuspamlaw_1.html> , (last visited 19 April 2004).
[76] Note that two private member's bills were introduced in 2003 at the federal level that would have created Canadian anti-spam legislation. Senator Don Oliver introduced a bill that called for the creation of a do-not-spam registry, required ISPs to block spam and join a self-governing council, and included a private right of action. MP Dan McTeague introduced a bill that would have established Criminal Code provisions for sending spam punishable with jail terms and substantial financial penalties. Neither bill became law, though Senator Oliver reintroduced his bill both in the 2004 Parliamentary session that concluded with the June 2004 federal election and the in the subsequent parliamentary session. The bill was at first reading as of January 2005. Further, Ontario MPP Judy Marsales introduced a private members bill in the Ontario legislature in May 2004 also designed to target spam. As of October 2004, Ontario Bill 69 remained at first reading.

The Personal Information Protection and Electronic Documents Act (PIPEDA),[77] Canada's private sector privacy legislation, could potentially be one of Canada's most powerful legal tools to challenge a Canadian spammer on privacy grounds.

PIPEDA covers personally identifiable information, which could include email addresses, where such an address can be identified to a specific individual.[78] Although some email addresses may not disclose sufficient information to be traced to an identifiable individual, many will be caught within the scope of the Act. Moreover, the statute would clearly apply where an individual identifies themselves and opts-out of further correspondence.

According to a December 2004 finding involving the author, the Privacy commissioner has also determined that business email address qualify as personal information and can be the subject of a PIPEDA complaint.[79] The case, which was not reported on the Privacy Commissioner's site as of February 2005, involved the collection of the author's email address from the University of Ottawa's website directory. The Ottawa Renegades, a team in the Canadian Football League, collected the email address and proceeded to send an unsolicited commercial email inviting the author to purchase season tickets to the team's games. The author declined and asked the organization to cease sending further commercial messages. When the team ignored the request and sent a second unsolicited commercial email, the author filed a complaint with the Privacy Commissioner.

The Assistant Privacy Commissioner issued a decision on the complaint in a letter dated December 1, 2004. The decision addressed three key issues. First, the Assistant Commissioner determined that the author's email address was a business email address and was not covered by Section 2 of the Act, which exempts name, title, business address or telephone number of an employee of an organization.[80] The Assistant Commissioner reasoned that the exclusion of an email address from the list of exempted information was

[77] S.C. 2000, c. 5
[78] PIPEDA, S.C. 2000, c. 5, s. 2(1).
[79] http://www.mgblog.com/resc/GeistPCCSpamdecision.pdf
[80] PIPEDA, S.C. 2000, c. 5, s. 2(1).

intentional. Second, the Assistant Commissioner ruled that the public directory exception was similarly inapplicable since the use of the public directory to market sports tickets was a secondary purpose (the primary purpose being communications related to the author's employment) that required proper consent.[81] Third, the Assistant Commissioner confirmed that failure to respect the opt-out request was a violation of PIPEDA.[82]

Given this recent ruling, it is clear that PIPEDA can be applied to several spam-related activities.[83] First, application of the Act would prohibit the collection of personally identifiable email addresses through harvesting techniques since the Act requires individual consent prior to the collection, use, and disclosure of personal information.[84]

Second, the Act may require an opt-in approach in certain circumstances. The Office of the Privacy Commissioner of Canada recently outlined its perspective on the limited circumstances when an opt-out approach will be appropriate.[85] It found that opt-out consent should only be used for the collection and use of non-sensitive information, when the information sharing is limited and well-defined, when the purpose is limited, well-defined, clear, and brought to the attention of the individual at the time of collection, and when there is a convenient, easy, and inexpensive system for opting-out.[86] In the spam context, this suggests that organizations using email addresses that have been harvested from Internet sources such as websites or listserves would likely run afoul of the law since it is unlikely that the purpose of the collection would have been made clear and brought to the attention of the individual at the time of collection. Moreover, spam that contains sensitive information, for example personal health information, would require an opt-in approach.

