A CALL FOR ACTION: THE NEED FOR CANADIAN SPAM LEGISLATION

Perry Cheung*

INTRODUCTION

What is Spam?

SPAM CAN BE DEFINED as unsolicited commercial e-mail sent to a large number of recipients.[1] Spam e-mails fill the inboxes of e-mail accounts all around the world, often attempting to entice sales for various products or services. It is a growing nuisance, which makes up for the majority of e-mail activity on the web today.

Why has spam become so popular? The development of the Internet and the emergence of e-mail have revolutionized the way individuals communicate and the way people do business. This revolution has created the opportunity for a new low-cost method of advertisement. Telemarketing and mailbox flyers were previously the popular methods of "cold calling," in which unsolicited advertisements were made to everybody, with no prior indications of potential interest in a product or service being necessary. This type of advertising still continues today, albeit at lesser volumes than in the past. Applying the cold calling methodology to e-mail accounts, however, has created a cheaper, faster, and ultimately more effective means of advertising. Not surprisingly, the practice of sending mass unsolicited commercial e-mails has become commonplace.

While success rates of spam as a method of advertising are lower than those of telemarketing and mailbox flyers, spam is a viable advertisement option because the marginal cost per recipient is negligible.[2] Spam is based on the idea that massive amounts of e-mail can be sent at a time at low cost and thus, sheer volume can make up for low success rates.

---

* LL.B. (UM, 2008)

1 *Meriam-Webster Online*, *s.v.* "spam", online: Merriam-Webster Online <http://www.m-w.com/dictionary/spam>.

2 John Magee, "The Law Regulating Unsolicited Commercial E-Mail: An International Perspective" (2003) 19 Santa Clara Computer & High Tech. L.J. 333 at 338.

Why is spam a problem?

Consider the fact that in 2000, spam made up approximately 10 percent of global e-mail traffic,[3] whereas by 2006, spam made up for 86.2 percent of e-mails.[4] Thus, the number of advertisement e-mails in circulation today greatly exceeds the number of legitimate e-mails. In 2003, America Online ("AOL") reported blocking two billion e-mails daily for their 26 million customers. This means that an average of approximately 75 spam e-mails was sent to every AOL customer on a daily basis.[5] Spam activities result in significant wasted time and energy spent on filtering out junk e-mails. Sometimes legitimate e-mails are accidentally deleted. Not surprisingly, this waste of human resources and these impediments to communication have had a highly negative impact on the business community.

Internet Service Providers ("ISPs") expend considerable effort on filtering out spam, which increases the costs of Internet service, as ISPs and e-mail servers spread fixed anti-spam software development costs to the consumer and are forced to increase their bandwidth capacity in anticipation of having spammers tie up large portions of bandwidth. While the additional per-user cost is likely negligible, access fees spent on time used filtering through e-mails from remote locations or from portable devices can have a significant cost to users.[6]

Spam also raises issues of security and privacy. Spam e-mails may contain spy-ware software that tracks activity or attempts to attain personal data. Sometimes software imbedded in spam e-mails will harvest e-mail addresses from contact lists of spam recipients, resulting in an abundant supply of additional e-mail addresses to which more spam can be sent. Furthermore, some spam e-mails contain viruses, Trojans, worms, and other forms of malicious software.[7]

Spam is also problematic because it creates opportunities for fraud. Spam e-mails are often the starting point for "phishing" schemes,

---

[3] Canada, Task Force on Spam, *Stopping Spam: Creating a Stronger, Safer Internet* (Ottawa: Information Distribution Centre, 2005) at 7, online: Industry Canada <http://www.e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/vwapj/stopping_spam_May2005.pdf/$file/stopping_spam_May2005.pdf > [Task Force on Spam].

[4] MessageLabs Intelligence, "A Year of Spamming Dangerously: The Personal Approach to Attacking (2006 Annual Security Report)" (December 2006), online: MessageLabs <http://www.messagelabs.com/resources/mlireports>.

[5] All Party Parliamentary Internet Group, *"Spam": Report of an Inquiry by the All Party Internet Group* (UK: October 2003) at 7, online: APIG <http://www.apcomms.org.uk/apig/archive/activities-2003/spam-public-enquiry/spam_report.pdf> [APPIG].

[6] *Ibid.*

[7] Task Force on Spam, *supra* note 3 at 1.

in which perpetrators fraudulently attempt to obtain sensitive personal information. In the current Internet era, perpetrators find it easy to hide behind false identities, as public e-mail services allow users to create numerous accounts without requiring any authentication of identity.[8] Technology also allows spammers to "spoof" e-mails, making them appear to originate from a false source in the header or in the IP address.[9] Accordingly, spammers are able to mislead consumers and hide from the authorities.

In the end, spam hurts everybody (save the spammers themselves), as it drains resources from all ends. Business efficacy and consumer confidence in the Internet is weakened, the growth of e-commerce is impeded, and negative economic consequences result. For large corporations, there are significant losses in productivity. In 2003, the Radicati Group, a research firm, estimated that spam cost corporations in the United States over $20.5 billion.[10] Thus, it seems that it is in the best interests of governments to take seriously the fight against spam.

Spam Legislation in Canada

Currently, there is no spam legislation in Canada. Initially, Canada's position on spam was one of passivity, as Industry Canada thought it would be best to allow market forces to deal with the problem.[11] In a 1997 discussion paper released by Industry Canada, it was said that spam legislation would not be necessary.[12] Spam was considered to be only a minor inconvenience at the time. It was said that in order to remain competitive, ISPs and e-mail service providers would learn to filter such activities. Furthermore, it was suggested that good business practices, privacy laws in the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), and remedies under the civil

---

[8] See U.S., Federal Trade Commission, *National Do Not E-mail Registry: A Report to Congress* (Federal Trade Commission, 2004) at 12, online: FTC <www.ftc.gov/reports/dneregistry/report.pdf> [FTC].

[9] *Ibid.*

[10] Industry Canada, *The Digital Economy in Canada: What is Spam?*, online: Industry Canada <http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00170e.html#spam>.

[11] Industry Canada, *The Digital Economy in Canada: Spam Discussion Paper: Internet and Bulk Unsolicited Electronic Mail* (Ottawa: July 1997) at 1, online: Industry Canada <http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf> [1997 Spam Paper].

[12] *Ibid.* at 4.

and criminal law could effectively combat spam. Unfortunately, spam has continued to grow.[13]

As foreign jurisdictions began implementing legislation to combat this problem in 2002,[14] the argument in favour of legislative action in Canada gained strength. In 2003, Industry Canada announced a change in its position, re-opening the debate about issues relating to spam.[15] Specifically, Industry Canada considered the need to implement legislation directed specifically towards spam. A "Task Force" was created to advise the government about an appropriate response to spam.[16]

In 2005, a report was released by the Task Force,[17] which discussed the growing problem of spam and made recommendations for its resolution. The report recognizes a need for legislative action in fighting spam, but it also suggests that this alone is insufficient. It recommends a multifaceted approach, drawing on all stakeholders to do their part in the fight. The report identifies sound business practices, consumer awareness, public education, and international cooperation as other tools necessary to combat spam.

Two years after the release of this report, there remains no spam legislation in Canada. More pressing issues, like healthcare, foreign policies, and the environment, seem to attract the attention of Canadian legislators. Thus, it appears that such legislation may not be enacted any time in the near future. This paper discusses why spam legislation is necessary in Canada nonetheless, and how such legislation should look.

DO WE NEED SPAM LEGISLATION IN CANADA?

