

Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet

Karen Ng*

EMAIL HAS EMERGED AS A HIGHLY popular means of communication in Canada and around the world, allowing individuals and businesses to transmit information to recipients anywhere and at very little expense. However, the inexpensive and ubiquitous nature of email is being exploited by "spammers," who seek to profit from mass mailings of incredible volumes of unsolicited emails. Once merely an annoyance, the problem of spamming has grown into a substantial commercial and social concern. Many countries have enacted legislation directed specifically at the issue of spamming, although Canada has only recently begun to seriously consider this option in detail. This paper begins by reviewing the rise and nature of spam along with its associated costs and problems. It then reviews various options others have considered to control spam. It is expected that Canada would consider these options as it enters its own dialogue in deciding whether to enact spam-specific legislation. The prospect of future Canadian spam legislation raises two important constitutional considerations: (1) which level of Canadian government (federal or provincial/territorial) is legislatively competent to regulate the problem of unsolicited email communications; and (2) whether any effective spam legislation can be proposed which is also likely to survive scrutiny under subsection 2(b) of the *Charter*. This paper concludes that Canada's Parliament is competent to enact legislation targeting the unsolicited nature of spam, and that spam legislation can be effective while also surviving *Charter* scrutiny as a section 1 demonstrably justified limitation upon the section 2(b) *Charter* rights of spammers.

LE COURRIER ÉLECTRONIQUE est devenu un moyen de communication très à la mode au Canada et partout dans le monde. Il permet aux individus et aux entreprises de transmettre des renseignements à des destinataires, peu importe où ils se trouvent et à peu de frais. En raison même de son caractère économique et ubiquiste, toutefois, les polluposteurs l'exploitent en cherchant à profiter du publipostage d'un volume incroyable de messages non sollicités. De simple désagrément initialement, le problème du publipostage est devenu une préoccupation commerciale et sociale importante. Un bon nombre de pays ont adopté des lois régissant la question, mais le Canada commence à peine à donner mûre réflexion à cette option. Cet article décrit d'abord le publipostage, son évolution ainsi que les coûts et les problèmes qu'il entraîne. Il fait ensuite un survol des diverses solutions envisagées par d'autres afin de contrôler le publipostage. Il est probable que le Canada les examinera au moment d'entreprendre son propre débat afin de décider s'il y a lieu ou non de légiférer directement en la matière. La possibilité que le Canada édicte une loi régissant le publipostage soulève deux questions constitutionnelles importantes : (1) quel palier de gouvernement au Canada (fédéral ou provincial/territorial) a la compétence pour légiférer en matière des communications électroniques non sollicitées et (2) sera-t-il possible de proposer une loi efficace en matière du publipostage qui résiste aux critères d'examen en vertu de l'alinéa 2 b) de la *Charte*. L'article conclut que le Parlement du Canada est compétent pour légiférer sur la question de la nature non sollicitée du publipostage et que la législation en la matière peut être efficace et résister aux critères d'examen en tant qu'une atteinte raisonnable aux droits des polluposteurs protégés par l'alinéa 2 b) de la *Charte* qui se justifie en vertu de l'article 1 de la *Charte*.

Copyright © 2005 by Karen Ng.

* BSc, LLB, LLM (Law & Technology), associate at Aird & Berlis LLP. The author wishes to thank Professor Michael Geist for his direction and comments, Kevin Sartorio for his editorial comments, and her family for their support.

- 449 1. INTRODUCTION
- 453 2. OVERVIEW OF THE RISE OF SPAM, ITS PROBLEMS AND ITS COSTS
- 453 2.1. *Defining the Problem: What is "Spam"?*
- 454 2.1.1. Lack of Consent
- 454 2.1.2. Volume
- 455 2.1.3. Indiscriminate
- 455 2.1.4. Content
- 455 2.2. *The Proliferation and Costs of Spam*
- 456 2.2.1. Reversal of Cost Burdens
- 457 2.2.2. Intrusiveness
- 457 2.2.3. Undermining User Confidence in the Internet
- 458 3. INDUSTRY CANADA'S SPAM POSITION PAPERS
- 458 3.1. *Canada's Position in 1997: Spam Legislation is Not Required*
- 458 3.1.1. Free Market Efficiency
- 459 3.1.2. Privacy Legislation
- 462 3.1.3. Private Actions
- 463 3.1.4. Criminal Law Enforcement
- 464 3.2. *Canada's Position in 2003: A Re-consideration*
- 464 3.3. *Canada's Position in 2004: Moving Forward*
- 465 4. SPAM REGULATION MODELS
- 466 4.1. *Regulating Consent*
- 466 4.1.1. Opt-In Models
- 466 4.1.2. Opt-Out Models
- 467 4.2. *Mandating Truth and Accuracy*
- 469 5. THE DIVISION OF POWERS
- 469 5.1. *Overview: The Concepts of "Pith and Substance" and "Concurrency"*
- 470 5.2. *Application to the Context of a Canadian Spam Law*
- 470 5.2.1. Overview
- 470 5.2.2. "Pith and Substance" Analysis
- 470 5.2.3. Selection of the Most Appropriate Head of Power
- 471 5.2.3.1. *The Provinces: Property and Civil Rights (Section 92.13)*
- 471 5.2.3.2. *Federal Heads of Power*
- 471 5.2.3.2.1. Trade and Commerce (Section 91.2)
- 472 5.2.3.2.2. Criminal Law (Section 91.27)
- 473 5.2.3.2.3. POGG (opening words to Section 91)
- 474 5.2.3.2.3.1. *What is a Matter of "National Concern"?*
- 475 5.2.3.2.4. Transportation and Communication (Subsection 92.10(a))
- 476 5.2.3.2.4.1. *The Facilities of Radio Communication*
- 476 5.2.3.2.4.2. *The Content of Radio Broadcasting*
- 477 5.2.3.2.4.3. *Extension to Broadcast Television*
- 477 5.2.3.2.4.4. *Extension to Telephone Communication*
- 478 5.2.3.3. *Conclusions*
- 479 6. SPAM LAWS AND SUBSECTION 2(b) OF THE CHARTER: A DEMONSTRABLY JUSTIFIED LIMITATION?
- 480 6.1. *Overview of Canada's Approach to Freedom of Expression*
- 481 6.2. *Is Spam a Form of Protected "Expression"?*
- 482 6.3. *Would Spam Legislation Violate Subsection 2(b)?*
- 482 6.4. *Analysis Under Section 1 of the Charter*
- 483 6.4.1. The Burden on the State
- 483 6.4.2. Pressing and Substantial Objective
- 485 6.4.3. Proportionality Analysis
- 485 6.4.3.1. *The "Rational Connection" Branch*
- 485 6.4.3.2. *The "Minimal Impairment" Branch*
- 486 6.4.3.2.1. Minimal Impairment Analysis Applied in the Context of Spam
- 487 6.4.3.2.2. Mandating Consent
- 488 6.4.3.3. *The "Overall Proportionality" Branch*
- 489 6.5. *Charter Summary*
- 490 7. CONCLUSIONS AND SUGGESTIONS FOR A MODEL CANADIAN LAW
- 490 7.1. *Model Law Checklist*
- 490 7.1.1. Constitutional Issues
- 491 7.1.2. Practical Issues

Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet

Karen Ng

The basic issue in this case is whether [the] respondents, in the exercise of asserted First Amendment rights, may distribute handbills on Lloyd's private property contrary to its wishes

[Although] ... the courts properly have shown a special solicitude for the guarantees of the First Amendment, this Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.

Powell J, writing for the majority of the US Supreme Court in *Lloyd Corporation, Ltd. v. Tanner*, 407 U.S. 551 at pp. 567-68 (1972).

1. INTRODUCTION

AS OUR WORLD CULTURE AND ECONOMIES become ever more dependent on novel and exciting advances in digital and online technologies, it is interesting to note that one of the earliest internet applications continues to be one of its most important. For hundreds of millions of people, electronic mail (email) functions as a critical means of communication.¹ However, the tremendous popularity and pervasiveness of email has spawned a new, profitable and problematic industry known as "spamming," which is also experiencing exponential growth.²

-
1. According to information provided by the International Data Corporation, there have been over 500 million individual email boxes in operation in the year 2000 and that number is expected to surpass 1.2 billion by 2005, see Michael Pastore, "More Mailboxes on the Way" *ClickZ Stats* (17 September 2001), <http://www.clickz.com/stats/sectors/software/article.php/1301_%20885551> [Pastore].
 2. See discussion in section 2.2 below. See also Mike Wendland, "Spam King Lives Large Off Others' E-mail Troubles" *The Detroit Free Press* (22 November 2002), <http://www.freep.com/money/tech/mwend22_20021122.htm>; Tim Lemke, "Spammers Make Profits Without Making a Sale" *The Washington Times* (4 August 2003), <<http://www.washtimes.com/business/20030803-110550-8329r.htm>>; Shar Van Boskirk, Charlene Li & Jennifer Parr, "Figure 7 - Forecast: U.S. Email Marketing Services, 2001 to 2006" *Effective Email Marketing Report* (August 2001), <<http://www.forrester.com/ER/Research/Figure/0,,17078,00.html>>.

"Spam" can be broadly understood as email, usually in the nature of a commercial solicitation, sent without recipient consent in a mass-mailing to many different people.³ The sheer volume of spam sent worldwide is staggering.⁴ In addition, a substantial portion of it originates from disreputable sources and contains content that is (at best) distasteful or (at worst) criminal in nature.⁵ There are few aspects of the internet that provoke the wrath of users as much as spam.⁶

The undesirability of spam has even caused some to argue for a re-thinking of the view that cyberspace should continue to be an open and self-regulating environment.⁷ Email users generally prefer to regulate each other's conduct through co-operative "netiquette" guidelines, shunning those who

Recently, a form of spam known as "phishing" has experienced rapid growth. Phishing occurs when email messages are sent to recipients, purportedly from an established and trusted company, containing webpage links directing them to websites that are designed to appear as though they are from a trusted service provider, financial institution or online merchant. Recipients are then asked to enter personal information such as their social security number, password or credit card information on these copycat websites. A recent 2004 study by Gartner shows that "phishing attacks" have spiked in the last year, during which time direct losses from identity theft fraud against these phishing victims cost US banks and credit card issuers about US\$1.2 billion. See "Gartner Study Finds Significant Increase in E-mail Phishing Attacks" *Gartner* (6 May 2004), <http://www3.gartner.com/press_releases/asset_71087_11.html>.