---

[81] PIPEDA, S.C. 2000, c. 5, s. 7(1)(d).
[82] PIPEDA, S.C. 2000, c. 5, Principle 4.3.
[83] *See*, S. Morin, Spam in Canada: How PIPEDA Can Do Its Part, 1 Canadian Privacy Law Review 85 (May 2004).
[84] PIPEDA, S.C. 2000, c. 5, Schedule One, 4.3.
[85] Case Summary 207, Cell Phone Company Meets Conditions for "Opt-Out" Consent, 6 August 2003, online at < http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_02_e.asp>, (last visited: 18 April 2004).
[86] Id.

Third, as illustrated in the Renegades decision, organizations that do not honour opt-out requests would clearly run afoul of the law, while organizations that adopt an opt-out approach must ensure that they feature a convenient and easy method for a future opt-out.

Several other PIPEDA provisions could also factor into an anti-spam analysis. The accountability principle, which requires the data collector to remain accountable for the protection of the personal information for which they are responsible,[87] could conceivably be used against organizations that permit personally identifiable email addresses to be sold or otherwise accessed without individuals' consent. The security principle might also be applied in a spam context, requiring data collectors to employ adequate security safeguards to ensure that personally identifiable email addresses are not disclosed without appropriate consents.[88]

In addition to its application to spamming activity, PIPEDA could also be applied to email list brokers, who actively sell millions of email addresses, where the transactions cross provincial or national borders.

Enforcement of PIPEDA rests with the Office of the Privacy Commissioner of Canada, who could become involved in anti-spam initiatives in two ways. First, an individual could launch a PIPEDA complaint. The Office would be required to investigate and issue a finding within one year.[89] Second, the Office could use its audit and investigatory powers to initiate a PIPEDA action against a known spamming organization based in Canada.[90]

Undercutting the effectiveness of PIPEDA, however, is the fact that the Office does not have order making powers. A Federal Court of Canada enforcement action would therefore be needed to obtain an actual damages award. For example, in the Renegades decision, the Assistant Commissioner advised the author that I was entitled to take the

[87] PIPEDA, S.C. 2000, c. 5, Schedule One, 4.1.
[88] PIPEDA, S.C. 2000, c. 5, Schedule One, 4.7.
[89] PIPEDA, S.C. 2000, c. 5, s. 13(1).
[90] PIPEDA, S.C. 2000, c. 5, s. 18(1).

matter to federal court. Without order making power, the Privacy Commissioner is unable to establish an effective deterrent against larger spamming organizations, many of whom will likely disregard a decision without concern for their (already tarnished) reputations.

2. Deceptive Business Practice Legislation

The Competition Bureau's Fair Business Practices Branch administers the deceptive practice provisions found in Canada's Competition Act. The Act includes both civil and criminal provisions addressing deceptive practices. On the civil side, the Act provides that "a person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever makes a representation to the public that is false or misleading in a material respect."[91] On the criminal side, the Act adds a knowledge standard by providing that "No person shall, for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever, knowingly or recklessly make a representation to the public that is false or misleading in a material respect."[92]

The potential punishment for engaging in reviewable conduct can be severe. The Act provides that a court may issue an injunction prohibiting further reviewable conduct as well as levy financial penalties of $50,000 for individual first time offenders and $100,000 for corporate first time offenders (the penalties are doubled for subsequent offences).[93]

[91] Competition Act, R.S. 1985, c. C-34, s. 74.01(1).
[92] Competition Act, R.S. 1985, c. C-34, s. 52(1).
[93] Competition Act, R.S. 1985, c. C-34. s. 74.1(1).

The Bureau successfully completed its first spam case in December 2004.[94] Part of its FairWeb initiative, the Bureau reached a settlement whereby a diet patch marketer agreed to cease using spam as a method for marketing its products and promised to provide a refund to anyone who had purchased a diet patch.

Although that case resulted in a consent agreement settlement, the legislation clearly empowers the Bureau to seek orders against Canadian-based spamming organizations on at least two grounds provided the materiality standard (as well as the knowledge or reckless standard if criminal sanction is pursued) is met. First, spamming organizations that use deceptive or false headers, a practice specifically targeted by many anti-spam statutes, could be targeted for a reviewable conduct order. Second, the Bureau could also consider the content of some spam such as the Nigerian net scam, phishing, and offers to sell suspect health products, many of which might meet the deceptive or materially false claim standard established by the Act.