SPAM LEGISLATION IS NECESSARY IN CANADA for two main reasons. Firstly, statistics show a relentless increase in spam,[18] which suggests that existing methods of spam control—criminal law, civil remedies, *PIPEDA*, and market forces—are not effective. Meanwhile, legislation targeted at spam in foreign jurisdictions seems to be showing some positive results. Secondly, as the Internet is a global resource, regulation and enforcement requires international cooperation. Canada is not pulling its weight in terms of combating spam. According to a study in the UK, Canada was the world's second leading source of spam

---

13 See Spam Growth Timeline, below.
14 See *ibid.*
15 Karen Ng, "Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet" (2005) 2 U. Ottawa L. & Tech. J. 447 at 464.
16 *Ibid.*
17 Task Force on Spam, *supra* note 3.
18 See Spam Growth Timeline, below.

in 2004.[19] The implementation of spam legislation would send a much-needed message to the world that Canada is on board in the global fight against spam.

Spam Growth Timeline	
1997	• Global spam volume represents less than 10 percent of total e-mail volume[20] • Industry Canada releases a discussion paper, saying spam legislation is unnecessary
2000	• Global spam volume reaches 10 percent of total e-mail volume[21]
2002	• Global spam volume climbs to 30 percent by the end of the year[22] • The EU implements its *E-Commerce Directive*, which includes a clause dealing with spam[23]
2003	• Global spam volume surpasses 50 percent[24] • In January, Industry Canada reopens dialogue to discuss issues relating to spam—the Task Force on Spam is created • Two high-profile legal actions in the United States are launched, reducing global spam rates to near 40 percent[25] • In December, the UK *Privacy and Electronic Communications Regulations*[26] take effect • Global spam rates at the end of the year exceed 50 percent[27]

[19] Michael Geist, "A recipe for battling spam in Canada" *Toronto Star* (3 May 2004) D.02.
[20] Task Force on Spam, *supra* note 3.
[21] *Ibid.*
[22] *Ibid.*
[23] EC, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] O.J. L 201/37, art. 13, s.4.
[24] Task Force on Spam, *supra* note 3.
[25] *Ibid.*
[26] *The Privacy and Electronic Communications (EC Directive) Regulations 2003*, S.I. 2003/2426.
[27] Task Force on Spam, *supra* note 3.

2004	• In January, the American *CAN-SPAM Act*[28] takes effect • In April, the Australian *Spam Act 2003*[29] takes effect • In July, global spam volume peaks at 94.5 percent of total e-mail volume[30] • Two high-profile legal actions in the United States are subsequently launched, reducing global spam rates to just below 75 percent[31] • Global spam volume makes up 80 percent of total e-mail volume by the end of the year[32]
2005	• In May, the Canadian Task Force on Spam releases a report recommending various actions to combat spam, including legislative action[33]
2006	• MessageLabs Annual Intelligence Report shows an average annual global spam rate of 86.2 percent[34]

The Statistics

The statistics clearly show that spam is on the rise globally. This explains the evolution of Industry Canada's position on spam and the implementation of spam legislation in other jurisdictions.

In a MessageLabs study conducted for the Task Force on Spam,[35] it was shown that certain events have made big dents in the amount of global spam sent out. Spam rates appear to have dropped following the implementation of the *E-Commerce Directive* and the *CAN-SPAM Act*.[36] The most significant drops, however, seemed to follow high-profile legal actions in the United States.[37]

Yet global spam rates are still climbing and are now at an all-time high. Some might argue that this means legislation is ineffective. However, the fact that spam rates are still climbing may simply suggest that there are flaws in existing legislation in foreign jurisdictions, which Canada now has the opportunity to avoid.

---

[28] *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, Pub. L. No. 108-187, 117 Stat. 2699 (2003) [*CAN-SPAM Act*].
[29] *Spam Act 2003* (Cth.).
[30] Task Force on Spam, *supra* note 3.
[31] *Ibid.*
[32] *Ibid.*
[33] Task Force on Spam, *supra* note 3.
[34] MessageLabs, *supra* note 4.
[35] Task Force on Spam, *supra* note 3.
[36] *Ibid.*
[37] *Ibid.*

Market Forces and Existing Methods of Combating Spam

As illustrated by increasing spam rates and Industry Canada's evolving position on spam legislation, it can be said that market forces, privacy legislation, good business practices, and existing civil and criminal penalties are simply not effective in fighting spam.

It was originally thought that Internet service providers and e-mail servers would invest in filtering technology in order to stay competitive. It was thought that this investment would be sufficient to stop spam.[38] Yet now, despite significant sums of money being spent on filtering, spam continues to be a problem.[39]

Private actions targeted towards spam could include trademark dilution and unfair competition, nuisance, interference with contractual or business relations, trespass to chattels, or breach of contract (regarding terms of use for ISPs).[40] There are many difficulties associated with these private actions, however. It is difficult to attain remedies for Internet torts, firstly because the defendants are not easy to identify. When they are identified, there may be issues of jurisdiction and conflict of laws.[41] Furthermore, for the private complainant, it would be impractical to spend the time and money necessary to attain a civil remedy, as the damages would be minimal and an injunction stopping one spammer would make no visible impact on the amount of spam received.[42]

Spammers who intend to injure by sending false messages or deceitful, fraudulent messages may be subject to penalty under ss. 372(1) and 380 of the *Criminal Code*.[43] However, like private actions,

---

[38] Ng, *supra* note 15 at 458.
[39] Task Force on Spam, *supra* note 3 at 8.
[40] Ng, *supra* note 15 at 462.
[41] *Ibid.*
[42] In a private small claims action between business owner Nigel Roberts and spammer Media Logistics Ltd., Roberts was awarded a mere £300 and an apology. See Chris Hunter, "UK Spam Landmark Case" *Spamfo* (29 December 2005), online: Spamfo <http://www.spamfo.co.uk/component/option,com_content/task,view/id,370/Itemid,2/>.
An example of a private action through non-legal means is the case of Vardan Kushnir of Russia. Kushnir was Russia's largest known spammer. Defiant about his right to spam, he sent millions of unsolicited e-mails daily, advertising his English Learning Centers. In July 2005, Kushnir was murdered and police believed that an anti-spam gang may have been responsible. See Hardware Geeks, "Russia's Biggest Spammer Murdered by Anti-Spam Group?", online: Hardware Geeks <http://www.hardwaregeeks.com/comments.php?shownews=3399>.
[43] *Criminal Code*, R.S.C. 1985, c. C-46, ss. 372(1) & 380.

criminal law enforcement is difficult because of issues with identification, jurisdiction, and the futility, from the individual e-mail recipient's standpoint, of reporting these illegal activities to the authorities, as one less spammer would not make a noticeable difference in the amount of spam received. Additionally, injurious, false, and deceitful messages make up only a portion of spam, leaving a significant amount of unsolicited commercial e-mails free from criminal sanctions.

In 2000, *PIPEDA*[44] was enacted in Canada in response to the concerns of the international business community about privacy. Legislative action became necessary in order for Canadian businesses engaged in certain activities to continue to do business abroad.

PIPEDA regulates the use, collection, and disclosure of personal information in the course of commercial activity. The Act protects information such as names, social insurance numbers, credit cards, or any other information that might be gathered in a business transaction. "Personal information" protected by *PIPEDA* is defined very broadly as "information about an identifiable individual."[45] Therefore, it can be said that a person's e-mail address also falls under the scope of protected personal information. This was the finding of the Office of the Privacy Commissioner ("OPC") in *PIPEDA Case #297*.[46]

PIPEDA also restricts the harvesting and sale of e-mail addresses and protects users from being added to spam lists without their consent,[47] as the collection, use, and disclosure of personal information is restricted under the Act.[48] *PIPEDA* requires that organizations identify and disclose the purpose for which they are collecting information, and acquire consent before using or disclosing the information. Thus, the Act seems to require that e-mail recipients opt-in to a mailing list before spammers may attempt to solicit sales to them by e-mail.

