CONTROLLING SPAM: THE PROSPECT OF LEGISLATIVE SUCCESS

Karla Dane*

INTRODUCTION

THE PREVALANCE OF UNSOLICITED COMMERCIAL EMAIL or spam has become a growing issue in the world of e-commerce. Since the first spam message was sent in 1994, email advertising has gained widespread recognition, becoming a popular tool used by businesses and other Internet users to relay messages.[1] This new technique, however, has not come without costs; in fact, the problems associated with spam have well surpassed any benefits that it may have created for Internet users. Spam has proven to be more than simply an annoyance to Internet users, as it is one of the largest barriers to legitimate e-commerce. The problems created by spam go beyond any existing technological solutions and require legislative measures.

In an attempt to combat growing concerns about spam, the United States government enacted the *CAN-SPAM Act*,[2] and although the Canadian government has yet to implement similar legislation, the need for it has been recognized. In addition, both governments have acknowledged the need to develop an international solution to battle spam on a global level. This paper will examine the U.S. legislation, identify possible areas for improvement, and then compare and contrast it with the approach taken by the Canadian government. The paper will conclude with a look at the international problems associated with spam, steps that have been taken at the international level and possible solutions to global spam problems.

WHAT IS SPAM?

SPAM IS GENERALLY REFERRED TO AS UNSOLICITED commercial or bulk email that is sent without the express consent of the recipients.[3] Generally, but not always, these emails have a commercial purpose, either the promotion or sale of products or services. There is no one fixed definition of spam; however, it has one universally

---

* B.A. (Brandon), LL.B. (UM).

1 E.A. Alongi, "Has the U.S. Canned Spam?" (2004) 46 Ariz. L. Rev. 263.

2 15 U.S.C. §§ 7701-7713 (2004).

3 Industry Canada, "What is Spam?" online: Industry Canada <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00170e.html#spam>.

accepted characteristic — it is unsolicited.[4] All of the unwanted and unrequested emails that end up in inboxes can be classified as spam.

WHY IS SPAM A PROBLEM?

THE DRASTIC ESCALATION IN SPAM HAS NOT ONLY proven to be an annoyance for email users, but has also created numerous problems for businesses and Internet Service Providers (ISPs). The sheer volume of spam causes serious problems for ISPs as the increase in spam occupies more space on Internet server bandwidths, resulting in slower Internet service. The results are more severe for smaller ISPs whose servers may be completely overwhelmed by the volume of spam. When the first spam message was sent in 1994 by two Arizona lawyers, the advertisement reached approximately 20 million people, and the resulting response crashed their ISPs' computer.[5]

In addition to Internet infrastructure problems, spam has created numerous financial problems for ISPs, businesses and recipients. Perhaps one of the biggest problems with spam is its unique cost-shifting structure. The bulk of fees resulting from spam and its advertising are incurred by the recipients of the mail rather than the spammers (senders).[6] If recipients pay for their Internet connection by the amount of time they are connected (such as dial-up), they will pay for the time it takes to download each email from the ISP. Therefore, the more spam received by the recipient will result in increased financial costs, as the time required to download the email will be greater. If recipients pay flat rates for their Internet connection, the price will increase in correlation with the costs incurred by the ISP due to the growing volume of spam. Several ISPs have had to expand their networks to accommodate the increase in spam, and many have implemented filtering systems to block spam in order to maintain customer satisfaction.

Many businesses are also feeling the financial effects that spam has created. For example, it has been estimated by the Radicati Group that in 2003, spam cost businesses worldwide US$20.5 billion.[7] Recent studies suggest that spam costs U.S. companies alone approximately US$9 billion annually.[8] These costs are the result of productivity decreases; for example, employees spend more time deleting spam

---

[4] Simon Kellett, "Legislative Definition of Spam for New Zealand" (2005) 36 V.U.W.L.R. 607.
[5] *Supra* note 1 at 263.
[6] Lily Zhang, "The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem" (2005) 20 Berkeley Tech. L.J. 301.
[7] Industry Canada, "The Cost of Spam," online: Industry Canada <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00170e.html#cost>.
[8] *Supra* note 6.

messages from their inboxes, and companies purchase filter systems in an attempt to decrease spam. In addition, some companies (and other spam recipients) have had to increase their disc space in order to accommodate the volumes of incoming spam messages.

A growing problem with spam is that as technological methods such as filtering and blocking have developed, spammers are finding new ways to ensure their messages are delivered to the recipients. For example, spammers have responded by increasing the number of emails sent in order to guarantee that at least one reaches the intended destination.[9] Spammers are also finding new ways to change the email header, which contains the recipient address, the sender address, and the routing information (the path the email takes), so that the spam goes undetected. Spammers use various methods to conceal the originating addresses of these emails. Some of the most commonly used techniques include open relays, zombie drones, open proxies, and spoofing. It is evident that technology plays a predominant role in eliminating spam, but it is not enough to combat the numerous complexities of spam. Any legislation implemented to address the spam problem must fill the gaps left by technological solutions.

THE U.S. APPROACH: THE *CAN-SPAM ACT*

IN RESPONSE TO THE GROWING SPAM EPIDEMIC, the U.S. has implemented both federal and state legislation. Thirty-eight U.S. states have passed their own anti-spam laws,[10] and on 16 December 2003, President Bush signed Senate Bill 877, the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)*, into law.[11] The Act establishes national standards defining and regulating spam and includes appropriate sanctions for violations. It only applies to commercial email, where the primary purpose is advertising or promoting a commercial product or service.

Many of the provisions in the Act parallel those found in the state statutes, which are aimed at reducing spam. The Act does not make email advertising illegal; its goal is simply to stop (or at least reduce the amount of) unsolicited commercial email. The Federal Trade Commission (FTC) is given numerous powers to enforce the Act's provisions, and the Department of Justice (DOJ) is given authority to enforce its criminal

---

[9] Anita Ramasastry, "Why the new federal 'CAN Spam' law probably won't work" *CNN.Com* (5 December 2003), online: CNN.com <www.cnn.com/2003/LAW/12/05/findlaw.analysis.ramasastry.spam/index.html>.