In addition to the December 2004 case, the Bureau has demonstrated a willingness to target fraudulent Internet conduct. For example, in 2002, it obtained a consent agreement from Thane Direct Canada over misleading representations made on a website regarding two electronic muscle stimulation devices contrary to Section 74.01 of the Act. The agreement included an immediate cessation of online promotion and a $75,000 administrative penalty.[95]

Interestingly, the U.S. Federal Trade Commission, which is generally regarded as the world's most aggressive anti-spam enforcement agency, has relied almost exclusively on deceptive practice legislation similar to that found in Canada to bring actions against more than 55 spamming organizations.[96]

---

[94] Consumers Receive Full Refund for Bogus Diet Patches, Competition Bureau Release, 13 December 2004, online at < http://cb-bc.gc.ca/epic/internet/incb-bc.nsf/en/ct03018e.html>, (last visited: 14 February 2005).

[95] The Commissioner of Competition v. Thane Direct Canada, CT-2002/007.

[96] Hugh Stevenson, Federal Trade Commission, Case Studies on Cross-Border Enforcement Cooperation Against Spam, OECD Workshop on Spam, 3 February 2004, online at < http://www.oecd.org/dataoecd/3/31/26991168.pdf>, (last visited 19 April 2004).

3. Criminal Code

Canada's Criminal Code could also be used to commence actions against certain spamming activity with at least four relevant sections. First, s. 380 of the Code, which covers fraudulent conduct, could be interpreted to cover spam that contains fraudulent or false content. The section applies to "Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service".[97] The Act proscribes punishments of up to ten years in jail for frauds of over $5000 and up to two years in jail for frauds under that amount.[98] The Supreme Court of Canada has adopted a broad interpretation of the provision, concluding in *R. v. Olan* that fraudulent means includes "not only means which are in the nature of falsehood or deceit but also all other means which can properly be stigmatized as dishonest."[99]

Second, s. 372(1) of the Code, which covers false messages, could be used to bring actions against whoever sends false emails with the intent to injure. The section provides that "Every one who, with intent to injure or alarm any person, conveys or causes or procures to be conveyed by letter, telegram, telephone, cable, radio or otherwise information that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years."[100] Canadian courts have granted their approval to aggressive enforcement techniques in targeting violators of this provision. For example, in *R. v. Skrepetz*, a 1990 B.C. case, the court accepted the use of an "annoyance call originator program" to monitor calls made from the accused's telephone. The court dismissed objections pertaining to the interception of private communications, concluding that the records did not interfere with the privacy of the communications.[101]

---

[97] Criminal Code, R.S. 1985, c. C-46 s. 380 (1).
[98] Criminal Code, R.S. 1985, c. C-46 s. 380 (2).
[99] R. v. Olan, [1978] 2 S.C.R. 1175.
[100] Criminal Code, R.S. 1985, c. C-46 s. 372(1).
[101] R. v. Skrepetz, [1990] B.C.J. No. 1457 (B.C. P.C.).

Third, the Criminal Code could also be applied to spamming organizations who access computer servers without permission, as is typically the case when spamming organizations make unauthorized use of email servers to send spam. Section 342.1, which typically has been used to target unauthorized hacking, might also be applied to unauthorized spam usage since it provides that "Every one who, fraudulently and without colour of right, obtains, directly or indirectly, any computer service is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years."[102] Computer service is broadly defined to include "data processing and the storage or retrieval of data."[103] Within the spam context, this could include not only the unauthorized use of email servers, but potentially email harvesting as well since the latter activity might be considered the fraudulent retrieval of data from a website. In fact, if email harvesting was covered by s. 342.1, then s. 342.2, which covers the possession, sale, offer for sale, or distribution of any device the design of which renders it primarily useful for committing a section 342.1 offence, might criminalize the sale and distribution of email harvesting software.[104]

Fourth, Section 430(1.1) creates a penalty for mischief to data. This provision provides that "every one commits mischief who willfully (*a*) destroys or alters data; (*b*) renders data meaningless, useless or ineffective; (*c*) obstructs, interrupts or interferes with the lawful use of data; or (*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."[105] While the mischief to data is best known for its applicability to denial of service attacks, the provisions could also be used in a spam context. In particular, the use of zombie computer networks to send spam and the harm incurred by ISP networks could fall within the ambit of the provisions.