There is one major shortfall of *PIPEDA* in its ability to combat spam, however. *PIPEDA* does nothing to impede the activities of those who spam accounts by randomly generating combinations of names, numbers, and words, as no personal information is used in this type of spam activity. Therefore, under Canadian law, in the absence of fraud or malicious conduct, spammers who send advertisements to e-mail accounts derived from random combinations of names, numbers, and words are free from prosecution.

---

44 *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c.5 [*PIPEDA*].

45 *Ibid.*, s.2(1).

46 Canada, Office of the Privacy Commissioner of Canada, "Commissioner's Findings: *PIPEDA* Case Summary #297" (28 April 2005), online: OPCC <http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_e.asp> [*PIPEDA* Case Summary #297].

47 See Ng, s*upra* note 15 at 459.

48 See *PIPEDA*, *supra* note 44, s.7.

Ultimately, while *PIPEDA* does impede the efforts of certain spammers, it alone is inadequate to stop spam. ISPs and e-mail servers now have advanced junk e-mail filters, but spam e-mails still find their way into inboxes. It is evident that the position that Industry Canada set out in their 1997 report was flawed. Market forces, existing privacy laws, and existing criminal and civil penalties are still insufficient to solve the problem of spam.

The Need for International Cooperation

The Task Force on Spam recognizes that international cooperation is required in order to effectively fight spam.[49] Spammers target e-mail accounts all over the world, not just those based in their home country. Especially where potential e-mail recipients are randomly generated, spammers outside of Canada are just as likely to target Canadians as they are to target non-Canadians. Thus, the fight against spam requires international cooperation,[50] with every country taking action within its own borders. Currently, Canada is not pulling its weight.

The European Union has led the way with its 2002 *E-Commerce Directive*, which includes a provision that member countries prohibit spammers from disguising their identities, and requires them to make available and respect opt-out registers.[51] This creation of uniform minimum standards across numerous member nations may be seen as a big first step.

A more critical analysis, however, shows that the spam provisions in the *E-Commerce Directive*[52] are still nothing revolutionary. The restrictions on spammers are very mild and thus, little ground is gained in the fight against spam. For example, the mandatory opt-out options required by the *EC Directive* are arguably useless when it comes to fighting spam, as the act of opting out can sometimes increase the amount of spam received by confirming for spammers: a) the validity of a user's e-mail address and b) that spam e-mails are in fact read by that user.[53]

More problematic is the fact that countries participating in the *EC Directive*[54] have no obligations with regards to putting resources into

---

[49] Task Force in Spam, *supra* note 3 at 5.
[50] See Industry Canada, *An Anti-Spam Action Plan for Canada* (2004) at 9, online: Industry Canada <http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/vwapj/Anti-Spam_Action_Plan.pdf/$file/Anti-Spam_Action_Plan.pdf>.
[51] *Directive 2002/58/EC of the European Parliament*, *supra* note 23.
[52] *Ibid.*
[53] Karla Dane, "Controlling Spam: The Prospect of Legislative Success" (2006) 6 Asper Rev. Int'l Bus. & Trade L. 241 at 248.
[54] *Ibid.*

enforcement. It is one thing for an act to be made illegal, but it is another to actually monitor and sanction the illegal acts. In order to be effective, any attempt to regulate the Internet requires a devotion of resources towards its monitoring. If this is not done, spammers will never be caught, as the nature of the Internet allows identities to easily be disguised. Thus, without adequate resources being put into monitoring and investigative activities, the *E-Commerce Directive* restrictions on spam activities will have little impact on spam rates.

As spam enforcement may not find itself as a top priority for many countries, the negotiation of large-scale multilateral spam treaties to push this agenda is necessary. Unfortunately, such a scheme is likely to be feasible only within the European Union at this point in time. The EU involves a sufficiently small number of countries with sufficiently similar interests such that areas like electronic commerce have already become internationally regulated.[55] Conversely, other international bodies currently lack the organizational capacity and united priorities of member states to achieve this goal. While it might be suggested that the United Nations ("UN"), the World Trade Organization ("WTO"), or the Organisation for Economic Co-operation and Development ("OECD") should push the agenda of anti-spam provisions,[56] an attempt to attain an agreement with too large a number of countries on an issue not seen as a priority to numerous member nations would be doomed to failure. For this reason, the OECD has created a Task Force on Spam with a purely educational mandate.[57]

The notion of spam treaties is not far-fetched, however, as combating spam is generally in the interests of all nations. Treaties regarding spamming restrictions are not like environmental treaties (e.g. Kyoto), in that participating countries should suffer no adverse economic consequences. Spam treaties would likely result in economic benefits, as productivity impediments in the workplace would be removed, resulting in productivity gains across the globe. Thus, with pressure being placed on the international community to act, there is potential for progress by means of small-scale international agreements.

The United Kingdom has made a start with its *London Action Plan* ("*LAP*").[58] In October 2004, government and public agencies from 27 countries met in London to discuss international cooperation regarding spam enforcement. Out of this meeting emerged a plan that ultimately facilitates communication and cooperation between various spam

---

[55] See *Directive 2002/58/EC of the European Parliament*, *supra* note 23.
[56] See APPIG, *supra* note 5 at 24.
[57] OECD Task Force on Spam, "About" (January 2006), online: OECD Task Force on Spam <http://www.oecd-antispam.org/article.php3?id_article=41>.
[58] Federal Trade Commission, "The London Action Plan On International Spam Enforcement Cooperation", online: FTC <http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf>.

enforcement agencies around the world. The *LAP* now makes up an international spam enforcement network involving membership from various enforcement agencies across the globe. Participating agencies from Canada include Industry Canada and the Office of the Privacy Commissioner of Canada.

The *LAP* is a big step in the fight against spam, as it has generated international recognition of spam by various countries, including developing ones.[59] Cooperation amongst international agencies has also shown results fairly quickly. In February 2005, operation "Spam Sweep" brought agencies from over 30 countries together to analyze 300,000 spam e-mails, which has triggered over 300 in-depth cross-border investigations.

Despite its positive impact on the fight against spam, the shortfall of the *LAP*, however, is that it still does not require legislative action from participating countries. It makes investigations of spam activities easier through information sharing where combating spam is already on a nation's agenda, but does nothing to require that anti-spam provisions be implemented or enforced for countries not currently involved in the fight against spam. Membership consists of enforcement agencies within countries, various anti-spam organizations, and observing members from around the world. Governments themselves however, do not directly participate as members.[60] Unfortunately, without encouraging legislative standards through treaties, spammers in jurisdictions without anti-spam laws remain untouchable. No level of cooperation between anti-spam agencies can solve the jurisdictional boundaries that prevent extra-territorial enforcement in a place where spam activities are legal. Perhaps this is why in July 2007, the United States Federal Trade Commission hosted a two day "Spam Summit," bringing businesses, government, technology experts, and consumer advocates together to discuss the problem of spam and its potential solutions.[61] Unfortunately, this meeting turned out to be more of a discussion about the state of things

---

[59] When the *LAP* was put into place, China was seen as the second largest source of spam. Their adoption of the *LAP* is significant because it indicates that spam is not just a problem for the developed world. See Chris Hunter, "Beijing signs up to global anti spam accord" (July 2005), online: Spamfo <http://www.spamfo.co.uk/component/option,com_content/task,view/id,346/Itemid,2/>.

[60] London Action Plan, "LAP Member Organizations," online: LAP <http://londonactionplan.org/?q=node/5>.