[10] "Spam Laws: United States: State Laws," online: Spam Laws <http://www.spamlaws.com/state/index.shtml>.

[11] *Supra* note 2.

sanctions.[12] ISPs are still entitled to bring actions against violators, but the Act eliminates the ability of individual spam recipients to bring civil actions, overriding some of the state laws. Since 1 January 2004, when the Act came into effect, to date the FTC has brought 20 cases alleging violations.[13] The DOJ, state Attorney Generals, and ISPs have together brought more than 50 actions.[14] However, the ramifications and future prospects of the Act remain to be determined.

The Act establishes certain requirements in order for spam to be sent legally. As long as an email follows these guidelines, there will be no violation and the message will be legal. First, the Act bans false or misleading header information,[15] the header must be accurate, and the person sending the email must be identifiable.[16] Spoofing and zombie drones, methods that spammers use to avoid detection, would therefore, be actionable under the Act.

Moreover, the Act prohibits the use of deceptive subject lines.[17] An email will be in violation of this provision if the recipient is misled as to the contents or subject matter of the message. The Act establishes an objective threshold for this provision: "[I]f such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient."[18] This is becoming increasingly important as a growing number of spam messages contain malicious or inappropriate (such as pornographic or sexually directed) contents. The Act specifically requires that warning labels be placed on spam messages containing sexually-oriented materials; a person in violation of this requirement may be subject to a fine and/or imprisonment of up to five years.[19]

Another requirement established by the Act is the inclusion of an opt-out method for the email recipient. Each email must contain a functioning return email address or other Internet-based response mechanism that a recipient could use to request that future emails not be sent to that address.[20] The sending email address must be able to

---

[12] "The CAN-SPAM Act: Requirements for Commercial Emailers," online: Federal Trade Commission <http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm>.

[13] Federal Trade Commission, *Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress* (Federal Trade Commission, December 2005) at ii, online: Federal Trade Commission <www.ftc.gov/reports/canspam05/051220canspamrpt.pdf>.

[14] *Ibid.*

[15] *Supra* note 2, § 7704(a)(1).

[16] *Ibid.*, § 7704(a)(1)(A).

[17] *Ibid.*, § 7704(a)(2).

[18] *Ibid.*

[19] *Ibid.*, § 7704(d).

[20] *Supra* note 12.

process opt-out requests for at least 30 days after the originating message has been sent, and the law gives 10 days for the originating sender to stop sending email to that address.[21] However, the Act specifically recognizes that if a recipient gives consent to receive email from the sender subsequent to the opt-out request, no violation will be found.[22]

This section of the Act also acknowledges the possibility that email addresses obtained from opt-out requests may be used on later occasions. As a result, the Act prohibits the sale, transfer, or release of email addresses obtained from opt-out requests. Such an action will only be legal if it is done to enable another entity to comply with the law.[23] Finally, the Act requires that commercial email be identified as an advertisement or solicitation and must include a valid physical postal address of the sender.[24]

In addition to establishing criteria for sending valid spam messages, the Act criminalizes some actions taken by spammers and creates a new section in the *Criminal Code.* The Act created criminal sanctions for spammers who use or conspire to use a computer other than their own, without authorization, to send multiple commercial emails either from or through that computer.[25] Further to this provision, the Act criminalizes the use of a computer to relay or transmit multiple commercial emails in order to alter the header information and deceive or mislead recipients about the origin of the message.[26] Often referred to as zombie droning, this has become an increasing method of choice for spammers, as it enables large volumes of emails to be sent while protecting the originating address from detection.

It is also criminally punishable to use materially misleading information to register multiple email accounts or domain names and initiate the transmission of multiple commercial emails from the accounts or domains.[27] The final two criminal activities provided for in the Act include falsely representing oneself as an owner of multiple IP addresses that are used to send commercial email messages and falsification of the header information on multiple email addresses.[28] Spam messages with false header information, a method commonly used by spammers, have created difficulties for the application and enforcement of the Act. These difficulties arise from the fact that false

---

[21] *Ibid.*
[22] *Supra* note 2, § 7704(a)(5)(B).
[23] *Supra* note 12.
[24] *Ibid.*
[25] 18 U.S.C. § 1037(a)(1) (2003), amended by 15 U.S.C. §§ 7701-7713 (2004).
[26] *Supra* note 12.
[27] *Supra* note 2, § 7703(1)(a)(4).
[28] *Supra* note 12.

header information makes it virtually impossible to determine where the message originated from. Much of the criticisms surrounding the Act arise from the problems associated with actually locating the spammers in order to penalize them.

The Act sets penalties for criminal violations, including fines, imprisonment or both. A violator may be imprisoned for up to five years if the offence is committed in furtherance of any federal or state felony, or if the defendant has been previously convicted of an offense under the Act. It allows the court to order forfeiture of any property traceable to the proceeds obtained from such an offence, or forfeiture of the equipment or software used or intended to be used for the facilitation of the offence.[29] Furthermore, the Act specifically recognizes enhanced sentences for spammers convicted of fraud, obscenity, identify theft, child pornography, or the sexual exploitation of children through the use of mass commercial email.[30] A provisional violation of the Act is subject to fines of up to US$11,000, and additional fines are provided for aggravated violations,[31] which include obtaining email addresses through email harvesting and dictionary attacks.[32] The Act also sets penalties for businesses that advertise in contravention of the established provisions.

Section 6 of the Act specifically provides for businesses that knowingly promote their business by email containing false or misleading information.[33] It is an offence for a business to promote or be promoted by commercial email containing false or misleading information. The section establishes that a person or business will be in violation of the Act if they knew or ought to have known that their business was being promoted through such commercial messages, or if they received or expected to receive a profit from such promotion.[34] Similar to the other sections, the problems that arise from this section pertain to the proper identification of the actual sender of the spam message and the application of the section by the FTC in proving that a business knew or ought to have known about the email.