3. As will be reviewed, various definitions of spam are possible. The moniker "spam" is widely thought to have originated as a nod to a popular Monty Python skit, involving a café that served dishes based on the infamous Hormel Foods meat product. In the skit, the word "spam" was repeated ad-nausea, infuriating others in the café. See Credence E. Fogo, "The Postman Always Rings 4,000 Times: New Approaches to Curb Spam" (2000) 18 *John Marshall Journal of Computer & Information Law* 915 at p. 918.
4. See Industry Canada, "E-mail Marketing: Consumer Choices and Business Opportunities," (January 2003), <<http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00189e.html>> [2003 Spam Paper], which estimates that over 30 billion spam were sent in the year 2002 alone. See also Australia, National Office for the Information Economy, *Final Report of the NOIE Review of the Spam Problem and How It Can be Countered*, <http://www.dcit.gov.au/ie/publications/2003/04/spam_report> (Canberra: Department of Communications, Information Technology and the Arts, 2003) [NOIE Report]. On 2 December 2003, the Parliament of Australia passed the government's *Spam Bill 2003*. On 12 December 2003, the Parliament of Australia enacted the *Spam Act 2003*, (Cth.), <http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366> [Australia Spam Act 2003], banning the sending of unsolicited commercial emails. A 120-day grace period, after the Governor General's signature of the Bill, is given for businesses to adjust procedures to ensure compliance with the new law. By mid-April 2004, penalties of up to US\$1.1 million have been levied on the sending of illegal commercial spam.

More disturbing, the latest Brightmail survey indicated that spam accounted for 60% of all email in January 2004. See Brightmail's Press Release, "Impact of CAN-SPAM? Brightmail Finds Spam is Still Flowing" (2 February 2004), <<http://www.forrelease.com/D20040202/sfm067.P2.02022004032439.11877.html>> [Brightmail 2004].

5. See US, Federal Trade Commission, *False Claims in Spam: A Report by the FTC's Division of Marketing Practices* (Washington, DC: Federal Trade Commission, 30 April 2003), <<http://www.ftc.gov/reports/spam/030429spamreport.pdf>> [FTC Study]. The FTC Study found that 17% of the spam reviewed contained pornography and that two-thirds of the claims were false or fraudulent in some respect. But see MessageLabs's Press Release, "Inappropriate Email Image Attachments Declining" (7 September 2004), <<http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=1123®ion=>>>.
6. See generally Michael Geist, *Internet Law in Canada*, 2d ed. (North York, Ont.: Captus Press, Inc., 2001) [Geist, *Internet Law*] at p. 216. In a 1999 study conducted by Gartner Consulting, 83% of the 13,100 users surveyed responded with a negative reaction to spam. See Gartner Consulting, "ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition" (14 June 1999), <<http://www.terracetech.com/jp/data/ISPs%20&%20Spam.pdf>>.
7. See generally David A. Gottardo, "Commercialism and the Downfall of Internet Self Governance: An Application of Antitrust Law" (1997) 16 *John Marshall Journal of Computer & Information Law* 125; Jennifer Kappel, "Government Intervention on the Internet: Should the Federal Trade Commission Regulate Unsolicited E-mail Advertising?" (1999) 51 *Administrative Law Review* 1011; Ari Lanin, "Who Controls the Internet? States' Rights and the Reawakening of the Dormant Commerce Clause" (2000) 73 *Southern California Law Review*. 1423; Karen Mika, "Information v. Commercialization: The Internet and Unsolicited Electronic Mail" (1998) 4 *Richmond Journal of Law & Technology* 6, <<http://law.richmond.edu/jolt/v4i3/mika.html>>.

refuse to comply.⁸ However, voluntary rules of internet civility do not appear to dissuade spammers, who continue to perfect their ability to exploit the open nature of the internet.⁹

Internet Service Providers (ISPs) and consumers try to minimize the reception of spam with filtering software designed to reject email from disreputable sources.¹⁰ Spammers respond to such efforts by adopting increasingly sophisticated avoidance tactics. For example, they adapted to early filtering technologies by concealing their identity through practices such as "spoofing," which is the misappropriation of a legitimate entity's domain name.¹¹ Spammers can also "hijack" a legitimate computer server to "launder" their own email.¹² Both practices are intended to increase the likelihood that spam email will pass through software filters and be read by the end recipients.

The battle against spam involves more than just deploying filtering software. Various traditional legal solutions have also been pursued, but with

No single authority governs the internet and there are no cross-jurisdictional mechanisms in place to enforce "real world" laws that may apply to internet conduct. For most of its short history, the internet has been perceived as a self-regulating medium of communication and several authors have argued for a continuation of that regime. See John Perry Barlow, "A Declaration of the Independence of Cyberspace," (8 February 1996), <<http://www.eff.org/~barlow/Declaration-Final.html>>; Jason Kay, "Sexuality, Live Without a Net: Regulating Obscenity and Indecency On the Global Network" (1995) 4 Southern California Interdisciplinary Law Journal 355 at p. 387.

Spam-related issues and other problems caused by a maturing internet culture have given rise to the realization that governmental regulation is sometimes desirable. As noted by Professor Michael Geist, "governmental regulation of [the] Internet is actually becoming increasingly the rule, rather than the exception." See Michael Geist, "Tax Holiday Expiring, Regulators Aspiring on Web" *The Toronto Star* (30 June 2003), <http://www.michaelgeist.ca/resc/html_bkup/june302003.html>.

Indeed, as the quantity of spam increases, the libertarian cries of the internet are gradually being drowned out by increased demands to regulate, ban, censor or tax spam. More drastic proposals contemplate the restructuring of the internet as a whole. See "Redesigning the Net to Save It from Spam" *CNN.com* (17 March 2003), <<http://www.cnn.com/2003/TECH/internet/03/17/hauling.spam.ap/index.html>>.

8. See David E. Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail" (2001) 35 *University of San Francisco Law Review* 325, <<http://www.sorkin.org/articles/usf.pdf>> at pp. 341-344 [Sorkin].
9. See Mitch Wagner, "Spam May Overtake E-mail in 2003" *CNN.com* (12 December 2002), <<http://www.cnn.com/2002/TECH/biztech/12/12/techweb.email.swamp/>>. See also Brightmail 2004, *supra* note 4.
10. Filtering techniques include black/whitelists, peer-to-peer spam identification and heuristic analysis to profile incoming email. There have been other private efforts by users to control spamming such as demanding that spammers stop sending unsolicited emails, and using vigilante techniques such as flaming and mail bombings. Flaming is sending hateful response messages to the unsolicited emailer. Mail bombing is a retaliatory act that involves sending mass messages to one user. For a thorough discussion, see Andrew Conry-Murray, "Fighting the Spam Monster and Winning" *Network Magazine* (4 April 2003), <<http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703510>>.
11. See David Ho, "Feds warn of e-mail con artists" *The Detroit News* (21 July 2003), <<http://www.detroitnews.com/2003/technology/0307/22/technology-224431.htm>> . See also Robert Lemos, "Analyst: Crime Pays For Identity Thieves" *CNET News.com* (21 July 2003), <http://news.com.com/Analyst+Crime+pays+for+identity+thieves/2100-1009_3-5050295.html>. The fight against spam has traditionally been waged by ISPs and only recently has there been corporate activity. See *Earthlink, Inc. v. Carmack*, 2003 U.S. Dist. LEXIS 9963 (ND Ga 2003) [*Earthlink v. Carmack*]; *America Online Inc. v. IMS*, 24 F.Supp. 2d 548 (ED Va 1998), <<http://lw.bna.com/lw/19981117/0011.htm>> [*AOL v. IMS*]; *America Online, Inc. v. LCGM*, 46 F.Supp. 2d 444 (ED Va 1998) [*AOL v. LCGM*]. See also Microsoft's Press Release, "America Online, Earthlink, Microsoft and Yahoo! Team Up to File First Major Industry Lawsuits under New Federal Anti-Spam Law" (10 March 2004), <<http://www.microsoft.com/presspass/press/2004/mar04/03-10CANSPAMpr.asp>>.
12. See Saul Hansell, "E-mail's Backdoor Open to Spammers" " *The New York Times* (20 May 2003) A1.

only varying degrees of success.¹³ Internationally, several jurisdictions (including the United States, the European Union, Australia, Korea, New Zealand and Japan) have either passed or are considering stand-alone spam legislation to tackle the problem.¹⁴ In a paper circulated in 1997, Industry Canada took the initial position that anti-spam legislation was unnecessary.¹⁵ Six years later, a second paper was released with comments that suggest Canada may be rethinking this position.¹⁶ However, to date, no spam-specific legislation has been tabled by any of the provinces or the federal government.

Against this background, this article begins by providing an overview of the rise of spam, as well as of some of its problems and costs. It then reviews Industry Canada's initial suggestions for non-legislative options to deal with spam, and the criticisms of those suggestions which appear to have led to a modification of Canada's stance. Next, various models of spam regulation under consideration in other countries are discussed, before looking more closely at the situation in Canada.

At the heart of this article is a consideration of two important constitutional questions that are raised by the prospect of future Canadian spam legislation:

First, which of the federal and provincial levels of government are legislatively competent under the *Constitution Act, 1867*¹⁷ to regulate the problem of unsolicited email?

Second, given that the purpose of any Canadian spam law would be to restrict email communications under some circumstances, can an effective regulatory model be proposed that is also constitutionally valid, having regard to the concept of freedom of expression enshrined in subsection 2(b) of the *Charter of Rights and Freedoms*?¹⁸

Finally, key elements of a model Canadian spam law are suggested at the conclusion of this article in light of the totality of issues discussed.

13. As reviewed later in this paper, spamming may give rise to potential liability under various heads of tort, contract or trespass. See, for example, the early junk mail case of *Allan Mather v. Columbia House*, an unreported Ontario Court (General Division) case decided on 6 August 1992, in which Columbia House was held liable for trespass in an action (in contract) that was brought against it by Mather. Mather had repeatedly requested Columbia House to be removed from the mailing list. The Ontario Court awarded Mather general and punitive damages. Depending on the context, various criminal and quasi-criminal regulations may also apply. See parts 3.1.3 and 3.1.4, below. See also Geist, *Internet Law*, *supra* note 6 at c. 9.
14. See discussion in Part 4 below.
15. Industry Canada, "Internet and Bulk Unsolicited Electronic Mail" (July 1997), <[http://strategis.ic.gc.ca/epic/internet/incec-ceac.nsf/vwapj/SPAM_1997En.pdf/\\$FILE/SPAM_1997En.pdf](http://strategis.ic.gc.ca/epic/internet/incec-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf)> [1997 Spam Paper].
16. 2003 Spam Paper, *supra* note 4. To date, at least two Private Member's Bills have been introduced in Parliament (in 2003): Bill S-23, <http://www.parl.gc.ca/37/2/parlbus/chambus/senate/bills/public/pdf/s-23_1.pdf> (which, among other things, contemplated setting up a "do not spam" list); and Bill C-460 <http://www.parl.gc.ca/PDF/37/2/parlbus/chambus/house/bills/private/c-460_1.pdf> (which suggested amendments to the *Criminal Code* to make spamming a criminal offence. Both bills later died on the order paper when Parliament was prorogued.
17. U.K., 30 & 31 Victoria, c. 3, reprinted in R.S.C. 1985, App. II, No. 5, <http://laws.justice.gc.ca/en/const/c1867_e.html#pre> [Constitution].
18. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, <http://laws.justice.gc.ca/en/const/annex_e.html#l1> [Charter].