[61] OECD Task Force on Spam, "Federal Trade Commission Spam Summit 2007" (28 May 2007), online: OECD Task Force on Spam <http://www.oecd-antispam.org/article.php3?id_article=277>.

and the effectiveness of certain tools, rather than a venue to discuss political anti-spam treaties.[62]

With no spam legislation of its own at the moment, however, Canada is in no position to press the issue of international spam agreements. Canada must first fight spam within its own borders before it can pressure other countries to take action. It seems that the first logical step in doing this is legislative action.

WHAT SHOULD CANADA'S SPAM LEGISLATION LOOK LIKE?

AS DISCUSSED, THERE ARE STRONG ARGUMENTS favouring the notion that Canada should implement spam legislation. The next question then, is how should Canada's spam legislation look? In considering this question, the spam legislation in foreign jurisdictions provides examples for potential Canadian legislation to model itself after. The United States, Australia, and the UK have been global leaders in implementing spam legislation in 2003 and 2004,[63] and by doing so, have provided examples from which Canada may draw ideas. The recommendations by the Task Force on Spam[64] are also available for further guidance. Finally, this paper considers the legal framework in which any Canadian legislation must fit, i.e. compliance with the *Canadian Charter of Rights and Freedoms*.[65]

Elements of Spam Legislation

This paper breaks down the contents of spam legislation into three main elements. Accordingly, three issues must be resolved. What activities should be prohibited? Who should be protected by the legislation and who should be held responsible? That is, what nexus to the spam activity should be necessary to result in liability? And finally, what should the penalties be and who should enforce them?

---

[62] Barry Leiba, "Staring At Empty Pages" (13 July 2007), online: BlogSpot <http://staringatemptypages.blogspot.com/2007/07/ftc-spam-summit-day-2.html>.

[63] See Spam Growth Timeline, above.

[64] Task Force on Spam, *supra* note 3 at 3.

[65] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

1. What activities should be prohibited?

Foreign jurisdictions have presented a variety of legislative options, most importantly with regards to deciding what is to be prohibited by such legislation. For example, as will be discussed in the following sections, legislation could include either an opt-in or an opt-out scheme, it might provide exemptions for business-to-business communications, and it might exempt certain parties, such as charities.

a. Other Jurisdictions

i. The United States

The *CAN-SPAM Act*[66] in the United States places restrictions on e-mails that promote goods or services. The Act bans false or misleading header information, prohibits deceptive subject lines, requires that e-mail recipients be given an opt-out method, requires that commercial e-mails are labeled as advertisements, and requires that senders include their valid physical addresses in their e-mails.[67] This approach appears to address the opportunities for fraud that spam presents by requiring the sender to provide accurate information about him- or herself. While these provisions do not reduce the amount of spam received, they make the spam received more identifiable; thus, easier to filter, addressing the problem of wasted time due to spam. However, the American legislation pre-empts stricter state laws and essentially creates a guideline on how to spam legally.[68] In doing so, the *CAN-SPAM Act* in fact reduces the risk of legal liability involved in spamming, while only partially negating its effects. Also, as discussed above, opt-out provisions arguably provide no protection to Internet users, as the act of opting out can potentially lead to an increase in the amount of spam received. For these reasons, the American anti-spam legislation has been harshly criticized.[69]

However, despite criticisms of the American legislation being too permissive, in 2004, a Virginia spammer was sentenced to nine years in

---

[66] *CAN-SPAM Act*, *supra* note 28.

[67] U.S., Federal Trade Commission, "The CAN-SPAM Act: Requirements for Commercial Emailers" (April 2004), online: FTC <http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.shtm>.

[68] Lily Zhang, "The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem" (2005) 20 Berkeley Tech. L.J. 301.

[69] See Spamhaus News, "United States set to Legalize Spamming on January 1, 2004" (22 November 2003), online: Spamhaus <http://www.spamhaus.org/news.lasso?article=150>. See also APPIG, *supra* note 5 at 22.

prison for violating state laws on spam.[70] These laws mimicked the federal *CAN-SPAM* law, merely limiting the number of spam e-mails sent in a given time frame and prohibiting the use of fake e-mail addresses.

More recently, a Nevada-based spamming company was ordered to pay Earthlink, an ISP, 5.8 million pounds in a law suit based on *CAN-SPAM* prohibitions.[71] It would appear that the *CAN-SPAM Act* is thus able to provide recourse for some complainants and in due course, it might prove its critics wrong.

Another interesting concept in the United States stems from the *Do Not Call Registry*,[72] which was enacted in March 2003 to protect consumers (but not businesses) from telemarketers. Under this program, residents of the United States are able to put their phone number in the registry free of charge. Telemarketers are then required to check the *Do Not Call Registry* every month and exclude registered phone numbers from their telemarketing activities. A 2005 Report to Congress by the Federal Trade Commission found that the *Do Not Call Registry* was highly effective in combating telemarketing.[73] Accordingly, an analogous "Do Not Spam Registry" might be an effective means of combating spam. This concept was suggested to Canadian Parliament through Bill S-2 in February 2004, but was ultimately rejected.[74]

One problem is that the use of such a registry would not prevent the outsourcing of spam activities to spammers outside of the Canadian jurisdiction, as a Do Not Spam Registry would be unenforceable in jurisdictions outside of Canada. Furthermore, the registry only protects those who are aware of it and actively participate in it. This is a problem, because the goal is to provide protection internationally, but for obvious financial and logistical reasons, such a registry would only be advertised in Canada. In addition, enforcement of such a registry would be difficult, as no authentication is required for the creation of new e-mail accounts and thus, spammers can disguise their identity. Furthermore, the potential for a database of registered e-mails to get into the hands of

---

[70] Spamhaus News, "September brings four powerful legal setbacks to the world's spammers" (October 2006), online: Spamhaus <http://www.spamhaus.org/news.lasso?article=610>.

[71] Spamhaus News, "Summer Spam Suits Show Some Success" (October 2006), online: Spamhaus <http://www.spamhaus.org/news.lasso?article=165>.

[72] "National Do Not Call Registry", online: National Do Not Call Registry <www.donotcall.gov>.

[73] U.S., Federal Trade Commission, *Annual Report to Congress for FY 2006: Pursuant to the Do Not Call Implementation Act of the Do Not Call Registry* (Federal Trade Commission, April 2007) at 11, online: FTC <http://www.ftc.gov/os/2007/04/P034305FY2006RptOnDNC.pdf>.

[74] Dane, *supra* note 53 at 260.

spammers presents a significant risk of counter-productivity.[75] For these reasons, the FTC, in a Report to Congress,[76] recommended against the implementation of a Do Not E-mail Registry.

An international Do Not E-mail Registry might be more effective than a domestic one in protecting Internet users from global sources of spam, as participating nations would only need to take responsibility for advertising and enforcing provisions of the registry within their own jurisdiction. However, the security concerns raised by the FTC in their Report to Congress[77] regarding the value of such a database to spammers would remain, and international efforts towards an e-mail identity authentication scheme would still be a necessary prerequisite in making the identification of deceptive spammers feasible. Furthermore, expecting negotiations for such an international design would not be realistic at present, as more pressing issues (i.e. war, the environment) currently take the international stage.

ii. Australia

Australian legislation takes the strictest position against spam, as it aims to reduce the actual amount of spam sent out by prohibiting all commercial e-mails from being sent without the consent of the receiver. Defining consent is of great importance with this approach.

In Australia, under the *Spam Act 2003*, consent may be express or inferred, with inferred consent arising through specific relationships and conduct between the parties. Essentially, a pre-existing two-way relationship is required, such that it can be inferred that the recipient would more likely than not be happy to receive a given e-mail.[78] While in the United States, spam e-mails must include an option to opt out of receiving spam e-mails, no spam e-mails may be sent in Australia unless recipients have signed up for a mailing list.