It is clear that the creators of the Act have identified major concerns and problems arising from spam and have attempted to eliminate them or at the very minimum, decrease their prevalence. The Act targets spammers' most commonly used techniques and provides sanctions for violators. Its effectiveness, however, has been heavily criticized and debated since coming into effect. Like any such legislation, the ability of

---

[29] 18 U.S.C. § 1037.
[30] *Supra* note 2, § 7703(b)(2)(B).
[31] *Supra* note 13.
[32] *Supra* note 2, § 7704(b)(1).
[33] *Ibid.*, § 7705(a).
[34] *Ibid.*, § 7705(a)(1).

the *CAN-SPAM Act* to eliminate unsolicited commercial email has attracted both support and criticism.

A) Criticisms of the CAN-SPAM Act

The Act's most commonly identified problem is that it does not make spamming illegal and, therefore, will not be able to eliminate spam altogether. It merely establishes a set of guidelines to be followed by businesses or individuals sending spam, thereby legalizing the sending of spam mail. This could potentially result in the volume of spam increasing, if the guidelines are followed.[35]

A further criticism of the federal Act is that it preempts the stronger state anti-spam laws. Many of the U.S. states have stricter anti-spam laws that provide greater protection for consumers. It has been suggested that the "problem is not that the state laws are preempted because often preemptions work to create uniformity, but rather that uniform federal law being imposed is much too weak to have any substantial effects."[36] An example of a more restrictive state law that is negatively affected by the federal Act is the California legislation. The California anti-spam law requires an opt-in system whereby a recipient must give preliminary consent to receiving spam.[37] This is contrary to the Act's opt-out system that allows the email to be sent, but requires that the message include a mechanism enabling the recipient to request that no future emails be sent to that address.

The express preemption provision of the Act was evaluated by the Fifth Circuit Court in *White Buffalo Ventures, LLC v. University of Texas*.[38] The court was to determine whether the federal legislation preempted the anti-spam legislation of the University of Texas. White Buffalo Ventures (WBV), an online dating service operator, brought an action to prohibit the University of Texas from blocking its mass commercial emails. WBV argued that the university's anti-spam law was preempted by the *CAN-SPAM Act*, essentially using the federal legislation as a defence.[39] The spam that had been sent by WBV was in compliance with the federal legislation and it was argued, therefore, that it could not be blocked. The court found that the university's anti-spam legislation

---

[35] S*upra* note 6.

[36] Erika Hallace Kikuchi, "Spam in a Box: Amending CAN-SPAM & Aiming Toward a Global Solution" (2004) 10 B.U. J. Sci. & Tech. L. 263 at 284.

[37] S*upra* note 6.

[38] *White Buffalo Ventures, LLC v. University of Texas at Austin*, 420 F.3d 366 (5th Cir. 2005).

[39] Jameel Harb, "White Buffalo Ventures, LLC v. University of Texas at Austin: The CAN-SPAM Act & the Limitations of Legislative Spam Controls" (2006) 21 Berkeley Tech L.J. 531.

was not preempted by the federal legislation, which recognizes certain entities that are exempt from the possible preemptive effect. Included in this list of entities are ISPs, most of whom have their own policies enabling them to decline to transmit certain emails. In reaching its decision, the court stated, "Supremacy Clause analysis is classic 'tie goes to the state' jurisprudence, and the existence of an express preemption provision does not always plainly demarcate what the federal law expressly preempts."[40] The University of Texas was found to be a provider of Internet services thereby falling within the express exemption in the legislation.

It has been argued by some that the court erred in its findings in the *White Buffalo Ventures* decision.[41] The conflicts arise in the express preemption provision within the Act. The provision itself establishes which state rules are preempted by the federal legislation, while at the same time indicating parties exempt from the preemption. The court is required to determine whether a party falls within the criteria of an ISP in order to be exempt. The University of Texas was functioning as an ISP for students, staff, and faculty and, therefore, fell clearly within the exemption as prescribed in the Act.[42] The decision by the court does, however, leave substantial room for future interpretation, which may only fuel further criticisms by opponents of the Act.

Although the Act specifically prohibits the use of addresses obtained from opt-out requests, some critics are wary that email addresses validated by opt-out requests will be reused, a technique that may actually result in more emails being sent to those addresses.[43] The justification for an opt-out provision appears to be that it facilitates e-commerce by allowing email marketing, while at the same time weeding unwanted messages. However, in order for any weeding out to occur, the recipient is required to request that no further messages be sent; this only furthers the cost-shifting problems associated with spam. Essentially, the recipients are required to take affirmative action to reduce the volume of these emails.[44] Many recipients are reluctant to even reply to these kinds of messages. Unless spammers actually fear being caught and punished, these messages might not actually include proper opt-out mechanisms.[45] Furthermore, The Spamhaus Project, an

---

[40] *Supra* note 38 at 2.
[41] Dan Hopper, "Do You Want Spam With that? The CAN-SPAM Act, Preemption, and First Amendment Commercial Speech Jurisprudence Concerning State University Anti-Solicitation E-mail Policy" (2006) 59 SMU L. Rev. 387.
[42] *Supra* note 39.
[43] *Supra* note 6.
[44] Erin E. Marks, "Spammers Clog In-boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion?" (2004) 54 Case W. Res. L. Rev. 943.
[45] *Supra* note 36.

anti-spam organization, strongly discourages individuals from opting-out of lists that they have not opted-into to begin with because "[b]y sending back a 'remove me' opt-out request you are confirming to the spammer that your address is live, you are confirming that your ISP doesn't use spam filters, you are confirming that you actually open and read spams, and that you follow the spammer's instructions such as 'click this to be removed.' You are the perfect candidate for more spam."[46] According to the organization, confirmed live email addresses are valuable amongst spammers and can be sold to others at a premium.[47]

The Internet is a worldwide medium and, therefore, the problem of spam has a global nature. Many of the spam messages received in the U.S. originate overseas, and the Act does not address the difficulty in identifying and prosecuting international spammers. Furthermore, to avoid sanctions, U.S. spammers can simply move their operations offshore, or they can re-route their messages to appear that they originate offshore. In order to truly eradicate the spam problem, international measures are required.