4. Telecommunications Act

[102] Criminal Code, R.S. 1985, c. C-46 s. 342.1(1).
[103] Criminal Code, R.S. 1985, c. C-46 s. 342.1(2).
[104] Criminal Code, R.S. 1985, c. C-46 s. 342.2(1).
[105] Criminal Code, R.S. 1985, c. C-46 s. 430(1.1).

Canada's Telecommunications Act, which is administered by the Canadian Radio-television and Telecommunications Commissioner, features a single, as yet-untested provision that might also be used in the battle against spam. Section 41 of the Act provides that "The Commission may, by order, prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression."[106]

Although the provision was initially intended to cover junk fax transmissions, since the Act broadly defines telecommunications to include "emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system",[107] there does not appear to be any limitation in the Act that would prevent the CRTC from applying the provision to email based unsolicited telecommunications. Moreover, the Act grants the CRTC powers that are equivalent to a superior court,[108] which would enable the Commission to issue binding orders prohibiting spamming organizations from using Canadian telecommunications facilities to send spam.

As the chart below illustrates, the collective powers found under Canadian law come close to approximating the provisions employed in targeted anti-spam legislation in other jurisdictions. Moreover, the Canadian provisions feature significant penal provisions including the potential for substantial fines, cease and desist orders, and imprisonment.

Anti-Spam Legislative Provision	**Canadian Statutory Equivalent**
General anti-spam provision	Telecommunications Act, s. 41
General anti-fraud provision to cover spam containing fraudulent content	• Criminal Code, s. 380 • Criminal Code, s. 372(1)

[106] Telecommunications Act, 1993, c. 38, s. 41.
[107] Telecommunications Act, 1993, c. 38, s.2(1).
[108] Telecommunications Act, 1993, c. 38, s.55 (c).

	• Competition Act, ss.52(1) and 74.01(1)
Labeling requirements	None
Prohibition on false header information	• Competition Act, ss.52(1) and 74.01(1) • Criminal Code, s. 380
Prohibition on email dictionary attacks	Criminal Code, s. 342.1
Prohibition on email address harvesting	• Criminal Code, s. 342.1 • PIPEDA, Schedule One, 4.3
Prohibition on email address harvesting software	Criminal Code, s. 342.2
ISP immunity for good faith activities	None. Canadian caselaw has supported ISPs that have terminated service contracts on spamming grounds.
Do Not Spam List	None
Commissioning spam offence	For spam containing fraudulent content: • Criminal Code, s. 380 • Criminal Code, s. 372(1) • Competition Act, ss.52(1) and 74.01(1) For spam featuring false header information: • Competition Act, ss.52(1) and 74.01(1))
Opt-in requirement	PIPEDA, Schedule One, 4.3
Opt-out requirement	PIPEDA, Schedule One, 4.3
Unauthorized use of email server	Criminal Code, s. 342.1, 430(1.1)
Spam reporting mechanism	None
Private right of action	None. Private lawsuits have been commenced in Canada against spamming

	organizations on trademark and contract grounds.

Notwithstanding the global anti-spam legislative efforts, in which it may now be reasonably said that virtually every developed country has implemented legal measures that can be used to combat spam, the amount of spam has continued to increase.

Much like the technological and education pillars, the legal pillar suffers from several limitations. As discussed in greater detail under Phase Three below, the existence of an arsenal of anti-spam legislative tools without a corresponding, aggressive enforcement policy is destined to fail. While laws are necessary, they are not sufficient. Enforcement agencies and the private sector must challenge the largest spamming organizations in the courts.

While the largest spamming organizations may be identifiable, cobbling together the necessary evidence to obtain a conviction under any anti-spam statute requires perseverance, significant resource allocations, and co-operation between enforcement agencies. For example, in December 2003, New York state attorney general Eliot Spitzer filed suit against Scott Richter, who is regularly cited in the Spamhaus Register of Known Spam Organizations[109] as the leader of one of the world's leading spamming organizations. The charges were the result of months of investigative work leading to a nearly 700-page indictment against the New York-based spammer.[110] The case settled in July 2004.[111]

Although anti-spam legislation (or its equivalent) is now commonplace, inconsistencies, particularly with respect to opt-in vs. opt-out, remain. These differences may create