However, a business function rule applies to allow businesses to send e-mails that are conspicuously published to a wide audience such that consent is clear, where the e-mail relates to a business function relevant to the commercial e-mail, or where parties fall under a specific set of enumerated relationships. Also, the receiver must not have expressed a desire not to receive the commercial messages. Within this legislation, an exception is set out that exempts charities, government bodies, registered political parties, and religious organizations from anti-

---

[75] See U.S., Federal Trade Commission, *National Do Not E-mail Registry: A Report to Congress* (Federal Trade Commission, 2004) at 15-24, online: FTC <www.ftc.gov/reports/dneregistry/report.pdf> [FTC].
[76] *Ibid.* at 37.
[77] *Ibid.* at 16.
[78] *Spam Act 2003*, supra note 29 at Schedule 2.

spam provisions.[79] Interestingly, this exception has been criticized in the UK as being too broad.[80]

Ultimately, the *Spam Act 2003* severely curtails the ability to send spam e-mails, but the carefully designed consent provisions attempt to prevent legitimate business from being impeded. Relative to spam legislation in other jurisdictions, the *Spam Act 2003* appears to provide the greatest amount of protection to the various stakeholders affected by spam. Critics have hailed this Act as being the most effective spam legislation currently in place.[81] According to a 2007 report by Sophos, Australia is now responsible for a mere 0.6% of the spam relayed globally.[82]

Recently, the Australian spam legislation has been the subject of a high profile case. In 2006, a $4.5 million penalty was delivered to Clarity1 Pty Ltd. and $1 million was awarded against its managing director for the company's acts of sending spam and using harvested e-mail address lists.[83] The Australian Communications & Media Authority ("ACMA"), the enforcers of the *Spam Act 2003*, have boasted about the effectiveness of the legislation, claiming to have required over 200 Australian businesses to amend their practices in order to comply with the Act and to have fined five of these businesses for substantial breaches.[84]

iii. The United Kingdom

On the opposing end of the legislative restrictiveness spectrum are the United Kingdom *Privacy and E-Commerce Regulations*,[85] where only unsolicited commercial e-mails sent to individual e-mail network subscribers are prohibited. In other words, spam directed towards

---

[79] *Ibid.* at Schedule 1, s.3.

[80] See APPIG, *supra* note 5 at 23.

[81] Spamhaus executives note seeing a decrease in Australian spam activities since the implementation of the *Spam Act 2003*, with spammers keeping a low profile, ceasing spam activities, or leaving the country. See Spamhaus, "Follow Australia!" (19 July 2004), online: Spamhaus <http://www.spamhaus.org/news.lasso?article=154>.

[82] Sophos, "Sophos research reveals dirty dozen spam-relaying nations" (April 2007), online: Sophos <http://www.sophos.com/pressoffice/news/articles/2007/04/dirtydozapr07.html>.

[83] *Australian Communications and Media Authority v. Clarity1 Pty Ltd*, [2006] FCA 410. For a brief summary of the *Spam Act 2003* in action, see Caslon Analytics, "Caslon Analytics profile: Australia & NZ spam regulation" (October 2006), online: Caslon Analytics <http://www.caslon.com.au/anzspamprofile3.htm#cases>.

[84] *Ibid.*

[85] *Privacy and Electronic Communications Regulations, supra* note 26, s.22.

business e-mail addresses is legal, given that there is no deception regarding its source. This exception exists because it is recognized that there is some value in allowing advertising between businesses, and the privacy interest is not as important for businesses as it is for the individual. A study of the business generated from spam was conducted and found that in the UK, 44 percent of Internet users had purchased something as a result of receiving an unsolicited e-mail.[86] The criticism of the approach in the UK, however, is that the economic damage caused by spam in terms of slowing down businesses is not adequately addressed.

Clearly, nobody wants to have their e-mail accounts flooded with uninvited advertisements for products or services that they have no interest in. However, the fact that actual sales sometimes occur as a result of spam e-mails suggests that there is some economic value creation from these advertisements. Thus, determining how much to restrict e-mail advertisements becomes the key question. The approaches in foreign jurisdictions differ, providing distinct balances between preventing e-mail account flooding and preserving legitimate business.

It is clear that there is no value in deceptive e-mails where the sender's identity is disguised, however. There is no countervailing interest to be considered in restricting such activities. Thus, it is appropriate for Canadian legislation to, at minimum, implement provisions prohibiting deceptive e-mails.

A dispute between a UK spammer and a small-business owner in the Channel Islands demonstrates the arguable ineffectiveness of the UK approach to finding the appropriate balance between minimizing the problems caused by spam while preserving the business it generates. Nigel Roberts, an Internet business owner who received spam from Media Logistics UK, received an apology letter and compensation of £270 plus an indemnification of his £30 filing fee.[87] This dispute illustrates and perhaps contributes to, through an anchoring effect, the futility of personal claims against spammers through the UK *Privacy and Electronic Communications Regulations*. In attempting to create a legislative solution with actual teeth, a Canadian approach should thus be more restrictive of spam activities and impose harsher penalties than those in the UK.

b. Task Force on Spam Recommendations

The report prepared by the Canadian Task Force on Spam provides some insight as to where Canadian values might lie. The report offers a list of recommendations as to what legislative action is required.

---

[86] See Business Software Alliance, "Consumer Attitudes Toward Spam in Six Countries" (December 2004) at 11, online: Coalition Against Unsolicited Commercial Email <http://cauce.ca/system/files/BSAConsumerAttitudes.pdf>.
[87] See Hunter, *supra* note 42.

The report suggested fairly restrictive measures, similar to those in Australia. The Task Force recommended that the following practices be made illegal:

- failing to abide by an opt-in regime for sending unsolicited commercial e-mail;
- the use of false or misleading headers or subject lines designed to disguise origins, purpose, or contents;
- the construction of false or misleading URLs for the purpose of collecting personal information or engaging in criminal conduct;
- the harvest of, use of, or supply of e-mail address lists without consent; and dictionary attacks.[88]

Clearly, preventing fraud is advantageous. Thus, provisions prohibiting misleading headers, subject lines, and URLs are necessary elements of any spam legislation that might be passed.

Restrictions on e-mail harvesting and supplying are already in place through *PIPEDA*; thus, such restrictions in new spam legislation would be redundant. However, the inclusion of such provisions, if consistent with *PIPEDA* provisions, would do no harm.

The area of debate is whether or not requiring an opt-in scheme is the best method of addressing spam. Requiring an opt-in scheme means that spammers can only e-mail those who have signed up for mailing lists. In other words, consent is required. This position recognizes that spam is a growing problem and that stronger measures are required to combat it. However, such a strict scheme could result in lost economic activity, as sales from spam e-mails would be significantly reduced. The UK has recognized economic value in some spam e-mails and has therefore drawn a line between business recipients and personal recipients.

The same 2004 survey conducted by Forrester Data that found 44 percent of UK Internet users to have made a purchase in response to a spam e-mail also found that 32 percent of Canadians have made purchases or have taken advantage of offers received by way of spam.[89] Thus, it can be said that there is economic value to spam in Canada, as well as in the UK. At 32 percent, however, Canadians were the least likely of countries surveyed to purchase products or services advertised through spam.[90] Accordingly, it can be said that Canadians place less

---

[88] Task Force on Spam, *supra* note 3 at 15. A dictionary attack consists of trying "every word in the dictionary" as a possible password for an encrypted message. See Tech Faq, "What is a dictionary attack?", online: Tech Faq <www.tech-faq.com/dictionary-attack.shtml>.

[89] See Business Software Alliance, *supra* note 86.