Some opponents of the Act argue that its harsh penalties are disproportionate to the violations.[48] The counter argument is that harsher punishments will have greater deterrent effects and, therefore, reduce the amount of spam. Perhaps the effectiveness of the Act is dependent on the fear that spammers will be caught and criminally prosecuted; the harsh penalties, such as extensive fines or possible jail time, may contribute to the prevention of inappropriate or multiple spam messages. However, opponents of the Act argue that despite the penalties, many spammers are not convinced that they will be caught or charged; many continue to include non-existent physical addresses or faulty opt-out mechanisms so as to appear to comply with the Act while avoiding prosecution.[49]

In order to ascertain how effective the Act is and identify possible changes that would enhance its efficiency, the FTC compiled a Report to Congress in December 2005.[50] It addresses areas of success and areas which require further development.

B) The Success and Future of the CAN-SPAM Act

Since the Act came into effect in 2004, more than 50 actions have been brought in the U.S. Although spam is still a prevalent problem, the

---

[46] "Should You Send 'Removes' back to Spammers?" online: The Spamhaus Project <http://www.spamhaus.org/removeisformugs.html>.
[47] *Ibid.*
[48] S*upra* note 6.
[49] *Supra* note 36.
[50] *Supra* note 13.

FTC reports that the volume of spam has started to level off and the amount reaching consumer inboxes has decreased, largely due to new anti-spam technologies.[51] The amount of spam being sent from U.S. sources, the greatest proportion of distributors, appears to have also decreased. Recent statistics reports that in January 2006, "43.18% of global spam [was] sent from U.S.-based sources, (down from approximately 50%)".[52] Other recent spam statistics suggest that spam continued to increase following the enactment of the Act but has been decreasing since mid-2005. Data released by MX Logic Inc. in September 2005, indicated that spam accounted for 67 percent of all email sent in the first eight months of the year, down from 76 percent for the same time period in 2004.[53] In addition, MX Logic Inc. reports that an alarming 97 percent of spam sent in 2004 failed to comply with the new legislation.[54] The statistics appear to indicate that spam is on the decline; however, it is evident that spam is a continuing problem regardless of the Act.

As a result of continuing concerns, in their Report to Congress, the FTC made three recommendations to improve the effectiveness of the *CAN-SPAM Act*. The first recommendation was to pass the *Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005* (*SAFE WEB Act*). The implementation of this Act would improve the FTC's ability to use the *CAN-SPAM Act* to trace spammers whose operations are outside the U.S. borders.[55] Second, the FTC recommends continued education to ensure that consumers are informed of the various ways they can protect themselves from unwanted sexually-explicit spam.[56] Finally, the FTC recommends continued improvement in anti-spam technology. It appears that the best way to combat spam must include both technological and legal solutions. More

---

[51] *Ibid.*

[52] Commtouch, Press Release, "January Virus and Spam Statistics: 2006 Starts with a Bang" (15 February 2006), online: Commtouch <http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=602&cat_id=1>.

[53] MXLogic, Press Release, "MXLogic Reports Spam Accounts for 67 Percent of All Email in 2005" (22 September 2005), online: MXLogic <http://www.mxlogic.com/news_events/press_releases/09_22_05_SpamStats.html>.

[54] MXLogic, Press Release, "On One-Year Anniversary of CAN-SPAM Act, MX Logic Reports 97 Percent of Spam Failed to Comply with the Law: Spam, Other Email Threats Will Continue to Increase in 2005" (3 January 2005), online: MXLogic <http://www.mxlogic.com/news_events/press_releases/01_03_05_CAN_SPAM.html>.

[55] *Supra* note 13.

[56] *Ibid.*

companies are purchasing and using filters and filtering technology is continually progressing; however, in response, spammers are finding new ways to ensure that their emails get to the designated inboxes.

Since the Act came into effect, spammers have changed the contents of their messages and the way they deploy them.[57] As previously mentioned, spammers continue to include false physical addresses and/or faulty opt-out mechanisms in order appear as if in compliance with the Act and avoid detection by filters and authorities. Further to these techniques, spammers are increasing their use of bot networks and affiliate marketing programs. Bot networks are made up of multiple zombie drones that are controlled by the same network and are used to obscure the originating address of a sender of multiple commercial emails.[58] Affiliate market programs involve a contract between the marketer and affiliates who send spam advertising the marketer's products or services. The affiliates are usually paid a commission whenever the spam message results in a sale or benefit to the marketer.[59] Apart from methods of sending spam, spammers are also changing the types of emails sent; commercial emails are being replaced with spam containing pornographic or sexual content. Moreover, spammers have developed 'phishing' spam which requests extremely personal information from the recipient and is most commonly used for "identity theft."[60]

The FTC has recognized that the international nature of spam has not changed substantially since the Act came into effect. Critics have gone so far as to say that it does nothing to solve problems relating to the global nature of spam.[61] The international nature of spam introduces new problems; these include issues of jurisdiction, enforcement of laws against offshore spammers and, most importantly, identification and location of international spammers. Most of these problems result from spammers who use zombie drones or alter the header information to make it appear that the message was sent from another location. The international nature of spam frustrates the FTC efforts because the Commission is not entitled to compel any third parties located abroad to provide information about websites hosted or registered offshore, or information about spam that may have come through their systems.[62] A further problem is that the Commission is unable to keep investigations

---

[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*
[60] Industry Canada, "What is Phishing?" online: Industry Canada <http://ecom.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00170e.html#phishing>.
[61] *Supra* note 36.
[62] *Supra* note 13.

confidential, due to civil investigative demands.[63] The Commission obtains information about suspects from ISPs and domain registrars; this makes maintaining complete confidentiality near impossible. It is not surprising that spammers who become aware of an investigation against them will discontinue their operations or move them offshore. This drastically reduces the effectiveness and successfulness of the FTC investigations.