★

2. OVERVIEW OF THE RISE OF SPAM, ITS PROBLEMS AND ITS COSTS

2.1. Defining the Problem: What is "Spam"?

ONE DIFFICULTY IN CONFRONTING the problem of spam is the fact that there is far from universal consensus as to how it should be defined. For example, some take the position that it should include all unsolicited email, regardless of content.¹⁹ Others define the problem more narrowly and would focus only on unsolicited commercial emails or those which contain unsavoury content.²⁰

In 2003, the Global Business Dialogue on Electronic Commerce provided a more comprehensive definition of spam as "electronic communication via any means that includes any or all of the following: absence of consent to receive either via opt-out or opt-in principles; harvesting of personal information; false information or claims including 'subject' and 'from' lines, as well as content; intent to defraud; or erroneous reply address information."²¹

It is these common characteristics of spam that legislatures will want to consider when drafting legislation targeting these communications. However, for every approach taken it seems that many additional questions can arise.

19. See e.g. *NOIE Report*, *supra* note 4.

20. See e.g. US, Bill S. 1052, *Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003*, 108th Cong., 2003, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s1052is.txt.pdf> [Bill S. 1052]; US, Bill S. 877, *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 or the CAN-SPAM Act of 2003*, 108th Cong., 2003, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s877is.txt.pdf>; US, Bill H.R. 2472, *Protect Children from E-mail Smut Act of 2001*, 107th Cong., 2001 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h2472ih.txt.pdf>.

Note that on 16 December 2003, President George W. Bush signed the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003* into law, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s877enr.txt.pdf> [CAN-SPAM Act]. Congress made several determinations of public policy under the CAN-SPAM Act:

- (1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;
- (2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and
- (3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

The law allows for statutory damages of US\$2 million for violations, tripled to US\$6 million for intentional violations, and unlimited damages for fraud and abuse. The law does not make the sending of spam illegal *per se*; rather, the Act sets limits on the sending of spam (i.e. knowingly sending commercial emails with the intention of deceiving or misleading recipients as to the origin of the email(s), materially falsifying header information in emails, create deceptive subject headings, or neglect to include identifiable marks or notices that an email contains sexually oriented materials, etc.). As Canada has yet to pass spam legislation, this paper will also consider relevant bills that were previously before the US Congress before the passing of the CAN-SPAM Act.

21. Global Business Dialogue on Electronic Commerce, "Building Consumer Trust: Unsolicited Electronic Communications (Spam) a Multilateral Framework" (November 2003), <<http://www.gbde.org/pdf/recommendations/spam03.pdf>>.

2.1.1. Lack of Consent

Fundamental to most notions of spam is a failure to secure an appropriate degree of recipient consent before an email is sent.²² Stakeholders have differing opinions as to what level of recipient consent ought to be required. Some argue that any email sent without express prior consent should be prohibited. However, this approach neglects the fact that most people engage in harmless exchanges of unsolicited email on a regular basis. For example, most of us have forwarded pictures, jokes or other messages to an extended circle of acquaintances, many of whom (if we had asked them) might not have opted to receive that communication.

The existence of a prior personal relationship between sender and recipient may be sufficient to presume that an element of consent exists, but should the same presumption exist for corporations that want to send emails to existing customers? Does it matter how the recipient's email address was obtained? Should everyone, people and corporations, be required to include in their emails a clear opportunity for recipients to "opt-out" of future emails?²³

2.1.2. Volume

Since the sending of email is essentially free, spammers are able to send the same email to a massive number of recipients without incurring substantial costs.²⁴ One may therefore consider addressing spam by targeting emails sent to a large number of recipients. However, what about an email sent to a large group of people who share a common interest? What about an organization that wishes to send out a mass holiday greeting to its customers? What about a fringe political candidate who wants to solicit email support from visitors to his or her website?²⁵ Could a spammer not circumvent any volume restriction simply by sending its emails in multiple small batches rather than a single large mailing?

-
22. This aspect of spam contravenes widely-adopted guidelines for electronic commerce. For instance, the Canadian framework for consumer protection in electronic commerce states that, "[v]endors should not transmit commercial E-mail without the consent of consumers, or unless a vendor has an existing relationship with a consumer." See Industry Canada, "Principles of Consumer Protection for Electronic Commerce: A Canadian Framework" (August 1999) at Principle 7, <<http://strategis.ic.gc.ca/pics/ca/principlese.pdf>> [Canadian Consumer Protection Principles]. See also US, Bill H.R. 3113, *Unsolicited Commercial Electronic Mail Act of 2000*, 106th Cong., 2000, s. 3(10)(A)(i) <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:h3113rfs.txt.pdf>; "British Code of Advertising, Sales Promotion and Direct Marketing," (4 March 2003) at cl. 43.4(c), <http://www.asa.org.uk/asa/codes/cap_code/ShowCode.htm?clause_id=1688>.
23. These and various other issues give rise to privacy concerns addressed later in this paper. See Part 3.1.2 below. See also Ian Ayres & Matthew Funk, "Marketing Privacy: A Solution for the Blight of Telemarketing (and Spam and Junk Mail)" (2003) 20 *Yale Journal on Regulation* 77, <<http://islandia.law.yale.edu/ayers/mprivacy.pdf>>; Eric J. Sinrod & Barak D. Jolish, "Controlling Chaos: The Emerging Law of Privacy and Speech in Cyberspace" (1999) *Stanford Technology Law Review* 1, <http://stlr.stanford.edu/STLR/Articles/99_STLR_1/article_pdf.pdf>; Ethan Preston, "Finding Fences in Cyberspace: Privacy and Open Access on the Internet" (2000) 6.1 *Journal of Technology Law & Policy* 3, <<http://grove.ufl.edu/~techlaw/vol6/issue1/preston.html>>; Jeff Sovern, "Protecting Privacy with Deceptive Trade Practices Legislation" (2001) 69 *Fordham Law Review* 1305.
24. Minimal operating costs include obtaining access to the internet and the time spent acquiring recipient addresses. See also discussion in Part 2.2 below.
25. As discussed in Part 6.4 below, the constitutionality of a spam law may depend on the breadth of its application, and on the balancing of competing interests such as protecting freedom of expression, e.g. political speech.

2.1.3. Indiscriminate

Spammers have a simple goal: to reach as many different people as possible.²⁶ They play a numbers game, knowing that a percentage of their recipients will read and respond to their email. As spammers experience little or no increased cost for adding recipients, they have no incentive to spend time or money targeting their messages to a focussed customer demographic.²⁷

2.1.4. Content

Finally, what role should the issue of content play in the spam debate? Should legislative measures be directed at any unsolicited electronic message regardless of content, or should only commercial emails be targeted? Should they be even more limited, and prohibit only emails that include false or misleading information or claims? This is a divisive issue and approaches seem to vary among countries.²⁸

2.2. The Proliferation and Costs of Spam

Statistics used to estimate the proliferation of spam speak to the gravity of the current situation. Various studies in the early 2000s estimated that junk email then accounted for between 30 percent to 50 percent of total internet traffic, and the problem has shown no sign of deceleration. In fact, the most recent studies indicate that the problem of spam is accelerating.²⁹ The practice has

26. Sorkin, *supra* note 8.

27. *Ibid.*

28. The European Union has taken the position that spam should be defined narrowly as an unsolicited commercial communication. See Etienne Drouard & Serge Gauthronet, *Unsolicited Commercial Communications and Data Protection* (Commission of the European Communities, 2001), <europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/spamstudy_en.pdf> at p. 98 [European Study]. See also EC, *Council Directive 2002/58/EC 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, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf> [European Directive]. On the other hand, Australia appears to be prepared to define spam more broadly as any unsolicited electronic message, regardless of content (*NOIE Report, supra* note 4). See also *Australia Spam Act 2003, supra* note 4. Prior to the passing of the CAN-SPAM Act, there were different definitions of spam in the US. Compare US, Bill S. 563, *Computer Owners' Bill of Rights*, 108th Cong., 2003 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s563is.txt.pdf>, and US, Bill S. 1052, *supra* note 20. The CAN-SPAM Act covers any "commercial electronic mail message" which is defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."

Finally, Finland, Germany and Italy all have laws prohibiting unsolicited commercial email, while Austria prohibits unsolicited email without regard to content. See EuroCAUCE, *Finland* <http://www.euro.cauce.org/en/countries/c_fi.html>; EuroCAUCE, *Germany* <http://www.euro.cauce.org/en/countries/c_de.html>; EuroCAUCE, *Italy* <http://www.euro.cauce.org/en/countries/c_it.html>; EuroCAUCE, *Austria* <http://www.euro.cauce.org/en/countries/c_at.html>.

29. See European Study, *ibid.*; "Brightmail Alerts about Spam Spike During Holidays: Anti-Spam Technology Leader's Predictions Confirmed" (23 December 2002), <http://web.archive.org/web/20040807180708/http://www.brightmail.com/pressreleases/122302_holiday_spam_alert.html >. It has also been estimated that within the next few months over 50% of global email traffic will be spam. See "European Commission Goes on the Offensive Against Internet 'Spam'" *Clari News* (15 July 2003), <http://quickstart.clari.net/qs_se/webnews/wed/di/Queu-internet-spam.Rwhp_DIF.html>. Such predictions certainly appear to be accurate. See *Brightmail 2004, supra* note 4.

become so lucrative that companies have been formed dedicated solely to distributing email solicitations on behalf of other entities.³⁰

The total financial harm caused by spam is substantial,³¹ and spam opponents raise several arguments to explain why it is a problem.³²

2.2.1. Reversal of Cost Burdens

Spammers are able to target large numbers of recipients without incurring substantial costs.³³ Spam recipients, on the other hand, have to waste productive time and effort repeatedly accessing, reviewing and discarding these emails. This wasted effort particularly affects those who pay for internet access based on the minutes of time spent online.³⁴ Further, some wireless internet access devices charge subscriber fees based upon the amount of data that is downloaded.³⁵ Therefore, users of such devices actually pay each time they receive unwanted spam.