[109] http://www.spamhaus.org/rokso/index.lasso [hereinafter ROKSO List]
[110] M. Reardon, Microsoft, New York Launch Spam Suits, CNET (18 December 2003), online at < http://news.com.com/2100-1028-5128806.html>, (last visited: 19 April 2004).
[111] Z. Rodgers, Spitzer Settles With Alleged Spammer Richter, ClickZ News (20 July 2004), online at http://www.clickz.com/news/article.php/3383431 (last visited: 4 October 2004).

uncertainty for both Internet users and businesses, both of whom now face potentially conflicting data collection regulations while operating in a global e-commerce environment.

Some anti-spam legislation may also simply be ineffective. For example, do-not-spam lists, currently under consideration in the United States and in effect in South Korea, have attracted considerable skepticism as even the Federal Trade Commission has expressed doubts about its viability.[112] Similarly, many anti-spam advocates have criticized opt-out approaches, arguing that its legal codification results in the legalization of non-fraudulent spam.[113]

After four years of developing new anti-spam legislative tools, accompanied by technological developments and greater consumer awareness, the spam problem continues unabated, leaving some to believe that even if you build it (the legal frameworks), the spam will still come. The answer may lie not in yet more laws, however, but rather in better enforcement of what we already have.

Phase Three - Getting Serious About Spam

Over the past ten years, spam has grown from a minor annoyance to a major, global concern, threatening the reliability of electronic communication and the adoption of electronic commerce. While all stakeholders – government, the private sector, and Internet users – have expressed their commitment to addressing the problem, the volume of spam continues to escalate.

As discussed in Phase Two, technology, education, and legal solutions have formed the pillars of most anti-spam strategies for the past four years. Notwithstanding these efforts,

---

[112] FTC Chair Says Do-Not-Spam List Would Be 'Ineffective', DMA, 20 August 2003, online at < http://www.the-dma.org/cgi/dispnewsstand?article=1413>, (last visited: 19 April 2004).
[113] D. McCullagh, Bush Oks Spam Bill – But Critics Not Convinced, CNET, 16 December 2003, online at < http://news.com.com/2100-1028-5124724.html>, (last visited: 19 April 2004) [hereinafter Bush Oks Spam Bill].

spam now constitutes well over half of all email communications. Moreover, there is every indication that the situation is likely to worsen in the coming months.

Phishing, which combines email and Web fraud, has its roots in identity theft and brings with it a new criminal dimension to spam. Furthermore, it is growing at alarming pace, with one recent study reporting that the number of phishing emails circulating the Internet mushroomed from 279 in September 2003 to 215,643 in March 2004.[114] Spamming organizations are also likely to identify new delivery channels for their messages. Instant messaging spam, dubbed spim, is growing faster than traditional email spam. Four hundred thousand spim messages were sent in 2003, while 1.5 billion were expected in 2004.[115]

Given the growing spam threat, the global community must get serious about dealing with the spam problem by recognizing that what we are facing is primarily an enforcement problem. While technological solutions as well as education and awareness campaigns have important roles to play, the primary energies should be devoted to using the legal tools established in recent years to wage a meaningful enforcement campaign.

Contrary to popular belief, however, the enforcement problem is not derived from an inability to identify or track down spamming organizations. Although spamming organizations are frequently characterized as elusive networks situated offshore beyond the reach of traditional law enforcement,[116] evidence suggests that the leading spamming organizations are not untouchable. In fact, the Spamhaus Register of Known Spam Organizations (ROKSO) lists the 200 leading spam organizations, who it says account for 90 percent of all spam worldwide.[117]

---

[114] M. Kotadia, Phishing Scams Luring More Users, CNET, 19 April 2004, online at < http://news.com.com/2100-7355_3-5194807.html>, (last visited: 20 April 2004).
[115] M. Reardon, Experts Downplay 'Spim' Threat, CNET, 1 April 2004, online at < http://news.com.com/2100-7343-5183549.html>, (last visited: 19 April 2004).
[116] J. Bick, An Overview of the CAN-SPAM Act, Gigalaw, online at < http://www.gigalaw.com/articles/2004-all/bick-2004-03-all.html>, (last visited: 19 April 2004).
[117] ROKSO List, supra.