The Commission, however, has had some success in the enforcement of the Act in international cases. Recently, in *FTC v. Creaghan A. Harry*, a U.S.–based spammer was identified and prosecuted.[64] The spammer used a Swedish address for contact information, a bank account in Latvia for any proceeds, and delivered spam messages to U.S. consumers using computers located around the world. A settlement was reached in June 2005, and the spammer agreed to pay US$485,000 in consumer redress in addition to an injunction.[65]

Although relatively few countries have implemented anti-spam laws, it is very clear that to be successful in combating international problems created by spam, global cooperation and participation are required. As noted in its Report to Congress, the FTC recognized that spam requires a global solution. As mentioned, the FTC suggested that greater results could be achieved if the U.S. were to enact the *SAFE WEB Act*, which would provide the FTC with the means to trace spammers whose operations are beyond the U.S. borders.[66]

It is evident from the report that the FTC recognizes that the Act alone will not solve the existing spam problems, let alone adequately provide for any new problems. Although the Act has purportedly had some success, critics have undoubtedly established its shortcomings. Many of the problems that were in existence prior to its enactment are still prevalent today, and they are not likely to be eliminated in the near future. The long term impact of the Act remains to be seen, but it is clear that a step has been taken in the right direction.

THE CANADIAN RESPONSE TO SPAM

DESPITE THE EXPONENTIAL GROWTH OF SPAM in recent years, the Canadian government has been slow to respond; so far, no anti-spam legislation has been enacted. It was not until January 2003 that Industry Canada released a discussion paper on its spam

---

[63] *Ibid.* at 25.
[64] *FTC v. Harry*, No. 04C 4790, online: FTC <http://www.ftc.gov/os/caselist/0423085/0423085.htm>.
[65] *Supra* note 13, n. 102.
[66] *Ibid.*

policy, raising the first prospect of developing Canadian anti-spam legislation.[67] Following the paper, Industry Canada established an Anti-Spam Task Force to further investigate growing problems and possible solutions to spam, and the Government of Canada announced its Anti-Spam Action Plan (the Plan) on 11 May 2004. The Plan provides for a joint government–private sector task force to help in the fight against spam and applies a "toolkit" approach.[68] The six-point Plan recognizes the importance of involving all parties, including government, businesses and consumers, both locally and internationally.

The first point set out in the Plan is the use of existing Canadian laws and regulations to combat spam. Canada has three existing pieces of federal legislation that can and have been used to control or reduce spam. Firstly, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) establishes that email addresses can only be used for the purpose for which they were collected and treats email addresses as protected personal information.[69] *PIPEDA* also establishes that recipients must give consent to receive commercial email before commercial bulk email senders transmit spam messages.[70] If successful in its application, *PIPEDA* could potentially reduce the volumes of unsolicited commercial email. The Assistant Privacy Commissioner recently dealt with a complaint under *PIPEDA*. The complainant alleged that his ISP "was reading his outgoing email messages" and was, therefore, violating Section 2 of *PIPEDA*.[71] The ISP required its customers' outgoing messages go through an outgoing mail server as part of its anti-spam measures. The Commissioner found the complaints to be unfounded as the process of reading and routing email information does not require the ISP to read the contents of the email.[72]

The second useful existing piece of legislation is the *Canadian Criminal Code*. The Code is applicable to messages that contain fraudulent or false contents and prevents the unauthorized use of computer services for the purposes of relaying spam messages.

---

[67] Michael Geist, "Untouchable?: A Canadian Perspective on the Anti-Spam Battle," Version 1.1 (May 2004), online: Michael Geist <http://www.michaelgeist.ca/geistspam.pdf>.

[68] Industry Canada, *An Anti-Spam Action Plan for Canada*, (May 2004), online: Industry Canada <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e.html>.

[69] Rosemary E. John, "Canada's Anti-Spam Action Plan," online: The Continuing Legal Education Society of British Columbia <www.cle.bc.ca/CLE/Analysis/Collection/04-12345-spam.htm>.

[70] *Supra* note 67.

[71] Office of the Privacy commissioner of Canada, "Commissioner's Findings: ISP's Anti-Spam Measures Quetioned: PIPEDA Case Summary #319" (8 November 2005), online: <http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp >.

[72] *Ibid.*

Violations of the Code may result in extensive fines and/or imprisonment. However, there are some issues that arise with the application of the Code, such as inter-jurisdictional enforcement issues between the provinces and the ability to prove the intention to commit an offence through spam.[73]

Canada's first criminal spam case was brought in 2002.[74] The case involved a spammer who sent emails offering to sell documents with instructions on how to make homemade bombs, how to break into private homes and how to generate credit card numbers.[75] The spammer was charged under section 464 of the *Criminal Code*. Since the Crown had difficulty proving the mental element of the crime, the judge found that the spammer had not intended for anyone to actually use the information. The Crown appealed on the matter of *mens rea*. The Court of Appeal upheld the acquittal, and the Crown appealed to the Supreme Court. The Supreme Court allowed the appeal on the count of counseling fraud and found that the trial judge had confused motive and intent. Justice Fish went on to say that "courts cannot contain the inherent dangers of cyberspace crime by expanding or transforming offences, such as counselling, that were conceived to meet a different and unrelated need."[76]

Finally, the *Competition Act* applies to messages that contain deceptive or misleading representations. It states:

> 74.01 (1) 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,
>
> (*a*) makes a representation to the public that is false or misleading in a material respect;
>
> (*b*) makes a representation to the public in the form of a statement, warranty or guarantee of the performance, efficacy or length of life of a product that is not based on an adequate and proper test thereof, the proof of which lies on the person making the representation; or
>
> (*c*) makes a representation to the public in a form that purports to be
>
> (i) a warranty or guarantee of a product, or

---

[73] *Supra* note 67.
[74] *Ibid.*
[75] *R. v. Hamilton*, [2002] A.J. No. 30.
[76] *R. v. Hamilton*, [2005] S.C.J. No. 48 at para. 31.

> (ii) a promise to replace, maintain or repair an article or any part thereof or to repeat or continue a service until it has achieved a specified result,
>
> if the form of purported warranty or guarantee or promise is materially misleading or if there is no reasonable prospect that it will be carried out.[77]

This Act also provides extensive financial penalties and severe punishment for individuals who engage in reviewable conduct.