An avalanche of spam (particularly if high quality graphics are included) will also degrade the efficiency of an ISP's computer network and email service.³⁶ ISPs are, therefore, forced to increase bandwidth and storage space and fund increased security and filtering measures to remain competitive in the marketplace.³⁷

-
30. See e.g. Ad-Up, <www.ad-up.com/adup_services_linked.html>; Multimedia, <www.masresults.com>. Attempts to recover damages in these circumstances have been relatively unsuccessful. *Seidl v. Greentree Mortgage Co.*, 30 F.Supp. 2d 1292 (D Colo 1998). The Australia Spam Act 2003, *supra* note 4, s. 8, appears to target (or at least attempt to discourage) organizations from retaining someone else to send electronic messages by attributing liability to the organization. Section 5 of the Australia Spam Act 2003 defines an electronic message as being a message that is sent using an internet carriage service (or any other listed carriage service) to an electronic address (which includes email addresses and telephone numbers) in connection with an email account, an instant messaging account, a telephone account, or a similar account.
31. It has been estimated that total spam costs to internet users exceed 10 billion Euros a year (European Study, *supra* note 28). Another study found that the cost of spam to US corporate organizations in 2003 alone surpassed US\$10 billion. See Marten Nelson, (March 2003), Ferris Research <<http://www.ferris.com>> [subscription required]. The infamous Nigerian financial scam operation alone is estimated to gross more than US\$2 billion in 2003 See Wagner, *supra* note 9. According to another report, costs to US businesses as a result of spam amount to between US\$10 and US\$87 billion each year in lost productivity and associated expenses. See United States Telecom Association, "Unsolicited Commercial Email—SPAM," <http://www.usta.org/index.php?urh=home.advocacy.industry_issues.ii_spam>.
32. See e.g. Geist, *Internet Law*, *supra* note 6 at p. 177.
33. In contrast, junk mail advertisers or telemarketers must pay for each flyer mailed or each telephone call placed.
34. Michael Geist, "Time to Hit Delete Key on Weak Spam Policy" *The Globe and Mail* (30 May 2003), <http://www.michaelgeist.ca/resc/html_bkup/may302002.html>.
35. For example, the Blackberry device by Research in Motion, <<http://www.rim.net>>.
36. Cindy M. Rice, "The TCPA: A Justification for the Prohibition of Spam in 2002?" (2002) 3 North Carolina Journal of Law & Technology 375, <<http://www.jolt.unc.edu/vol3/Rice-V312.htm>> at p. 382. In 2003, America Online estimated that it blocked more than 2 billion spam *per day*, and that approximately 70% of incoming email were spam. See "Experts Warn Spam Could Ruin E-mail" *CNN.com*, <<http://web.archive.org/web/20030502041845/http://www.cnn.com/2003/TECH/internet/05/01/spam.alert.reut/index.html>> [America Online, *Experts Warn*].
37. Rice, *ibid*. Viruses that infiltrate network systems can also be introduced through unsolicited email. See US, Bill H.R. 2214, *Reduction in Distribution of Spam Act of 2003*, 108th Cong., 2003 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2214ih.txt.pdf>, which recognized that unsolicited commercial email posed network security risks to business and governments because of the introduction of viruses and malicious code delivered via unsolicited commercial email.

2.2.2. Intrusiveness

We have grown accustomed to sorting, once a day, the paper junk mail flyers received in our physical mailboxes. In contrast, internet spam messages are received continuously in our electronic inboxes,³⁸ and must frequently be accessed, read and deleted.³⁹ It is the intrusiveness of spam that may lead to its prohibition.⁴⁰

2.2.3. Undermining User Confidence in the Internet

A substantial percentage of spam contains questionable or even fraudulent content; for example, adult solicitations, pyramid and other schemes are common.⁴¹ To make matters worse, spammers routinely take steps to disguise the nature of their content by providing false or inaccurate subject line descriptions such as "Message from a Friend."⁴² On a larger scale, these and other practices work to undermine user confidence in the internet as a whole.⁴³

Bearing all of these costs and problems in mind, the following section of this article examines two papers released by Industry Canada outlining Canada's response regarding the problem of spam. The first paper was released in 1997 while the second, and much different paper, was released in 2003.

38. Geist, *Internet Law*, *supra* note 6 at p. 177.

39. *Olmstead v. United States*, 277 U.S. 438, <<http://www.justia.us/us/277/438/index.html>> at p. 478, 48 S. Ct. 564 (1928) [*Olmstead* cited to U.S.], Brandeis J dissenting. See also Bill S-21, *An Act to guarantee the human right to privacy*, 1st Sess., 37th Parl., 2001, cl. 2, <http://www.parl.gc.ca/37/1/parlbus/chambus/senate/bills/public/S-21/S-21_1/S-21_text-e.htm>, states the purpose as to give effect to certain principles, including: (a) privacy being essential to an individual's dignity, integrity, autonomy, well-being and freedom, and to the full and meaningful exercise of human rights and freedoms; (b) that there is a legal right to privacy; and (c) that an infringement of the right to privacy, to be lawful, must be justifiable. Additionally, Clause 3 recognizes that every individual has a right to privacy, including: (a) physical privacy; (b) freedom from surveillance; (c) freedom from monitoring or interception of their private communications; and (d) freedom from the collection, use and disclosure of their personal information.

40. *R. v. Dyment*, [1988] 2 S.C.R. 417, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol2/html/1988scr2_0417.html> [*Dyment*] where La Forest J stated at p. 427 that "[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, privacy is worthy of constitutional protection, but it also has profound significance for the public order."

41. See FTC Study, *supra* note 5. In a May 2003 study by Brightmail, roughly a quarter of spam email reviewed were "adult" in nature and 8% were categorized as "scams." See "May 2003 Spam Category Data," <http://www.brightmail.com/pdfs/0503_spam_definitions.pdf> (last accessed 1 January 2004) [no longer available].

42. See FTC Study, *ibid*.

43. Particularly in light of other considerations such as the total financial harm caused by spam, *supra* note 31.

★

3. INDUSTRY CANADA'S SPAM POSITION PAPERS

3.1. *Canada's Position in 1997: Spam Legislation is Not Required*

INDUSTRY CANADA RELEASED ITS FIRST discussion paper on unsolicited email in 1997,⁴⁴ in which it concluded that new legislative measures were not required. Instead, the position advocated was that spam could be controlled through various existing means; including:

- the free market for ISP services;⁴⁵
- good business practices;⁴⁶
- privacy legislation;⁴⁷
- private civil actions;⁴⁸ and
- existing *Criminal Code* provisions.⁴⁹

Given the growth statistics on spam, it appears clear that these mechanisms have not been as successful as the government may have hoped. In retrospect, the failure to combat spam through these means may be explained as follows.

3.1.1. Free Market Efficiency

One of Industry Canada's recommendations was to allow free market efficiency to dictate that ISPs who fail to deal with spam effectively (e.g. through the latest software filters) will lose customers to those that do. This reliance on consumer choice may have been misplaced in that while all ISPs try to block spam communications,⁵⁰ there are limits to what can be done in the face of spammers'

44. See 1997 Spam Paper, *supra* note 15.

45. Consumers were urged to select ISPs most responsive to their needs, to exercise caution when choosing internet navigation tools and to be wary of open discussion areas on the internet.

46. Industry stakeholders (such as the Canadian Marketing Association and Canadian Association of Internet Providers) were urged to enact industry-wide codes and practices. For example, the Canadian *Code of Advertising Standards*, the Canadian Marketing Association's *Code of Ethics and Standards of Practice* and the Canadian *Code of Practice for Consumer Protection in Electronic Commerce*, which establish business practices with respect to email advertising or soliciting.

47. See e.g. *Personal Information Protection and Electronic Documents Act*, 2000, c. 5, <<http://laws.justice.gc.ca/en/P-8.6/text.html>> [PIPEDA], where email addresses may fall under the definition of "personal information." As such, there is an obligation on organizations falling under PIPEDA to collect, use and disclose information regarding one's email address (or personal information) in the course of commercial activity within certain restraints. Also, there is obligation for these same organizations to provide appropriate security for this personal information. See also discussion in Part 3.1.2 below.

48. See discussion in Part 3.1.3 below.

49. Various sections of Canada's *Criminal Code*, R.S.C. 1985, c. C-46, <<http://laws.justice.gc.ca/en/C-46/text.html>>, may be triggered by the content or the practice of spam. For example, s. 342.1 of the *Criminal Code* makes it an offence to fraudulently use a computer system with the intent to commit mischief under s. 430 of the *Criminal Code*. See also discussion in Part 3.1.4. below.

50. *Supra* note 10. See also America Online, *Experts Warn*, *supra* note 36. MessageLabs, which scans millions of emails per day using "heuristics" scanning, intercepts 45 spam emails every *minute*, with a spam filtering accuracy of 96.03%, <<http://www.message-labs.com/home/default.asp>>. Also, Microsoft has spent more than a half-billion dollars trying to build software to filter out spam. See Saul Hansell, "How to Unclog the Information Artery" *The New York Times* (25 May 2003), <<http://www.nytimes.com/2003/05/25/business/yourmoney/25SPAM.html?ex=1369195200&en=b7bfb2724bdeabdb&ei=5007&partner=USERLAND>>.

increasingly sophisticated filter-avoidance tactics.⁵¹ Moreover, regardless of the extent to which ISPs could deal with spammers if enough money was spent, all of these costs are ultimately passed on to consumers in access fees.⁵²

3.1.2. Privacy Legislation

Industry Canada also expressed hope that spam could be controlled through federal privacy legislation in both the public and private sector.⁵³

At the public sector level, the *Privacy Act*⁵⁴ aims to protect the privacy of personal information held by federal institutions and provide Canadians with a right to access and correct information about them held by those institutions.⁵⁵

At the private sector level, as of 1 January 2001, individuals have also been protected by the provisions of the PIPEDA.⁵⁶ PIPEDA sets out rules for how private sector organizations may use, collect or disclose personal information in the course of their commercial activities. This legislation attempts to strike a balance:

...between an individual's right to the protection of personal information and the need of organizations to obtain and handle such information for *legitimate business purposes*....Canadians have the right to know and...ask why a business or organization is collecting, using or disclosing their personal