[90] See *ibid.*

value on the potential economic stimulation that spam provides than citizens in foreign jurisdictions. This conclusion suggests that an approach placing greater value on protecting individuals and businesses from spam, thus, an approach that severely restricts spamming activities, with few exceptions, is consistent with Canadian values.

c. Fitting into the Canadian Legal Framework

As recognized by Industry Canada in their comparison of international spam legislation, each country has a unique legal framework that must be studied in considering imitating legislation abroad.[91]

It is likely that restrictions on spam violate s.2(b) of the *Charter*, as it limits a form of expression.[92] However, such restrictions could most likely be saved under s.1. Protecting consumers and businesses from the problems caused by spam is arguably a pressing and substantial objective. Legislative prohibitions on spam activities would clearly help address these problems.

The problem is the concept of minimal impairment. Does minimal impairment require that legislation not restrict all unsolicited commercial e-mails, but rather restrict only the elements of deception and fraud? Does it require that the United States approach be adopted, and spam merely be identified as advertising?

While it should be accepted that protecting businesses and individuals from time consuming spam e-mails is a pressing and substantial purpose, it could be said that merely requiring the identification of spam e-mails as advertisements would adequately fulfill this purpose. However, if the objective of the legislation is to reduce the influx of unwanted e-mails, a mere identification requirement would not fulfill the legislative purpose, as provisions requiring proper identification would probably not contribute to any reduction in spam volume; rather it would only result in a slight change in the content of spam e-mails. Thus, if the objective of spam legislation is to reduce spam volume, it can be said that making consent a requirement does minimally impair a s.2(b) infringement. Ultimately, considering the extent to which the spam problem has risen, proportionality should not be a problem and the restriction on freedom of expression should be justifiable under s.1.[93]

---

[91] Industry Canada, "International Spam Measures Compared" (May 2005), online: Industry Canada <http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/gv00345e.html>.

[92] See *R. v. Keegstra*, [1990] 3 S.C.R. 697 at para. 34.

[93] Ng, *supra* note 15 at 485.

Accordingly, the *Charter* is unlikely to become an issue in the passing of spam legislation.[94]

Canadian federalism also presents an interesting question. Is combating spam the responsibility of the provinces or the federal government? Just as international cooperation is important, Internet regulation is something that must also be enforced consistently across the country if it is to be effective. Because of the borderless nature of the Internet, an Internet regulator must face as few jurisdictional problems as possible to be effective. In Canada, failure to enforce spam regulations in one province would create a safe haven situation, where spammers could continue to target recipients outside the safe haven province. Thus, it can be said that spam is a matter that is indivisible in nature. Accordingly, spam is a matter of national concern, bringing it under the s.1 *Charter* POGG power of the federal government.[95]

The desire for consistency with other legislation is also a factor to be taken into account. Currently, Canadian legislation dealing with spam is limited to *PIPEDA* and the *Criminal Code*. Provisions in *PIPEDA* and the *Criminal Code* require consent for the use of personal information, including e-mail addresses, and prohibit unauthorized use or abuse of computers. It could thus be argued that Canada currently has in place an opt-in scheme,[96] albeit practically ineffective, and it would be appropriate to continue this approach for consistency purposes.

In addition, a recent Canadian Radio-television and Telecommunications Commission ("CRTC") decision regarding a Do Not Call List ("DNCL") that is in the works provides further guidance.[97] While it seems that a Do Not Spam registry is not the best approach at this time,[98] the exemptions set out in the Do Not Call List framework created by the CRTC might be appropriate exemptions for anti-spam legislation as well. Examples of entities exempt from the DNCL are registered charities, political parties, surveyors, and telemarketers that have existing business relationships with consumers.[99]

d. The Final Product

The position of the Task Force on Spam suggests that Canadians would find the economic activity generated by spam to be insignificant

---

[94] See *ibid.* at 489.
[95] See generally *R. v. Crown Zellerbach Canada Ltd.*, [1988] 1 S.C.R. 401. See also *ibid.* at 478.
[96] See Industry Canada, *supra* note 91.
[97] See Canadian Radio-Television and Telecommunications Commission, "Telecom Decision CRTC 2007-48" (3 July 2007), online: CRTC <http://www.crtc.gc.ca/archive/eng/decisions/2007/dt2007-48.htm> [CRTC].
[98] See FTC, *supra* note 75.
[99] CRTC, *supra* note 97.

compared to the nuisance imposed on individuals and the economic harm caused to businesses, as discussed above. As spam continues to grow relentlessly and spam rates now approach the 90 percent mark, strict methods of combating spam are justified.

Accordingly, Parliament should pass legislation that prohibits unsolicited commercial e-mails. To comply with the law, mass commercial e-mails should require consent, which could be obtained either through users signing up for mailing lists or by having existing business relationships, as is the case in Australia.[100] In other words, an opt-in scheme is the best approach. The Australian legislation sets out a schedule in which consent is defined in great detail with regards to particular relationships and the communications that occur between the two parties. A similar approach in Canadian legislation would be effective.

In order to prevent the loss of legitimate economic activity arising from commercial e-mails, consent should specifically be inferable from existing relationships with customers, both individuals and businesses. This approach would be similar to those taken in Australia and the UK. With regards to other exceptions for charitable institutions or political parties, however, the propensity for fraud on the Internet should make the notion of spam-based marketing for charities and political parties unappealing, as it would seemingly take away from the credibility of the charity or party being promoted. Accordingly, no exceptions for special groups should be set out beyond the existing relationship exception.

In addition, as mentioned earlier, Canadian spam legislation should prohibit the disguising of the sender's identity and any deception in commercial e-mails. Such deceptive activities create no economic benefit. They merely create opportunities for fraud.

With regards to surveys, it seems that the dangers of fraud would not be as pressing in survey-based spam e-mails as they would be in spam soliciting sales or donations. It seems that optional surveys sent via e-mail would be no more intrusive than those conducted over the phone. Thus, in light of the CRTC exempting telephone surveys from their Do Not Call List that is in the works,[101] it seems that an exemption for surveys in Canadian spam legislation might be appropriate as well.

2. Who is protected and who is to be held responsible?

If spam legislation is intended to protect Canadian businesses and individuals, it might be appropriate to hold liable any person or corporation that sends spam to Canadians. However, the provisions of

---

[100] *Spam Act 2003*, *supra* note 29 at Schedule 2.
[101] CRTC, *supra* note 97.

the Australian *Spam Act 2003* requiring an Australian connection[102] raise interesting hypothetical situations that should be addressed. Is a Canadian who is on vacation overseas protected? Should this Canadian be held liable for acts committed outside of Canada? Should a multinational company with a head office in Canada be liable if it sends spam to another country through an offshore office? Should Canadians in general be prevented from sending spam to recipients outside of Canada? Generally speaking, what degree of involvement should attract liability?

The Australian *Spam Act 2003*[103] covers all e-mail messages with links to Australia. This includes situations where senders are physically present in Australia, the physical devices used to send messages are in Australia, businesses have central management in Australia, e-mail messages are received by computers in Australia, or messages are read in Australia.[104] It is also stated that the Act applies to jurisdictions outside of Australia.[105] While this provision would present enforcement difficulties in most instances, if somebody in violation of the Act were to subsequently go to Australia, they could then be prosecuted. Furthermore, this Act prevents Australians from engaging in spamming activities when outside of Australia. In other jurisdictions, details regarding a necessary link to the jurisdiction are not specified.

The Task Force on Spam recognized the need for international cooperation in the fight against spam. In implementing any new legislation, Canada can become a leader in international anti-spam efforts by following Australia's method of restricting all spamming activities with any Canadian connection. By providing protection to foreign recipients, Canada would be placed in a position where it could expect to receive reciprocal protection from foreign jurisdictions.