The second point in the Plan is a review of current legislative, regulatory, and enforcement measures.[78] The effectiveness of current legislation at reducing or combating spam should be reviewed in order to determine whether the government must take further legislative or enforcement actions in fighting it. A review would also determine the likelihood of new anti-spam legislation reducing the frequency of spam.

The third point in the Plan relates to improving current industry practices, including the development and use of technological resources, such as filtering systems and industry best business practices.[79] Better network management practices could reduce the possibility of email abuse, and agreements on the basic operating practices or codes of conduct for network facilities would decrease the amount of spam received. These codes should include information on acceptable commercial email and policies; in addition, they should be monitored and enforced by everyone involved in the marketing and communications chain.[80]

Similar to the American *CAN-SPAM Act*, the creators of the Canadian Anti-Spam Action Plan recognize the contribution that filtering technologies have made towards the reduction or elimination of spam. More importantly, Industry Canada acknowledges the limitations presented by the extensive use of these kinds of technologies. For example, as these technologies have developed, spammers have found new ways to ensure their messages are delivered to the intended recipients. Problems also arise where filtering programs accidentally block legitimate commercial communications, thereby contributing to the problems associated with spam messages. In an attempt to address these problems, Industry Canada's fourth point in the Plan is the recommended use of technology to validate commercial communications. Similar to some of the provisions in the *CAN-SPAM Act*, the Plan

---

[77] *Competition Act*, R.S.C. 1985, c. C-34
[78] *Supra* note 68.
[79] *Supra* note 68 & 69.
[80] *Supra* note 67.

establishes that these techniques would require the sender's proper identification and the nature of the communication, and include an effective means of refusing further email from the sender.[81] The potential problem with this approach is that it requires stakeholders to reach an agreement on the most effective technology; businesses and ISPs may have common interests, but they also have different concerns about regulating spam. The costs associated with varying technologies may impose different burdens on the many diverse stakeholders.

The fifth point in the Plan is the need for continuing consumer education and awareness. There are many ways that Internet users can protect themselves and limit the amount of spam mail that they receive, but they have not been informed of these techniques. The Plan recommends that the government consider a private-sector plan to develop programs in conjunction with consumer groups, provincial governments, and international partners.[82] To solve the basic problem of getting the information to the consumers, the Plan suggests that it should be relayed through ISPs and legitimate sellers of goods and/or services who advertise via email. It would seem logical for ISPs to educate their customers about ways to reduce spam when they are signed up for Internet access and email accounts.

The global nature of spam has not gone unrecognized by Industry Canada, and the final point in the Plan is the need for governmental support for global anti-spam initiatives. The Plan recognizes that in order to achieve success at the international level, cooperation is needed between governments, businesses, and consumers. Under the Plan, the government supports the development and adoption of an international best practices regime (similar to the local best practices codes) for email marketing and network management, coordinated internationally.[83] This has yet to be accomplished, so the effectiveness of such an approach remains unknown, but it is evident from both the Canadian approach and the *CAN-SPAM Act* that countries must work together to defeat spam at the international level.

In May 2005, the Task Force on Spam issued a report which addressed the effectiveness of the Anti-Spam Action Plan and provided recommendations for further actions to be taken in order for Canada to be successful in combating spam. The report was released a year after the Task Force and Action Plan came into effect, and it is clear that these approaches were not sufficient to achieve the government's goals without the help of legislation directly aimed at regulating spam. Importantly, the Task Force was able to verify the strategies that had been successful

---

[81] *Ibid.*
[82] *Supra* note 69.
[83] *Supra* note 67.

throughout the previous year and used that information to determine best practices for future effectiveness.

The Task Force confirmed that in order to be successful against spam, "clear laws, strong penalties and vigorous enforcement are needed."[84] It is not shocking that simply relying on existing Canadian laws would not be enough to achieve these goals. Although the applications of those laws have had some success, there are too many uncertainties and weaknesses in the application and enforcement of the laws to achieve long term effectiveness. Clearly, it is time for the Canadian government to enact legislation aimed towards reducing and eliminating spam in conjunction with already existing laws and technological methods being used.

Atop the list of recommendations from the Task Force is the need for the government to "establish in law a clear set of rules to prohibit spam and other emerging threats to the safety and security of the Internet . . . by enacting new legislation and amending existing legislation as required."[85] The Task Force recognizes the need to protect consumers against the various forms of spam, including current and future forms of spam. Implementing these recommendations would take the legislation a step farther than implementing the provisions found in the *CAN-SPAM Act*, as the U.S. legislation is only applicable to unsolicited commercial email. It is extremely important to recognize that spammers are determined to continue using this forum as a means for delivery of their messages and will find new and exciting ways to accomplish this.

The report establishes a list of email activities and practices that should be offences under the new anti-spam legislation. Some of these offences reflect the provisions found in the *CAN-SPAM Act* and others take a stricter approach. First, it would be an offence to fail "to abide by an opt-in regime for sending unsolicited commercial email."[86] Therefore, in order to send a commercial email, the sender must have permission from the recipient. This is a more stringent approach than the U.S. has taken; the *CAN-SPAM Act* has been heavily criticized for requiring merely an opt-out provision. It appears that the opt-in technique could have a significant impact on the amount of spam ending up in inboxes. Second, it would be an offence to use "false or misleading headers or subject lines . . . designed to disguise the origins, purpose or contents of an email."[87] This is identical to the provisions provided in the *CAN-SPAM Act* and

---

[84] Industry Canada, *Stopping Spam: Creating a Stronger, Safer Internet: Report of the Task Force on Spam*, (Ottawa: Information Distribution Centre, May 2005) at 2, online: Industry Canada <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00317e.html>.

[85] *Ibid.* at 3.

[86] *Ibid.*

[87] *Ibid.*

would likely receive the same criticisms. The purpose of having such an offence is to enable the originating address to be obtained and the recipient to recognize that the email is commercial or sexually explicit in nature. Again, the problem with such an offence is that spammers can and will alter the headers, making enforcement very difficult.