-
51. See Jim Hu, "AOL Filters Out Some E-mails From ISPs" *CNET New.com* (11 June 2003), <<http://news.com.com/2100-1032-1014827.html>>; Amit Asaravala, "Yahoo Spam Filter Thwarts FTC" *Wired.com* (28 June 2003), <<http://www.wired.com/news/politics/0,1283,59427,00.html>>.
52. The real question is whether it is fair to require consumers to pay for no spam.
53. Various provinces have also enacted sector-specific laws dealing with the protection of personal information. For instance, every province except New Brunswick has legislation dealing with consumer credit reporting. See e.g. *Consumer Reporting Act*, R.S.O. 1990, c. C.33, <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c33_e.htm>; *Credit Reporting Act*, R.S.B.C. 1996, c. 81, <http://www.qp.gov.bc.ca/statreg/stat/C/96081_01.htm>; *Consumer Reporting Act*, R.S.N.S. 1989, c. 93, <<http://www.gov.ns.ca/legi/legc/statutes/consumrp.htm>>. In the health sector, Alberta, Manitoba and Saskatchewan have all passed privacy legislation: *Health Information Act*, R.S.A. 2000, c. H-5, <<http://www.qp.gov.ab.ca/documents/acts/H05.cfm>>; *Health Information Protection Act*, S.S. 1999, c. H-0.021 (not yet proclaimed into force), <<http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf>>; and *Personal Health Information Act*, R.S.M. 1997, c. 51-Cap.P33.5, <<http://web2.gov.mb.ca/laws/statutes/csm/p033-5e.php>>, respectively. Ontario has enacted its *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3 – Bill 31, <http://www.e-laws.gov.on.ca/DBLaws/Source/Statutes/English/2004/S04003_e.htm>, which came into effect on 20 May 2004.
54. R.S. 1985, c. P-21, <<http://laws.justice.gc.ca/en/P-21/>>. The *Privacy Act* defines "personal information" as "information about an identifiable individual that is recorded in any form."
55. *Ibid.*, s. 12. With the exception of Prince Edward Island, all provinces in Canada also have public sector privacy legislation operating in parallel to the federal statute. See e.g. *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, <http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90f31_e.htm>; *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c.165, <http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm>; *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, <http://www.qp.gov.ab.ca/documents/Acts/F25.cfm?frm_isbn=0779729218>.
56. Parliament passed PIPEDA in April 2000, *supra* note 47. With the exception of Quebec, Alberta and British Columbia respectively, no other province has yet enacted privacy legislation that applies to the private sector: *An Act Respecting the Protection of Personal Information in the Private Sector*, S.Q. 1993, c. 17, R.S.Q., c. P-39.1, <<http://www2.publicationsduquebec.gouv.qc.ca/home.php>> [search term A-2.1_A]; *Personal Information Protection Act*, S.A. 2003, c. P-6.5, <http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779725816> and *Personal Information Protection Act*, S.B.C. 2003, c. 63, <http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm>. For greater discussion, see Canada, Privacy Commissioner, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (Ottawa: Privacy Commissioner of Canada, June 2003), <http://www.privcom.gc.ca/legislation/leg-rp_030611_e.asp>.

information...businesses must obtain the individual's consent when they collect, use or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk.⁵⁷

PIPEDA defines "personal information" broadly as "any information about an identifiable individual whether recorded or not."⁵⁸ It further defines "commercial activity" as conduct of a "commercial character," which clearly applies to spam (the majority of which attempts to solicit some sort of commercial transaction with the recipient).⁵⁹

PIPEDA applies to the collection, use and disclosure of personal information such as one's name, address, social insurance number or credit card number, all information which may be gathered by spammers in their attempts to solicit a business transaction. Given the breadth of PIPEDA's definition of "personal information," it may also be argued that a person's email address, user name and password (whether recorded or not) qualifies as information about an identifiable individual, thus falling under the auspices of PIPEDA.⁶⁰ Such legislation, therefore, prohibits corporations and other entities from collecting personal email information and selling it without individuals' consent. This was noted by Industry Canada in 1997 as follows:

Since electronic mail addresses, other than business addresses, are deemed to be personal information, the legislation will impose some restrictions and obligations on how these addresses and other personal information are collected, used and disclosed in the course of commercial activity. The law also creates an obligation for these firms and others who store electronic mail addresses to provide appropriate security for this personal information. In the first three years after coming into force, the legislation will apply to federally-regulated undertakings and to private sector firms who engage in the interprovincial and international trade in personal information. After this time, all organisations using personal information in the conduct of commercial activities will be covered, unless they are subject to provincial privacy

-
57. Privacy Commissioner, "An Overview of the Personal Information Protection and Electronic Documents Act" (December 2000), <http://www.privcom.gc.ca/legislation/02_06_07_e.asp> [PIPEDA Backgrounder]; PIPEDA, *supra* note 47, s. 3 [emphasis added].
58. PIPEDA, *ibid.*, s. 2(1). Note that "personal information" does not include the name, title or business address or telephone number of an employee of an organization.
59. *Ibid.*, s. 2(1) defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."
60. Just as one's residential telephone number qualifies as personal information under PIPEDA. See Privacy Commissioner, "PIPED Act Case Summary #99: Personal Information Improperly Disclosed to Collection Agency," (2 December 2002), <http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021202_2_e.asp>. See Suzanne Morin, "Fighting Spam from Canada: How PIPEDA can do its Part" (2004) 1 Canadian Privacy Law Review 8, <<http://strategies.ic.gc.ca/sitt/spamforum/servlet/JiveServlet/download/1-102-357-38/PIPEDA%20Article.doc>>, who argues that the use of one's work email address in a non-work context should not be subject to the "business card data exemption" just as the collection, use or disclosure of one's email address for purposes not related to one's employment should not be subject to the exemption. See also Barry B. Sookman, *Sookman on Computer, Internet and Electronic Commerce Law* (Toronto: Carswell, 2004) vol. 2 at p. 8-107; Adam Kardash & Rhonda Shirreff, "Privacy Law" in Alan M. Gahtan, Martin P.J. Kratz & J. Fraser Mann, eds. *Electronic Commerce: A Practitioner's Guide* (Toronto: Carswell, 2003) at p. 19-9 to p. 19-10.

legislation which has been deemed to be substantially similar to the federal law. Thus, firms buying, selling, leasing or bartering electronic mailing lists, which are the basis for bulk unsolicited electronic mail, will be subject to the provisions of the legislation, if these transactions take place over provincial and national borders.⁶¹

Privacy legislation, such as PIPEDA, acts primarily as an obstacle to the brokering of information lists, rather than to the act of spamming itself. Such legislation was never drafted with spam in mind.⁶² While it may act to restrict the sale of email lists, the potential impact of this approach may be undermined by the global nature of the internet. PIPEDA applies only to organizations in Canada and, internationally, rules for the collection of personal information are not necessarily uniform.⁶³ Moreover, spammers can easily acquire their own sophisticated software, available over the internet or through mail order, to harvest email addresses.⁶⁴

It may, however, be too early to evaluate PIPEDA's impact on spam in that the legislation only came into effect on 1 January 2004.⁶⁵ However, the fact that other jurisdictions with substantially similar privacy regulations have also seen the need to adopt spam-specific legislation,⁶⁶ suggests that PIPEDA and other such legislation may not constitute a comprehensive solution for Canada.

61. 1997 Spam Paper, *supra* note 15.

62. The enactment of PIPEDA was, in fact, prompted to conform with OECD Guidelines which attempted to harmonize data protection regimes within various member states in 1995. See EC, *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31, <http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf> [Privacy Directive 95/46/EC]. See also Paul Festa, "New OECD Guidelines Target Spam, Fraud" *CNET News.com* (17 June 2003), <http://news.com.com/2100-1028_3-1018413.html>.

63. See Jennifer Stoddart, "Transferring Personal Information about Canadians Across Borders—Implications of the USA Patriot Act" (18 August 2004), <http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_e.asp>, who concludes that PIPEDA applies to personal data held in Canada (*i.e.* PIPEDA also applies to data relating to persons outside of Canada but which (personal) data is held by an entity in Canada). Personal data about Canadians held by extraterritorial organizations are subject to the laws of the country in which the organization is located. See also Morin, *supra* note 60, who notes that "...an e-mail address as personal information need not belong to a Canadian citizen or resident as [PIPEDA] applies to all personal information collected, used or disclosed in the course of commercial activities in Canada. This was made quite clear when Parliament amended s. 3 during its Bill C-6 stage replacing 'Canadians' with 'individuals' to accommodate the concerns of the European Commission regarding adequate protection for transfers to Canada."

PIPEDA also applies to personal information practices of websites with a physical presence in Canada. Whether PIPEDA will apply to the collection or use of personal information of Canadians by a website with no physical presence in Canada, however, is more questionable. See Kardash, *supra* note 60 at p. 19-9. The US resolved differences in its approach to privacy issues in the private sector with Europe by adhering to "Safe Harbor Privacy Principles," <<http://www.ita.doc.gov/td/ecom/menu.html>>.

64. Examples include Atomic Harvester, Desktop 2000, or EMAIL_ID. Note that most existing legislation contain provisions prohibiting activities such as harvesting email addresses. See *e.g.* CAN-SPAM Act, *supra* note 20, s. 5(b)(1); *Australia Spam Act of 2003*, *supra* note 4, ss. 20-22.

65. PIPEDA came into force in three stages, such that non-federally regulated private sector organizations became affected since January 1, 2004. See PIPEDA Background, *supra* note 57. PIPEDA's survival, however, remains uncertain as it is anticipated that Quebec will challenge its constitutionality. See Michael Geist, "Fighting Privacy Law Questionable" *The Toronto Star* (19 January 2004), <http://www.michaelgeist.ca/resc/html_bkup/jan192004.html>.

66. For instance, despite Europe's Privacy Directive 95/46/EC, *supra* note 62, and the European Directive, *supra* note 28, were enacted to deal with unsolicited direct marketing communications. Specifically, it was enacted to provide an equal level of protection across its Member States of personal data and privacy for users of publicly available electronic communication services, with respect to the processing of personal data in electronic communications.