The next major issue to be determined is the connection to the spam activity necessary for one to be held liable. For example, in Australia, the *Spam Act 2003* holds any businesses associated with the spam activities liable[106] in order to prevent outsourcing to foreign jurisdictions. In other jurisdictions, only the senders are liable.

In Australia, the *Spam Act 2003* holds liable not only the senders, but those who aid, abet, counsel, procure, conspire to, or induce others to breach the Act.[107] Furthermore, a broad all-encompassing provision makes anybody knowingly involved in a violation, whether directly or indirectly, liable.[108] Thus, senders, those instructing senders, and even

---

[102] *Spam Act 2003*, *supra* note 29, ss. 7 & 16.
[103] *Ibid.*
[104] *Ibid.*, s.7.
[105] *Ibid.*, s.14.
[106] *Ibid.*, s.16(9).
[107] *Ibid.*
[108] *Ibid.*

those providing support facilities, knowing that their facilities will be used to breach the Act (this particularly applies to Internet Service Providers), are liable. Broad reaching provisions ensure that offshore operations are unable to shield spammers from liability, as the Act allows a large number of people connected to the spamming activity to be held liable.

While legislation in the United States exempts ISPs from liability,[109] it is the opinion of the author that holding ISPs to a certain standard of responsibility is absolutely necessary in order to ensure cooperation in the fight against spam. As the *CAN-SPAM Act* allows ISPs a special right of action,[110] it seems to characterize ISPs as victims. While this is true to an extent, ISP services are used in the sending of spam e-mails as well.[111] Thus, they are in the best position to conduct investigations based on patterns of use regarding their services. Accordingly, they should bear a portion of the responsibility in stopping spam.

Effective legislation should deter anybody within the Canadian jurisdiction from engaging in, encouraging, or supporting spam activities. The Task Force on Spam recognized this in their recommendation that third-party beneficiaries of spam be held liable.[112] Thus, an approach similar to that in Australia, with a broad reaching provision to hold anybody knowingly involved liable, is the correct one. Such an approach would deter businesses from outsourcing advertising activities to spammers, it would make the business of spamming more difficult, as Canadian support facilities would become unavailable, and it would encourage ISPs to be more aggressive in sanctioning known abuses (i.e. spamming) of their Internet service agreements.

While it could be argued that a "knowingly involved" approach might encourage ignorance, prominent educational campaigns could rebut any such claims. The knowingly involved approach should, in fact, encourage independent investigations by stakeholders who face potential liability, where they have any suspicions of being involved in spam activities.

A supplementary clause providing certain investigative requirements, perhaps arising from certain bandwidth usage patterns, would be helpful in increasing the actual knowledge that ISPs have about spam activities. In the report of the Task Force on Spam, it was suggested that a multifaceted approach requiring cooperation from various parties was needed.[113] By holding ISPs accountable for activities

---

109 Industry Canada, *supra* note 91.
110 *Ibid.*
111 FTC, *supra* note 8 at 4.
112 Task Force on Spam, *supra* note 3 at 15.
113 *Ibid.* at 3.

that they know occur through their service, this multifaceted approach is fostered.

3. What should the penalties be and who will enforce them?

a. Penalties

The obvious penalty for a breach of spamming restrictions is a fine, as businesses generally spam in an attempt to increase profits. The risk of fines neutralizes the potential profit that can be made by spamming and thus, fines should act as an adequate deterrent. Furthermore, statutory powers to fine can easily be given to administrative agencies, whereas most other penalties are reserved for the courts to apply.

In the United States, the *CAN-SPAM Act* imposes fines of up to $250 per e-mail received in breach of the Act, to a maximum of $2,000,000.[114] The difficulty with such a per-recipient scheme may be determining the number of e-mail recipients, however. Requiring proof of each receipt would be onerous on the enforcing body. Thus, a better approach would be a more contextual one, considering the number of recipients where ascertainable.

In determining the amount of the fines, policy dictates that harsher fines are superior, as large pecuniary penalties act as better deterrents than smaller penalties. Furthermore, with heavier fines, greater revenue from spam fines can be generated and ultimately used to finance anti-spam enforcement.

An injunction is another remedy that can be used to fight spam. However, an injunction alone is insufficient as a remedy, as the injunction of one spammer's activities does little to protect spam recipients. Without pecuniary penalties, spammers would face no real adverse consequences resulting from their spam activities.

Imprisonment, while an option under Australian and American legislation, is an inappropriate penalty in Canada. The prison system is generally intended for public safety and rehabilitation—deterrence has recently taken a back seat to these other purposes of incarceration.[115] Incarceration is seen as a last resort, where adequate, less restrictive measures are unavailable.[116] Accordingly, incarceration is an inappropriate punishment in the case of spam law violations, where

---

[114] *CAN-SPAM Act*, *supra* note 28, s.7(f)(3).

[115] See Department of Justice, "Fair and Effective Sentencing—A Canadian Approach to Sentencing Policy" (October 2005), online: Department of Justice Canada <http://www.justice.gc.ca/en/news/nr/2005/doc_31690.html>.

[116] *Ibid.*

fraud and malice are lacking. Furthermore, as this paper recommends keeping the enforcement of anti-spam legislation out of the courts as much as possible, incarceration becomes an even less attractive option for jurisdictional reasons, as administrative bodies generally lack the power to incarcerate.

b. Supervision and Enforcement

As stated earlier, legislation prohibiting spam is useless without a proper mechanism to monitor certain Internet activities and catch spammers. Who then, should monitor spam activity and enforce spam restrictions? Should it be up to private individuals to complain? Should private rights of action even be available? Should spam legislation be fused with the criminal law, so that it is enforced through Crown prosecutors? Would it be most appropriate to use an existing regulatory body or perhaps to create a regulatory body to monitor the Internet including spam activity, with statutory powers to hold hearings and impose fines?

It seems that relying on individual complainants, the police, and the public courts to prosecute would not be an effective way of combating spam. Firstly, as evidenced by the UK small claims case of *Roberts v. Media Logistics (UK) Ltd.*, the compensation available to private individuals is negligible, such that it is not worth going after spammers in civil suits, except for in principle.[117] In using the criminal law system, the police, who usually compile evidence for the Crown and initiate most prosecutions, cannot be relied on to investigate spamming activities, as they lack the expertise, they face jurisdictional boundary problems making investigations practically unfeasible, and they have more pressing priorities regarding public safety. Without the police in the picture, an independent regulatory body would still be necessary just to conduct investigations for criminal prosecutors.

In the United States, spam laws are generally enforced by the Federal Trade Commission. However, when parties that are already regulated by various other agencies are involved, the existing regulating bodies take responsibility.[118] For example, the Office of the Comptroller of the Currency monitors the activity of national banks and accordingly would be responsible for ensuring that national banks comply with spam provisions.[119] The advantage of having these independent regulatory bodies deal with the problem of spam is that they are already engaged in supervisory roles.

---

[117] Spamhaus News, *supra* note 71.
[118] *CAN-SPAM Act*, *supra* note 28, ss. 7(b) & (f).
[119] *Ibid.*

By assigning spam enforcement to numerous existing agencies with other mandates, however, spam monitoring takes a back seat to other tasks and, in many instances, resources necessary to be effective are unavailable. Recipients of spam would not know where to file complaints and most agencies would lack the expertise necessary to conduct thorough investigations. Furthermore, even if a spammer was caught and found by the regulatory body to have engaged in illegal spam activities, the available sanctions might not be appropriate. Removal or suspension of a license might be too strict a sanction and the proceeds of any fines would likely be directed towards something other than fighting spam.