Further to these offences, the Task Force recommends that dictionary attacks and email harvesting without consent, as well as the supply, use, or acquisition of these lists be deemed offences. Finally, the construction of "false or misleading URLs and websites for the purpose of collecting personal information under false pretences or engaging in criminal conduct" should be recognized as an offence and punishable under the Act.[88] The Task Force recommends that these offences should be civil or strict liability offences with proportionate penalties for violations. Similar to the *CAN-SPAM Act*, the Task Force acknowledges that harsher penalties with criminal liability should be given for more serious offences or repeat offenders. The Task Force, however, strays from the U.S. approach as it proposes that an appropriate right of action should be available to individuals and corporations. Enabling private parties to bring actions could further the deterrent effect of government enforcement and fill gaps created by resource limitations on government enforcement agencies.[89] It would also enable individual parties to receive compensation and/or damages for harm inflicted directly upon them. The *CAN-SPAM Act* specifically eliminates the right to bring civil actions against spammers.

Similar to the *CAN-SPAM Act*, the Task Force acknowledges the need to hold "the businesses whose products or services are being promoted by way of spam . . . responsible for the spamming."[90] It seems unreasonable to prosecute the sender of spam messages and not the party that actually stands to benefit from the messages. The degree of awareness that businesses would be required to have of spam messages promoting their goods/services in order to be held accountable is problematic. Clearly, this is something that any legislation would need to adequately address.

The above recommendations pertain to the implementation of new Canadian anti-spam legislation. The report also addresses the continuing need for businesses and other stakeholders to implement industry best business practices and consumer awareness programs. Since the 2004 Action Plan came into effect, the government has developed a Stop Spam

---

[88] *Ibid.* at 14.

[89] *Debates of the Senate (Hansard)*, Volume 142, Issue 31, (3 February 2005) (Hon. Daniel Hays), online: Parliament of Canada <www.parl.gc.ca/38/1/parlbus/chambus/senate/DEB-E/031db_2005-02-03-e.htm>.

[90] *Supra*, note 84 at 4.

Here campaign that establishes three key tips for consumers to reduce the amount of spam they receive.[91] The campaign is only one way of distributing information to Internet users; other programs should also be examined.

Again, the global nature of spam did not go unrecognized by the Task Force. Unlike the U.S., the biggest producer and receiver of spam messages, only a small percentage of the spam received in Canada actually originates there. The report reiterates the need for international cooperation to combat spam at an international level, and goes on to address Canada's continuing involvement and commitment to finding a solution.

If Canada is to be successful in its fight against spam, anti-spam legislation is required. The Canadian government and the Anti-Spam Task Force have had the benefit of comparing and contrasting the anti-spam legislation of other countries to learn what has and has not worked. Canadian legislation should exploit the criticisms that have arisen from the *CAN-SPAM Act* to avoid making similar mistakes. The Task Force has had the opportunity to examine existing Canadian legislation that has been and will continue to be useful in the fight against spam; however, this has clearly not been enough. The particular nature of spam must be specifically addressed by legislation, having regard to its evolving nature as well.

A) Proposed Canadian Legislation

The Standing Senate on Transportation and Communications met with representatives from the Canadian Association of Internet Providers (CAIP) on 6 May 2004 to discuss and examine Bill S-2, *An Act to prevent unsolicited messages on the Internet.*[92] Although this was five days prior to the implementation of the Anti-Spam Task Force, the parties were aware of the goals and approaches that would be taken by the Task Force. CAIP took the position that a new anti-spam law was not the answer to the spam problem. The representatives were adamant that the elements of most anti-spam legislation found in other jurisdictions could already be found in existing Canadian laws, and the solution was not a new law but "targeted and aggressive enforcement" of these existing laws.[93] One of CAIP's concerns was the effectiveness of legislation to address future problems that may arise. Spam is continuously evolving

---

[91] "Three Key Tips for Combatting Spam," online: Stop Spam Here <http://stopspamhere.ca/spam-e.html#Tips>.

[92] *Proceedings of the Standing Senate Committee on Transport and Communications: Issue 10 – Evidence*, (6 May 2004), online: Parliament of Canada <www.parl.gc.ca/37/3/parlbus/commbus/senate/com-e/TRAN-E/10ev-e.htm>.

[93] *Ibid.*

and as a result, any legislation implemented today must take into consideration and be able to address future problems.

The Bill was thoroughly debated by the parties and ultimately rejected. The First Reading of Bill S-2 was on 3 February 2004 and following these further discussions, the Bill was discarded. The spam issue was reintroduced to the Senate in a second proposed Bill. This Bill, to prevent unsolicited messages on the Internet, made it to a second reading and was part of the Senate debates on 3 February 2005. Introduced by the Honorable Senator Oliver, Bill S-15 was an attempt to amend some of the problems that had arisen with the previous Bill S-2. Senator Oliver emphasized Canada's need for legislative action in the fight against spam and discussed legislative trends in other parts of the world. As a result of this analysis, Senator Oliver formulated what he felt to be the appropriate path for Canada. This path included legislation containing a "no-spam list," requiring individuals to give notice to the Minister (or delegated body of the Minister) that they wish to appear on the "no-spam list," and any individual sending spam would be required to check the list for addresses.[94] Furthermore, any implemented law would "explicitly permit a private right of action against spammers," and the statute would contain a fixed statutory damage.[95] This private right of action would include the ability to take action against businesses and individual spammers.

The Senator recognized the problems with simply using the existing legislation to combat spam. Not only does the legislation have substantial gaps, but it can also be too costly for individuals to use.[96] New legislation could alleviate some of the expense or uncertainty resulting from the use of the existing laws. Recognizing the global problems caused by spam, Senator Oliver indicated that any new legislation should permit the Competition Bureau and other investigative agencies, for example, the Privacy Commissioner, "to share information on spam investigations with counterparts in other countries."[97] In addition, the Senator addressed the need for this new legislation to address the various forms of spam, most specifically 'phishing' messages. It is evident that Senator Oliver had studied solutions that have achieved some success in other jurisdictions. However, Bill S-15 was not passed and spam legislation in Canada remains a controversial issue to be re-evaluated in the future.