3.1.3. Private Actions

The internet is not a “lawless” medium and existing national laws can apply to the practice of spamming depending on the circumstances. For example, spammers have been pursued civilly (with varying degrees of success) for several causes of action, including:

- false designation of origin;⁶⁷
- trade-mark dilution and unfair competition;⁶⁸
- nuisance;⁶⁹
- interference with contract or business relations;⁷⁰
- trespass to chattels;⁷¹ and
- breach of contract (primarily by ISPs according to their terms of use provisions).⁷²

Nevertheless, the effectiveness of pursuing spammers in the civil courts is discounted by a number of factors. First, spammers are skilled at concealing their identities in cyberspace, which makes it difficult even to locate them to commence a legal process.⁷³ Second, it is far from certain that a spammer, once located, would clearly be tied to a claimant’s home forum, raising complicated questions of jurisdiction and conflict of laws. Even if a process can be initiated, civil litigation can take years to bring to trial in Canada, by which time the spammer can simply have re-established under a new identity to continue its activities.⁷⁴

67. *AOL v. IMS*, *supra* note 11; *AOL v. LCGM*, *supra* note 11; *Hotmail Corp. v. Van\$ Money Pie Inc.*, 47 U.S.P.Q. 2d (BNA) 1020 (ND Cal 1998); *America Online Inc. v. The Christian Brothers*, 98 Civ. 8959 (SD NY 1999) [*AOL v. Christian Brothers*].
68. *AOL v. Christian Brothers*, *ibid.*; *Classified Ventures, L.L.C. v. Softcell Mktg., Inc.*, 109 F.Supp. 2d 898 (ND Ill 2000).
69. *AOL v. Christian Brothers*, *ibid.*; *Parker v. C.N. Enterprises*, No. 97-06273 (Tex Dist Ct Travis County 1997).
70. *Concentric Network Corp. v. Wallace*, No. C-96 20829-RMW(EA) (ND Cal 1996).
71. In *Intel Corporation v. Hamidi*, 30 Cal. 4th 1342 (2003), <http://www.law.berkeley.edu/clinics/samuels/son/projects_papers/2002sp_intel_hamidi_decision.pdf> at p. 1347 [*Hamidi*], the California Supreme Court recognized that email, like other forms of communication, may in some circumstances cause legally recognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories. However, it held that an electronic communication that neither damages the recipient computer system nor impairs its functioning does not constitute an actionable trespass to personal property. Previous cases had been more successful. See *Earthlink v. Carmack*, *supra* note 11; *Earthlink Network, Inc. v. Cyber Promotions, Inc.*, No. BC167502 (Cal Ct LA County 1997); *AOL v. IMS*, *supra* note 11; *Hotmail Corp. v. Van\$ Money Pie Inc.*, *supra* note 67; *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015 at 1017 (SD Ohio 1997) [*CompuServe*]. See also Anne E. Hawley, “Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail” (1997) 66 *UMKC Law Review*. 381; Dan L. Burk, “The Trouble With Trespass” (2000) 4 *Journal of Small & Emerging Business Law* 27, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=223513>; Susan Ballantine, “Computer Network Trespasses: Solving New Problems with Old Solutions” (2000) 57 *Washington & Lee Law Review* 209.
72. As a condition of subscription, many ISPs restrict their customers’ right to send junk email. See e.g. *1267623 Ontario Inc. v. Nexx Online Inc.* (1999), 45 O.R. (3d) 40, (1999), 46 B.L.R. (2d) 317 (S.C.J.). See also *Internet Direct Inc. v. Altelaar*, [1999] O.J. No. 1804 (S.C.J.) (QL).
73. See Helen Carter, “Anti-Spam Writ ‘Names Wrong Man’” *Guardian Unlimited* (26 June 2003), <<http://www.guardian.co.uk/print/0,3858,4699088-103690,00.html>>.
74. Although there are those who contend that the majority of spam comes from only 100 or 200 sources, suggesting that a concerted worldwide effort can shut down the worst offenders. See Kate Hearfield, “Enough already! Spam is getting more aggressive, but so, too, are efforts to stop it” *The Ottawa Citizen* (19 June 2003) H2.

Quick injunctive relief against spammers and their directors is needed before trial but, at least in Canada, interlocutory injunctions are an increasingly rare event.⁷⁵ Injunctions can also cost well in excess of CAN\$100,000 to bring successfully.⁷⁶ Even if judgment is ultimately obtained against a spam business, it may be nothing more than a shell company with no assets in the jurisdiction, rendering a costs or damages award effectively meaningless.⁷⁷

3.1.4. Criminal Law Enforcement

Various existing criminal and quasi-criminal statutes and regulations can also be triggered by the spam content or the practices of some spammers.⁷⁸ The *Criminal Code*, for example, contains several sections that may be used to bring actions.⁷⁹ Spammers that make unauthorized use of property belonging to ISPs or an individual's email server may be subject to section 342.1 of the *Criminal Code*.⁸⁰ Spammers may also be caught by section 372(1) of the *Criminal Code*, which may be used as a basis for an action against spammers who—with intent to injure—send messages they know to be false.⁸¹ Similarly, deceitful and fraudulent behaviour may be subject to section 380 of the *Criminal Code*.⁸²

However, prosecutors or claimants must often establish violations of such provisions to a high criminal burden of proof (“beyond a reasonable doubt”). Many applicable *Criminal Code* provisions also require proof of intention on the part of the spammer to have acted “fraudulently”⁸³ or to have

75. Particularly in intellectual property matters, courts are requiring “clear and non-speculative evidence of irreparable harm” caused by the respondent’s actions prior to considering such injunction. See e.g. Diane E. Cornish, “‘Clear and Not Speculative’ Evidence of Prospective Harm: The Conundrum of Proving Irreparable Harm” (1994) 10 C.I.P.R. 589; *Centre Ice Ltd. v. National Hockey League* (1994), 166 N.R. 44, (1994), (1994), 53 C.P.R. (3d) 34 (FCA).
76. As described to the author by intellectual property litigators from Gowling Lafleur Henderson LLP’s Toronto office.
77. See Fogo, *supra* note 3 at p. 922. Fogo suggests that private suits by ISPs have failed to solve the problem because enforcement is limited to those ISPs who can afford to pursue such claims, and spammers are a step ahead of anti-spam ISPs by attempting to circumvent litigation by paying other networks to carry its junk email.
78. See e.g. *Competition Act*, R.S. 1985, c. C-34, s. 52.1 (telemarketing) and Part VII.1 generally (deceptive marketing practices), <<http://laws.justice.gc.ca/en/C-34/>>; *Telecommunications Act*, 1993, c. 38, s. 41, <<http://laws.justice.gc.ca/en/T-3.4/index.html>>.
79. In 1985 the *Criminal Code*, *supra* note 49, was amended to create two groups of new offences. One group dealt with unauthorized access and use of computers, the other with mischief in regard to computers and data. See also 1997 Spam Paper, *supra* note 15.
80. *Criminal Code*, *supra* note 49, s. 342.1(a) states that “[e]very one who, fraudulently and without colour of right...obtains, directly or indirectly, any computer service...is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.”
81. *Ibid.*, s. 372(1) states that “Everyone who, with intent to injure or alarm any person, conveys or causes or procures to be conveyed by letter, telegram, telephone, cable, radio or otherwise information that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.”
82. *Ibid.*, s. 380.(1) states that “Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service...is guilty of an indictable offence and liable to a term of imprisonment ...”.
83. For example, in *R. v. Hamilton*, 2002 ABQB 15, <<http://www.albertacourts.ab.ca/jdb/1998-2003/qb/Criminal/2002/2002abqb0015.pdf>>, [2002] 8 W.W.R. 334, the accused was charged under s. 464 of the *Criminal Code* for sending spam emails which counselled recipients on how to assemble bomb-making equipment. Hamilton was acquitted, as the Crown was unable to prove the constituent *mens rea*, which in this case required proof, beyond a reasonable doubt, that he intended a bomb to be constructed.

had an intention to injure. Given these realities, it is perhaps not surprising that there have been very few criminal spam prosecutions in Canada to date.

3.2. Canada's Position in 2003: A Re-consideration

In January of 2003, Industry Canada released a second discussion paper on unsolicited email to re-open a dialogue "to identify possible areas where both industry stakeholders and consumers will find a common interest in achieving effective solutions [to the problem of spam]."⁸⁴ This new discussion paper identifies several "key" issues in this dialogue, including whether Canada needs to introduce new spam-specific laws. This latest paper therefore represents a departure from Industry Canada's earlier position in 1997 that existing civil and criminal prohibitions would be sufficient to combat the problem of spam.⁸⁵

The Canadian government's renewed interest in seeking input on the appropriateness of spam legislation in Canada may be a reaction to legislative efforts undertaken recently in other countries. Indeed, the suggestion has been made that Canada must move forward on this issue if it is to avoid becoming perceived as a haven for international spammers.⁸⁶

3.3. Canada's Position in 2004: Moving Forward

One result of Canada's 2003 position paper was the creation of a new "Spam Task Force" as announced on 11 May 2004, by the federal Minister of Industry, Lucienne Robillard. Initially, the Spam Task Force also advised against the enactment of specific spam legislation, choosing instead to explore the effectiveness of the current Canadian enforcement framework (discussed above in Part 2.1).⁸⁷ However, on 17 May 2005, the Honourable David L. Emerson received the final report of the Spam Task Force entitled *Stopping Spam: Creating a Stronger, Safer Internet*, which includes a range of recommendations,

84. 2003 Spam Paper, *supra* note 4.

85. The 2003 Spam Paper identifies the remaining issues as: (1) the role of ISPs in managing consumers' email preferences in light of PIPEDA; (2) filtering technologies; (3) consideration of a zero-tolerance policy; (4) network solutions to curtail the abuse by spammers of improperly configured servers; and (5) consumer awareness issues.

86. Douglas Hunter, "Toronto Will Be Spam Central: U.S. Fights e-Marketing: Bulk Lists Hurt Companies' Bottom Lines" *The National Post* (7 July 2003) FE 1. According to security software firm, Sophos, the majority of spam (56.74%) originates from the United States, with Canada trailing in second at 6.80% ("Sophos Outs 'Dirty Dozen' Spam Producing Countries" (26 February 2004), <<http://www.sophos.com/spaminfo/articles/dirtydozen.html>>). But see Jack Kapica, "Canada Drops in Global Spam Ranking" (26 August 2004), <<http://www.globetechnology.com/servlet/story/RTGAM.20040826.gtspamaug26/BNStory/Technology/>> [subscription required], the article reports that Canada dropped to fifth place since the first Sophos survey released in February 2004.

87. See Industry Canada, Spam Task Force, <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html>. In a recent paper, Professor Michael Geist, a member of the Spam Task Force, argues that the current Canadian legislative framework provides Canada with similar legal powers to fight spam and spam legislation in other jurisdictions. Professor Geist cites the lack of enforcement of these laws as a significant factor to Canada's failure, to date, to successfully combat (Michael Geist, "Untouchable?: A Canadian Perspective on the Anti-Spam Battle," (May 2004), <<http://www.michaelgeist.ca/geistspam.pdf>>).

including the establishment of a clear set of rules to prohibit spam and the creation of spam-specific legislation.⁸⁸

With the prospect of future Canadian spam legislation in mind, the following section of this article briefly reviews some models of spam regulation being pursued by other countries, before turning to the Canadian context.

*

4. SPAM REGULATION MODELS

THERE ARE SEVERAL JURISDICTIONS, including the United States and Europe, that have already implemented spam legislation.⁸⁹ Broadly speaking, the measures introduced in such countries have attempted to deal with the practice and consequences of spamming in two ways:

First, by focusing on the unsolicited nature of spam and mandating recipient consent, either through an "opt-in" or an "opt-out" model.