The ROKSO list suggests that the majority of the leading spamming organizations are based in the United States, though all sophisticated spamming organizations make use of offshore servers to disguise their tracks. Canada has featured ten or more organizations on the ROKSO list, a number consistent with studies by Sophos, an anti-virus company, which has reported that Canada trails only the U.S. as the world's second largest source of spam, accounting for 6.8 percent of global spam.[118]

Private sector spam suits provide further evidence that spamming organizations can certainly be found. Notwithstanding the lack of anti-spam enforcement initiatives by Canadian authorities, several leading U.S. ISPs and Internet companies have commenced lawsuits against Canadian-based spamming organizations using both U.S. and Canadian law. In a highly publicized action in March 2004, Yahoo! launched a suit under the CAN-Spam Act in U.S. courts against a Kitchener-based spamming organization.[119] That case settled in June 2004 with agreement to pay at least $100,000 and to cease sending spam to Yahoo! customers.[120] Several months later, Amazon.com and Microsoft joined forces to again sue the Kitchener organization under the CAN-Spam Act in the U.S. courts.[121] Meanwhile, both Amazon.com[122] and Earthlink,[123] a leading U.S. ISP, have brought suits against Canadian spamming organizations in Canadian courts on trademark grounds.

The true challenge of anti-spam enforcement is not, therefore, finding the spamming organizations. Rather, it is bringing sufficient resources to bear such that enforcement actions generate genuine deterrence to stop the spamming activities perpetrated by the

---

[118] Sophos Outs 'Dirty Dozen' Spam Producing Countries, 27 February 2004, online at < http://www.linuxworld.com.au/index.php/id;832527808>, (last visited: 19 April 2004).
[119] Ontario Trio Among Those Sued in U.S. Over Spam, 11 March 2004, online at < http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1078940487005_64/%3Fhub=Canada>, (last visited: 19 April 2004).
[120] Canadian Spam King Agrees to Stop Sending Junk E-mail, USA Today, 16 June 2004, online at < http://www.usatoday.com/tech/news/2004-06-16-spam-king-abdicates_x.htm>, last visited: 4 October 2004).
[121] Microsoft and Amazon Take Spam Suits to "Head Operation", Computer Wire, 29 September 2004, online at < http://uk.news.yahoo.com/040929/221/f3iyo.html>, last visited 5 October 2004.
[122] R. Weisman, Amazon Sues Spam Spoofers, E-commerce Times, 26 August 2003, online at < http://www.ecommercetimes.com/perl/story/31433.html>, (last visited: 19 April 2004).
[123] P. Roberts, Earthlink Sues Spammers, IDG News Service, 27 August 2003, online at < http://www.pcworld.com/news/article/0,aid,112212,00.asp> , (last visited: 19 April 2004).

worst offenders. To achieve that level of enforcement, several steps are needed.

First, the Internet community must reconcile itself with the reality that private sector leadership has failed to stem the spam tide. Serious spam enforcement requires law enforcement to assume the lead role. While the private sector remains an essential part of any anti-spam initiative through private sector suits, investigative assistance, implementation of technological innovations, as well as business and consumer education, it must be government that leads on the enforcement of the current anti-spam legal frameworks.

Second, on a national level, a Canadian spam strategy must look to the Office of the Privacy Commissioner of Canada, the Competition Bureau's Fair Business Practices Branch, the Ministry of Justice, and the CRTC, the four government departments responsible for administering the Canadian laws that could be applied to spam, to proactively enforce those laws consistent with their statutory mandates. If those organizations prove unable to meet the enforcement challenge either due to insufficient resources or a lack of clarity within the law, legislative provisions may be needed to increase spam penalties, to remove any loopholes in the current framework, to establish a private right of action, and to send an unequivocal signal that anti-spam enforcement is a government priority.

Third, on an international level, Canada should actively support the emerging trend toward bi-lateral and international anti-spam enforcement co-operation. Australia and South Korea provide an excellent example of bi-lateral anti-spam enforcement co-operation. In October 2003, the two countries signed a memorandum of understanding designed to promote the regulation of spam. Although currently limited to information sharing, the two countries are working to expand their understanding to include enforcement actions.[124] The U.S. and United Kingdom have also taken steps to forge closer co-operation on anti-spam initiatives, with two U.S. senators and three U.K.