In Australia and the United Kingdom, a single regulatory agency takes responsibility for enforcing spam legislation. In Australia, it is the Australian Communications Authority ("ACA") that enforces spam laws. The ACA has powers to investigate, levy fines, and impose various other penalties. In the United Kingdom, it is the Information Commissioner's Office that is responsible for enforcing spam laws.[120]

Utilizing independent regulatory agencies, with Crown prosecutors only taking part in serious violations and enforcing rulings made by the regulatory agencies, appears to be the common approach in other jurisdictions. It is also, in the author's opinion, the best approach for Canada. Enforcement through an independent regulatory body is ideal because such a body is best able to accumulate expertise and thus, provide better investigatory functions while maintaining the statutory powers to impose fines. Such a body, unlike the courts, would have the freedom to work closely with ISPs, e-mail service providers, and foreign agencies responsible for combating spam. Joint international efforts would significantly increase the success of investigations, as the integration of known spammer databases and "spam boxes"[121] would make locating and prosecuting spammers much easier. This is precisely the international effort that was envisioned by the Task Force on Spam and that is being pursued through the *London Action Plan*. Furthermore, an independent regulatory body could exercise functions beyond mere investigations, hearings, and punishments. It could engage in awareness and educational campaigns and it could assist businesses in setting up certain practices to help combat spam. Such a coordinating body was envisioned by the Task Force on Spam in their *Stopping Spam* report.[122]

---

[120] Industry Canada, *supra* note 91.

[121] In France, the National Data Processing and Liberties Commission is responsible for enforcing spam. In fulfilling its mandate, it compiles evidence against spammers in a national spam box in order to prepare for legal action. See *ibid.*

[122] Task Force on Spam, *supra* note 3 at 13.

While this paper does not focus on the technological logistics of catching spammers, it is clear that any tracing of e-mails or supervision of ISPs and e-mail service providers demands special technologies and expertise. A single regulatory body, as opposed to various Crown prosecutors across numerous jurisdictions, is best able to establish working relationships with e-mail service providers to implement a system whereby spamming activities can be reported with ease. Google Mail[123] currently gives users a "Report Spam" option, in addition to the simple delete command. By integrating such "Report Spam" options with the proper anti-spam enforcement authorities, spammers are more likely to be located and brought to justice.

The next question, then, is whether there currently exists a Canadian regulatory body capable of enforcing spam provisions. In Canada, there are three agencies with mandates relevant to fighting spam: the Competition Bureau, the Office of the Privacy Commissioner of Canada, and Industry Canada.[124]

The Competition Bureau "promotes and maintains fair competition so that Canadians can benefit from competitive prices, product choice and quality services."[125] This mandate does not generally deal with the marketing practices of businesses and thus, is too far removed from the issue of spam regulation to have the Competition Bureau as an effective regulator.

The mandate of the Office of the Privacy Commissioner of Canada ("OPC"), on the other hand, is "to protect and promote the privacy rights of individuals."[126] The Privacy Commissioner is thus responsible for enforcing the *Privacy Act* and *PIPEDA*. As discussed above, *PIPEDA* is currently the best legislative protection against spam available and thus, it can be said that the Privacy Commissioner's mandate is sufficiently related to the issues raised by spam. If protection against spam can be considered a privacy right, the expansion of this mandate to protect businesses as well as individuals would allow the OPC to deal with combating spam.

---

123 Gmail, "About Gmail", online: Gmail <http://mail.google.com/mail/help/intl/en/about.html#spam>.

124 See Industry Canada, *supra* note 91.

125 Competition Bureau Canada, "Competition Bureau", online: Competition Bureau Canada <http://www.competitionbureau.gc.ca/internet/index.cfm?lg=e>.

126 Office of the Privacy Commissioner of Canada, "About Us", online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/aboutUs/index_e.asp>.

Industry Canada's Task Force on Spam proposed the creation of a Canadian Anti-Spam Action Centre.[127] It was proposed that this agency could promote national and international anti-spam coordination, provide educational campaigns, receive complaints, maintain a spam database, acquire the expertise needed to investigate spam, and coordinate the sharing of information.[128] The Task Force on Spam in its proposal also recognized the cost-savings that could be realized by utilizing an existing government agency to run its proposed Canadian Anti-Spam Action Centre. Their recommendation was that this agency be Industry Canada.[129]

Industry Canada's mandate is "to help make Canadians more productive and competitive in the knowledge-based economy, thus improving the standard of living and quality of life in Canada."[130] This is a highly broad mandate, which could also encompass combating spam. However, the Office of the Privacy Commissioner is a more attractive option because with a minor adjustment, its mandate could be highly specific in combating spam. Additionally, the OPC has already had experience in addressing cases of spam where *PIPEDA* provisions applied.[131] Like Industry Canada, the OPC has also been involved with the *London Action Plan*, and thus has the necessary relationships to keep Canada involved in international anti-spam efforts. With this existing experience, a more specific mandate, and fewer responsibilities elsewhere, administering an anti-spam operation would likely be easier in the OPC.

Accordingly, Parliament should extend the mandate of the OPC to include the enforcement of spam laws and, therefore, the protection of privacy of both individuals and businesses. The OPC should also be responsible for the educational component envisioned by the Task Force on Spam.[132] Moreover, the OPC should be responsible for assigning fines and damage awards, based on private rights of action from individuals and businesses. While awards comparable to those granted in the United States may not be available, the availability of some private recourse and the presence of some individuals like Nigel Roberts who may continue to complain based on principle still could go further to reduce the appeal of

---

127 Task Force on Spam, "Proposal for the Canadian Anti-Spam Action Centre" (May 2005), online: Industry Canada <http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/vwapj/Action%20Centre.pdf/$file/Action%20Centre.pdf>.

128 Industry Canada, "Proposal for the Canadian Anti-Spam Action Centre", online: Industry Canada <http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00338e.html>.

129 *Ibid.*

130 Industry Canada, "Mandate", online: Industry Canada <http://www.ic.gc.ca/cmb/welcomeic.nsf/ICPages/Mandate>.

131 See *PIPEDA* Case Summary #297, *supra* note 46.

132 Task Force on Spam, *supra* note 3 at 5.

engaging in spam activities. Furthermore, as more individuals come forward and complain, the knowledge base regarding known spammers will increase and subsequent prosecutions and private actions may become easier.

CONCLUSION

SPAM RATES CONTINUE TO RISE and this presents a significant impediment to the growth of e-commerce. It is clear that existing methods of spam enforcement in Canada, such as market forces, privacy laws, tort law, and the criminal law, are inadequate. While there are better solutions available at the international level, Canada must first take care of matters within its own borders before it can expect any cooperation from foreign jurisdictions.

There is some hope for international cooperation in combating spam, however, as jurisdictions such as the United Kingdom, the United States, and Australia, among others, have recognized spam as a problem and have responded by implementing legislation. Cross-border regulations in the EU have even gone so far as to include anti-spam provisions, while enforcement agencies around the globe have banded together through the *London Action Plan*. It seems that there is indeed a movement, albeit quiet and slow, towards an international effort in combating spam. As other nations have led the way in this fight, it is now time for Canada to demonstrate its commitment to this cause through legislative action, the necessary first step.

Unfortunately, spam still takes a back seat to hotter topics in today's legislative agenda, while inboxes continue to be relentlessly flooded with unwanted, unsolicited commercial e-mails. As Canadian society becomes increasingly dependent on the Internet as a way of life, the appeal of spam as a marketing strategy increases, and spam rates continue to rise, creating many problems. Hopefully, this issue will attract the attention of Parliament soon and we will see legislation that will decrease productivity losses suffered by Canadian businesses, generate respect from the international community, and create a more enjoyable Internet experience for both Canadians and Internet users across the globe.