Second, by focusing on the deceptive practices of spammers and prohibiting tactics intended to disguise their identities or the nature of their emails from recipients.

Each of these regulative strategies, which can be pursued individually or concurrently, are discussed below.

88. See Canada, Spam Task Force, *Stopping Spam: Creating a Stronger, Safer Internet* (Ottawa: Industry Canada, May 2005), <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html>. As outlined in the preamble to the European Directive, *supra* note 28, with the increasing use of public communications networks, legal, "specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons," regardless of the technology used. However, monitoring and enforcing legislation must also be rigorously enforced, see Martyn Williams, "Spam Falls After South Korea Strengthens E-Mail Law" *IDG News Service* (16 September 2003), <<http://www.pcvorldmalta.com/news/2003/Sep/161.htm>>.

89. The 108th US Congress was considering no less than seven proposed national bills, including (1) US, Bill H.R. 2515, *Anti-Spam Bill of 2003*, 108th Cong., 2003, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2515ih.txt.pdf> [Anti-Spam Bill of 2003]; (2) Bill S. 1052, *supra* note 20; (3) Bill S. 877, *supra* note 20; (4) Bill S. 563, *supra* note 28; (5) Bill H.R. 2214, *supra* note 37; (6) US, Bill H.R. 122, *Wireless Telephone Spam Protection Act*, 108th Cong., 2003, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h122ih.txt.pdf>; (7) US, Bill H.R. 1933, *Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003 or the REDUCE Spam Act of 2003*, 108th Cong., 2003, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h1933ih.txt.pdf> [REDUCE Spam Act of 2003]. This last bill was also strongly supported by Lawrence Lessig, who publicly made a wager to resign from his job as Stanford University law professor if the antispam law, which offers a bounty to the first person who reports an unlabelled spam, will not effectively reduce spam (Declan McCullagh, "A Modest Proposal to End Spam" *CNET News.com* (28 April 2003), <<http://news.com.com/2010-1071-998513.html>>).

Beginning in October, 2003, the European Union made unsolicited emails illegal between member European Union states (European Directive, *supra* note 28, art. 13). Within a few months, the Parliament of Australia enacted legislation in its own attempts to combat spam, see *Australia Spam Act 2003*, *supra* note 4. It is interesting to note that the US CAN-SPAM Act appears to be at odds with the European Directive as it, in effect, sets certain limits in its legalization of sending spam.

4.1. Regulating Consent

There are two primary models for securing recipient consent, under which recipients either “opt-in” to receiving e-mails or “opt-out” from receiving e-mails.⁹⁰

4.1.1. Opt-In Models

Under an opt-in regulatory scheme, a party interested in sending an email may be prohibited from doing so unless it has first secured consent from its intended recipients. “Consent” can be satisfied under various circumstances. For example, the current European regime permits a corporation to send unsolicited emails to customers with whom it has an existing business relationship.⁹¹ However, recipients must also be provided with a “clear and distinct” opportunity to remove themselves—free-of-charge—from all further transmissions. The European Directive further provides that recipients should be able to refuse future use of their contact details with each subsequent direct marketing message.⁹²

Note that an exception which requires an existing (or prior) business relationship does not assist any marketer who wants to use email to contact a potential new customer for the first time. Reasonable accommodations can therefore also be considered, such as incorporating a “one kick at the can” exception.⁹³

In short, an opt-in model requires a marketer to put in effort to either establish a relationship with a recipient or otherwise secure their consent before sending any email. While this appears to be the preferred model advocated by anti-spam groups, it raises concerns for anyone who hopes to exploit email as a “legitimate” and inexpensive form of mass communication.⁹⁴

4.1.2. Opt-Out Models

Under an “opt-out” model, spammers are free to target any recipients until told to stop. This model is incorporated, for example, in the CAN-SPAM Act in the United States, which provides that commercial email messages must contain a

90. European Directive, *supra* note 28, contemplates an opt-in scheme. See also The European Coalition Against Unsolicited Commercial Email, *An Opt-in Manifesto*, <<http://www.euro.cauce.org/en/manifesto.html>>. On the other hand, the US CAN-SPAM Act, *supra* note 20, contemplates an opt-out regime. Several previous US bills contemplated an opt-in regime. See e.g. Bill H.R. 2214, *supra* note 37; REDUCE Spam Act of 2003, *ibid*.

91. European Directive, *ibid.*, art. 13(2).

92. *Ibid.*

93. Geist, *Internet Law*, *supra* note 6 at p. 250.

94. “Legitimate” direct marketing organizations have expressed two primary concerns in regard to the opt-in regime: (1) opt-in increases transaction costs ultimately leading to higher prices and decreased competition; and (2) freedom of expression concerns. See Fred H. Cate & Michael E. Staten, “Protecting Privacy in the New Millennium: The Fallacy of ‘Opt-In’” *Direct Marketing Association* <<http://www.the-dma.org/isec/optin.shtml>>; Michael A. Turner, “The Impact of Data Restrictions on Consumer Distance Shopping” *Direct Marketing Association* <<http://www.the-dma.org/isec/9.pdf>>. See also European Coalition Against Unsolicited Commercial Email, “Opt-in vs. Opt Out,” <<http://www.euro.cauce.org/en/optinsoptout.html>> [EuroCAUCE, “Opt-in vs. Opt Out”].

notice indicating that the recipient will be given an opportunity to refuse further commercial email messages. Commercial email messages must also include the sender's return email address and a valid physical postal address clearly and conspicuously displayed that allows a recipient to inform the sender (s)he does not wish to receive future commercial email messages,⁹⁵ along with a valid physical postal address of the sender.⁹⁶

Anti-spam groups point to a number of perceived deficiencies with the opt-out model:⁹⁷

Under an "individual" opt-out model, recipients bear the onus of responding to each spam email to expressly request they be removed from the sender's email list. Given the growing tide of spam emails, this may place an unfair burden on consumers. In addition, opponents question why a recipient should be required to remove himself or herself from a list they never sought to join.⁹⁸

Under a "national" or "global" opt-out model, a private or perhaps public database is proposed that would record and update which consumers are willing to receive unsolicited emails. Such a regime has, however, been criticized as being "administratively unworkable."⁹⁹

4.2. Mandating Truth and Accuracy

Several countries' proposed spam models also incorporate one or more provisions which target spammers' avoidance tactics. For example, the European Directive prohibits sending email, for the purposes of direct marketing, and "disguising or concealing" the identity of the sender. It also prohibits the use of false return addresses when sending unsolicited communications for direct marketing purposes.¹⁰⁰ Similarly, the US CAN-SPAM Act prohibits the

95. CAN-SPAM Act, *supra* note 20, s. 5(a)(3)(A)(i). Section 5(a)(3)(A)(ii) further provides that the functioning return email address must remain capable of receiving "unsubscribe" messages for no less than 30 days after the transmission of the original message. See also *Australia Spam Act 2003*, *supra* note 4, s. 18, requiring that commercial electronic messages must contain a functional unsubscribe facility.

96. CAN-SPAM Act, *ibid.*, s. 5(a)(5).

97. See e.g. EuroCAUCE, "Opt-in vs. Opt Out," *supra* note 94; Sorkin, *supra* note 8 at pp. 352-354. See also Roy Mark, "Bush Signs Can Spam Bill" *Internet News.com* (16 December 2003), <<http://www.internetnews.com/bus-news/article.php/3289551>>.

98. See e.g. CAUCE, "Non-Solutions," <<http://www.cauce.org/problem/nonsolutions/>>.

99. Indeed, JupiterResearch released a survey, "JupiterResearch Finds Legitimate E-Mail Marketers Struggling with Federal Can-Spam Compliance" (20 April 2004), <<http://www.jupitermedia.com/corporate/releases/04.04.20-newjupresearch.html>> [JupiterResearch, 2004], which tracked over fifty leading (and legitimate) email marketers in different industries, including retail, travel, media. JupiterResearch found that, *inter alia*, only 64% of commercial electronic mail messages tracked included the sender's street address (which is required by the US Federal CAN-SPAM Act) and almost one-quarter of marketers continued to send email even after opt-outs were submitted.

The British Department of Trade and Industry states that an effective opt-out scheme would have to satisfy at least five criteria: (1) all subscribers must be aware of it; (2) it must be simple and free to join; (3) it must become effective within a reasonable time of joining; (4) companies engaged in unsolicited emailing must update their lists regularly in light of changes to the global opt-out database; and (5) an adequate complaint resolution process must be in place. EuroCAUCE, "Opt-in vs. Opt Out," *supra* note 94.

100. European Directive, *supra* note 28, art. 13(4).

transmission of false or misleading information.¹⁰¹ The CAN-SPAM Act also makes it unlawful for persons to transmit a commercial email message to a protected computer if that person knew the subject heading of the message would likely mislead a recipient regarding the contents or subject matter of the message.¹⁰²

A further requirement may be that the commercial nature of the email be described in the subject line in a clear, conspicuous and accurate manner (e.g. by stating "Commercial Advertisement").¹⁰³

In summary, while the Canadian government has only recently sought input on the need for spam legislation in Canada by implementing its Spam Task Force, it is reasonable to expect that the Canadian spam debate will include a discussion about the respective merits of the opt-in and opt-out models, which have been considered and implemented in other countries. However, regardless of which models are ultimately proposed, the prospect of spam legislation in Canada raises two important constitutional questions that need to first be considered:

First, which of our two levels of government—provincial or federal—is legislatively competent under the Constitution Act to craft legislation that targets unsolicited electronic communications?

Second, is it possible to propose an effective regulatory model that is also constitutionally sustainable, in regard to subsection 2(b) of the *Charter*?

Each of these questions is discussed in the following sections of this article.¹⁰⁴

101. CAN-SPAM Act, *supra* note 20, s. 5(a)(1).

102. *Ibid.*, s. 5(a)(2). It may, however, be difficult to prove that the sender had "actual knowledge" or "knowledge fairly implied on the basis of objective circumstances" that a subject heading of a commercial email message would likely mislead a reasonable recipient, which may render this provision ineffective. See also Australia Spam Act 2003, *supra* note 4, ss. 16 (unsolicited commercial electronic messages must not be sent) and 17 (commercial electronic messages must include accurate sender information).