---

[94] *Supra* note 89.
[95] *Ibid.*
[96] *Ibid.*
[97] *Ibid.*

B) Suggested Canadian Legislation

Any anti-spam legislation enacted in Canada must be supplemented by continuously evolving technological solutions, as it is evident that legislation alone will not be enough. The Canadian government has had the benefit of examining the successes and failures of current legislation in other jurisdictions and can formulate legislation upon these foundations. The suggestions proposed by the Anti-Spam Task Force incorporate these findings into what can be considered a respectable proposal for anti-spam legislation. Some of the problems associated with spam, however, are unaddressed by these propositions.

Canadian anti-spam legislation should incorporate the stricter approach of the required 'opt-in' provision. This approach, which has been taken in Australia, would curtail the amount of junk mail received by involuntary recipients; however, it is questionable if the legislation should go so far as to require a "no-spam list." The FTC issued a report in June 2004 regarding the proposal for a "National Do Not Email Registry."[98] The FTC reported that "without a system in place to authenticate the origin of email addresses," a registration system "would fail to reduce the burden of spam and may even increase the amount of spam received by consumers."[99] Canadian legislation would be subject to the same problems, and the effectiveness of a "no-spam list" is doubtful at this point in time.

In Bill S-15, Senator Oliver indicated that Canadian agencies involved in spam investigations must be able to discuss investigatory information with other countries. This would be a crucial provision in any anti-spam legislation. The American legislation has limited the FTC's enforcement capabilities, due to restrictions on the information it is allowed to divulge to other jurisdictions, thereby limiting the information they will be able to obtain from these jurisdictions in return. In order to manage spam, Canadian agencies need to be able to use the resources at their disposal and work together with other countries. Some leeway for the disclosure of investigatory information should be permitted to these agencies in the performance of their assigned roles.

In addition to the suggestions proposed by the Task Force, new anti-spam legislation needs to address the evolving forms of spam and tactics used by spammers. Other countries, such as Korea, have recognized the

---

[98] Federal Trade Commission, *National Do Not Email Registry: A Report to Congress* (Federal Trade Commission, June 2004), online: FTC <www.ftc.gov/reports/dneregistry/report.pdf>.

[99] *Ibid.*

need for guidelines pertaining to wireless spam.[100] With the increase in wireless products, such as BlackBerry technology, spam is now appearing in the form of text messages. Legislation needs to accommodate these wireless Internet technologies which will no doubt flourish in the future.

The Task Force also recognized the increase of 'phishing' spam messages and the dangerous nature of these messages needs to be addressed. As mentioned, these types of messages are primarily used for identity theft, which is a personal violation above and beyond that inflicted by regular spam messages. Strict penalties should be enforced against spammers who use these egregious methods. If the legislation is to have any deterrent effect on spammers, violators need to be punished so as to increase the fear of being caught. Penalties should include both substantial fines, and in the most severe cases, penal sanctions.

Together, the provisions of the *CAN-SPAM Act* and the rules outlined by the Anti-Spam Task Force provide a solid foundation for successful Canadian anti-spam legislation. It is doubtful that any legislation will be the 'silver bullet' against spam without making it illegal altogether. Like the U.S. legislation, any legislation implemented in Canada will be scrutinized and criticized. To date, Canada has conducted enough research and examined similar foreign laws that a responsible approach to the matter can be undertaken. This initial legislative attempt will not cure the problem, but is necessary in order to achieve long term success.

A GLOBAL SOLUTION TO SPAM

IT IS THE GLOBAL NATURE OF SPAM THAT MAKES eliminating or reducing it difficult. Existing anti-spam legislation is geared towards eliminating the problem locally, while recognizing the need for an international solution. While some countries have established agencies or cooperation networks to work together in the fight against spam, international legislation remains to be developed. Unfortunately, these existing agreements and arrangements have some obvious weaknesses that need to be addressed.

In 2004, representatives of private and public sectors from 15 countries met to discuss ways to improve international cooperation in the enforcement of anti-spam laws and regulations.[101] The result of the meeting was the London Action Plan on International Spam Enforcement Cooperation. The Action Plan is aimed at enhancing existing agreements

---

[100] *Supra* note 94.

[101] Federal Trade Commission, News Release, "FTC, International Agencies Adopt Action Plan on Spam Enforcement" (October 2004), online: FTC <www.ftc.gov.opa/2004/10/spamconference.htm>.

between enforcement agencies for the purposes of improving international cooperation. More recently, the Organisation for Economic Co-operation and Development (OECD) has established an anti-spam toolkit to provide countries with policy orientation and support in the fight against spam.[102] The toolkit addresses regulatory and policy issues, technical solutions, and enforcement concerns; it also includes suggestions for improved cross-border cooperation, as well as education and awareness tools.[103] This is a step in the right direction; however, without commitment and support from numerous countries, the long-term effectiveness of the toolkit is debatable.

It appears that in order to achieve the greatest success possible, an international treaty or agreement needs to be implemented. Such an approach would enable countries to share information, conduct investigations, and enforce laws across borders. The agreement would have to address any jurisdictional issues that may arise in relation to offshore spammers. The agreement would also have to compensate for the varying anti-spam laws that have been implemented in different countries. This would no doubt be a difficult task, as numerous countries have taken varying approaches in their fights against spam. It is evident that spam is a continuing, if not growing, problem worldwide and to achieve any success at the international level, further measures need to be taken.

CONCLUSION

THE UNIQUE CHARACTERISTICS OF SPAM make controlling it difficult. The *CAN-SPAM Act* and the Canadian Anti-Spam Task Force have demonstrated that reducing spam has not been and will not be an easy task. The *CAN-SPAM Act* and various other anti-spam legislations implemented by countries around the world have revealed tactics that have been successful and others that have not. These findings will no doubt enable other countries to develop their own legislation and perhaps be used in establishing a successful international treaty or agreement. Legislation must address not only the existing problems associated with spam but also provide for any potential future problems that may arise. If appropriate steps are not taken now, spam will continue to be a problem in the future.

---

[102] "Anti-Spam Toolkit" *Organisation for Economic Co-operations and Development*, online: OECD <http://www.oecd-antispam.org/>.
[103] *Ibid.*