[124] Australia, South Korea Sign Agreement on Spam Regulation, The Age, 20 October 2003, online at < http://www.theage.com.au/articles/2003/10/20/1066502122751.html>, (last visited: 19 April 2004).

members of Parliament endorsing close "cross-border" cooperation between the two countries in a joint letter signed in December 2003.[125]

On the multinational front, several international organizations have started to provide anti-spam policy leadership by facilitating dialogue and raising the prospect for further international co-operation. For example, the Organization for Economic Cooperation and Development hosted a global spam summit in February 2004,[126] and established a global anti-spam task force in August 2004.[127] Meanwhile, the International Telecommunications Union hosted an anti-spam event in July 2004[128] and the World Summit on the Information Society, which held the first of two global meetings in Geneva in December 2003, has also begun to consider the potential for an anti-spam initiative as part of its mandate to address Internet governance issues by October 2005.[129] Although an international agreement or spam code of conduct seems unlikely, these initiatives may help facilitate more effective enforcement through greater international investigative cooperation.

More than two-dozen countries recently joined forces on another anti-spam initiative targeting open relay servers. Spamming organizations use open relays to send at least 40 percent of the world's spam. In January 2004, 36 agencies in 26 countries launched "Operation Secure Your Server", an international effort to reduce spam by urging the Internet community to close open relays.[130]

Fourth, effective enforcement will increasingly depend upon focusing on what is occurring offline, rather than online. While spamming organizations employ

---

[125] Bush OK's Spam Bill, supra.
[126] Id.
[127] T. Richardson, OECD Unveils Spam Task Force, The Register, 12 August 2004, online at < http://www.theregister.co.uk/2004/08/12/oecd_spam/>, last visited: 4 October 2004.
[128] First Can Spam Suit Filed, ITU Weblog, 9 March 2004, online at http://www.itu.int/osg/spu/newslog/categories/spam/2004/03/09.html#a509>, (last visited: 19 April 2004).
[129] D. McCullagh, United Nations Ponders Net's Future, CNET, 26 March 2004, online at http://news.com.com/2100-1028-5179694.html>, (last visited: 19 April 2004).
[130] FTC and International Agencies Announce "Operation Secure Your Server", FTC, 29 January 2004, online at http://www.ftc.gov/opa/2004/01/opsecure.htm>, (last visited: 19 April 2004).

sophisticated technical methods to cover their tracks online, many experts agree that the offline money flows may prove far easier to identify.[131] Such a strategy would be consistent with evidence that the majority of spamming organizations are based in North America, even if they frequently use offshore mail servers.

Conclusion

In the 1987 hit film The Untouchables, federal agent Eliot Ness' did battle with the seemingly untouchable Al Capone during the Prohibition.[132] The movie features a memorable scene in which Jim Malone, a veteran police officer played by Sean Connery, confronts Ness over whether he is serious about taking on the Chicago mobster. Malone challenges Ness by asking "What are you prepared to do?". When Ness affirms that he is committed to bringing down Capone, Malone literally leads Ness across the street, where the presence of alcohol is apparently an open secret. As they prepare to enter the building, Malone notes that everyone knows where the booze is located, the question is whether they are prepared to do something about it.

Although the battle against spam is not quite as simplistic as Hollywood's portrayal of the battle against Al Capone, the challenge similarly rests not with finding the spamming organizations nor does it rest with instituting fundamental legal reforms. We know the location of many of the leading Canadian-based spamming organizations. The Canadian legal framework features many of the tools needed to launch anti-spam legal actions, despite the absence of specific anti-spam legislation. Rather, the challenge rests with our willingness to enforce the existing laws by engaging in aggressive anti-spam national enforcement as well as cooperating with global anti-spam enforcement initiatives. It is time for Canada to get serious about spam. With either stronger enforcement or the establishment of additional legislative provisions, we must answer the question: what are we prepared to do?

---

[131] K. Dean, Stop The Cash Flow, Kill The Spam, Wired News, 6 February 2004, online at http://www.wired.com/news/infostructure/0,1377,62177,00.html>, (last visited: 19 April 2004).
[132] <http://www.imdb.com/title/tt0094226/maindetails>