103. For example, Anti-Spam Bill of 2003, *supra* note 89, s. 101; REDUCE Spam Act of 2003, *supra* note 89, s. 4(a); Bill H.R. 2214, *supra* note 37, s. 101. The CAN-SPAM Act further provides that if the commercial email message contains sexually oriented content, such email message must include in the subject heading the proper notice(s) prescribed by the Federal Trade Commission. See CAN-SPAM Act, *supra* note 20, s. 5(a)(5). The Australia Spam Act 2003, *supra* note 4 at s. 16, prohibits the sending of a commercial electronic message that is not designated as a commercial electronic message.

104. While likely only of academic note, Professor Hogg suggests that it is only after the resolution of a division of powers dispute that a court should proceed to consider whether the law is consistent with the *Charter*. See Peter W. Hogg, *Constitutional Law of Canada*, looseleaf (Scarborough: Carswell, 1997) vol. 1 at p. 15-3.

★

5. THE DIVISION OF POWERS¹⁰⁵

5.1. Overview: *The Concepts of "Pith and Substance" and "Concurrency"*

THE QUESTION OF LEGISLATIVE JURISDICTION to regulate the internet—either as a whole or over its component parts—has not been addressed by a superior court in Canada at the time this article was being written.¹⁰⁶ Canada is a federation in which power is distributed between the national government and the several provincial and territorial authorities. The Constitution defines which laws can be enacted by Parliament (on the one hand) and each of the provincial and territorial Legislatures (on the other). When a law is challenged on division of powers grounds, it is left to the courts to decide whether the law is valid (*intra vires*) or invalid (*ultra vires*) of the level of government that made it.

Any court reviewing a law on division of powers grounds must go through a two-step conceptual process.¹⁰⁷ First, the court must characterize the law's "pith and substance," meaning what the law actually does and why.¹⁰⁸ Second, the court must then attempt to fit the law's pith and substance into the most appropriate classes of power enumerated by the *Constitution*, thereby determining which level of government was competent to have made the law.

The difficulty is that many statutes can be interpreted as having one feature that should fall within a federal head of power and a second that should fall within a provincial head power. Professor Hogg provides the example of a provincial statute that imposes a direct tax on banks. One feature of such law could be "direct taxation" (a provincial head by virtue of section 92.2) but another could be "banking" (which is a federal head under section 91.15). In such a case, Hogg suggests that a court would attempt to characterize the dominant feature (the "pith and substance") of the law, and classify the secondary feature as merely incidental and irrelevant for constitutional purposes.¹⁰⁹

This important technique of constitutional interpretation, known as "concurrency," permits each level of government to enact legislation that impacts upon subject matter beyond its own jurisdiction.¹¹⁰

105. In this and subsequent sections, all references to ss. 91 and 92 are to be understood as referring to the applicable provisions of the *Constitution*, *supra* note 17. Full references are sometimes omitted to avoid repetition.

106. Though it has been addressed in two labour board decisions, see *infra* note 153.

107. As reviewed by Hogg, *supra* note 104, c. 15.

108. The characterization of the law's "pith and substance" may require investigation beyond its purpose or legal effects, leading courts to inquire into its social or economic purposes. See *Alberta (A.G.) v. Canada (A.G.) (Bank Taxation)*, [1939] A.C. 117 (P.C.) at p. 130, *per* Lord Maugham L.C.

109. Hogg, *supra* note 104 at p. 15-8. One could then say, for example, that the provincial law was "in relation to" taxation but merely "affected" the federal powers over banking.

110. In choosing between competing, plausible characterizations of a law, a court should normally choose the one which would support a finding of validity. See *Re Firearms Act*, [2000] 1 S.C.R. 783, <http://www.lexum.umontreal.ca/csc-scc/en/pub/2000/vol1/html/2000scr1_0783.html>, [*Firearms*] at para. 26. Further, a court may sever or read down the sections of an impugned law that are *ultra vires*. See Hogg, *supra* 104 at p. 15-21 to p. 15-24.

5.2. Application to the Context of a Canadian Spam Law

5.2.1. Overview

Imagining that a spam law has been enacted and challenged in Canada, the first task for a court would be to determine that law's "pith and substance." It is suggested, in accordance with the earlier sections of this paper, that the problem of spam raises several potentially relevant "aspects."

The regulation of spam might involve restrictions on both the content of electronic communications and on the facilities used to permit those communications to occur. It may or may not be the case that both aspects can be regulated by the same level of government.

A great deal of spam is commercial in nature and any regulatory model might have a real impact on the laws of advertising and contracts, as well as on other aspects of trade and commerce. Legislative authority may differ depending whether the law relates to all electronic solicitations or only those made wholly within a province.

Criminal law aspects may also be discerned, given the content of some spam and the deceptive practices employed by spammers.

5.2.2. "Pith and Substance" Analysis

For the purpose of this article, an assumption will be made that any spam legislation enacted in Canada would be modeled in one form or another on the approaches taken by our major economic partners.¹¹¹ Those approaches suggest that a fair characterization of the dominant purpose of a spam law could be as follows: *to protect the rights of recipients not to receive email (either all or of only a limited class) against their wishes, and to prescribe the circumstances in which recipient consent can be reasonably presumed to exist.*¹¹²

With this suggested characterization in mind, the most likely competing heads of constitutional subject matter will now be reviewed.

5.2.3. Selection of the Most Appropriate Head of Power

The respective heads of legislative competency in Canada are prescribed by sections 91 (federal) and 92 (provincial) of the *Constitution Act, 1867*. Applied to spam communications, and bearing in mind that neither "spam" nor the "internet" were conceivable at the time of Confederation, the following are suggested as the leading competing classes of subject matter:

111. Namely, the United States, the European Union and Australia, as described above.

112. This characterization is adopted while acknowledging that other aspects of spamming may be regulated concurrently. However, in the opinion of this author, the issue of recipient consent would be at the heart of any proposed law.

- Provincial:
 - Property and Civil Rights (Section 92.13)
- Federal:
 - Trade and Commerce (Section 91.2);
 - Criminal Law (Section 91.27);
 - Peace, Order, and Good Government [“POGG”] (opening words to Section 91); and
 - Transportation and Communication (Section 92.10).

Each of these will be reviewed in turn.

5.2.3.1. *The Provinces: Property and Civil Rights (Section 92.13)*

By far the most important power conferred on the provinces and territories is the power to regulate “property and civil rights” within their respective jurisdictions. In division of powers cases, it is usually this provincial head of power which is litigated in competition with one or more federal heads.¹¹³ The phrase “property and civil rights” is very broad and, in practice, is limited only by the exclusive heads of subjects expressly withdrawn for vesting in the federal Parliament.¹¹⁴ “Property and civil rights” is considered generally to include most of the private law of property, contract and tort within the provinces.¹¹⁵ As such, unless a federal head of power can be invoked, the problem of spam should be considered an issue falling within the legislative competency of the provincial Legislatures.

5.2.3.2. *Federal Heads of Power*

5.2.3.2.1. Trade and Commerce (Section 91.2)

Section 91.2 of the *Constitution* confers upon the federal Parliament the power to make laws in relation to “the regulation of trade and commerce.” The clear interpretive problem that arises is how to construe this federal authority in light of the provinces’ exclusive jurisdiction over “property and civil rights.” Case law has demonstrated that the courts have avoided overlap by modifying the jurisdiction of both heads of power. Since *Citizens’ Insurance Co. v. Parsons*,¹¹⁶ it has been accepted that intra-provincial trade and commerce falls within “property and civil rights,” whereas the federal power is confined to either inter-provincial/international trade and commerce or trade and commerce “in general.”¹¹⁷

113. Hogg, *supra* note 104 at p. 21-2.

114. According to Professor Hogg, “it is clear that the framers ... understood [Property and Civil Rights] as a compendious description of the entire body of private law which governs the relationships between subject and subject.” Hogg, *supra* note 104 at p. 21-2 to p. 21-3.

115. *Ibid.* at p. 21-3.

116. (1882), 7 App. Cas. 96.

117. Hogg, *supra* note 104 at p. 20-2.

Accordingly, if spam legislation can be characterized as being in pith and substance in relation to “trade and commerce,” then it is possible that the provinces would have the authority to regulate spam that is transmitted entirely within their provinces, while the federal government would have authority to regulate all other transmissions. It would seem that any proposed spam control regime targeting only unsolicited *commercial* emails might lend particular support to this “trade and commerce” characterization.

However, on balance, it is suggested that even a spam law targeting only commercial spam would more properly be regarded as an effort to regulate the manner in which entities communicate with each other over the internet (*i.e.* the focus is on securing consent), as opposed to the rules between contracting parties.

If correct, this would likely preclude the assertion of a federal “trade and commerce” power, given that this power has never been held to confer any federal authority over communications.¹¹⁸

5.2.3.2.2. Criminal Law (Section 91.27)

Section 91.27 of the *Constitution* provides the federal Parliament with power to make laws relating to “the criminal law.”¹¹⁹ To be within the realm of criminal law, case law suggests the law in question must prohibit with a penal consequence and “serve a public purpose which can support it as being in relation to the criminal law,” examples of which include “public peace, order, security, health and morality.”¹²⁰

These public purposes have been interpreted broadly, and as a result, Parliament has been given wide authority to regulate all things which would otherwise fall within “property and civil rights” in the provinces.¹²¹ For example, La Forest J (writing for the majority of the Supreme Court of Canada) commented in *RJR-MacDonald Inc. v. Canada (Attorney General)* that section 91.27 must assign Parliament exclusive jurisdiction over criminal law “in the widest sense of the term.”¹²² That said, the test for jurisdiction is whether the law is directed at “some evil or injurious or undesirable effect upon the public.”¹²³

118. Colin H. McNairn, “Transportation, Communications and the Constitution: The Scope of Federal Jurisdiction” (1969) 47 *Canadian Bar Review* 355.

119. The precise scope of this law-making authority proved difficult to define for some time. Lord Atkin stated the following in *Proprietary Articles Trade Assn. v. A.-G. Can.*, [1931] A.C. 310 (P.C.) at 324 [P.A.T.A.]: “The criminal quality of an act cannot be discerned by intuition; nor can it be discovered by reference to any standard but one: Is the act prohibited with penal consequences?” This definition, however, was criticized as being too broad in that it would enable Parliament to expand its jurisdiction indefinitely, simply by framing its legislation in the form of a prohibition coupled with a penalty. Hogg, *supra* note 104 at p. 18-4. Lord Atkin’s definition was supplanted in *Reference Re Validity of s. 5(a) of Dairy Industry Act (Canada)*, [1949] S.C.R. 1, (1949), 1 D.L.R. 433 [*Margarine Reference*], *aff’d* [1951] A.C. 179 (P.C.).

120. *Margarine Reference*, *ibid.*

121. Patrick Monahan, *Constitutional Law*, 2d ed. (Toronto: Irwin Law, 2002) at pp. 332-340.

122. [1995] 3 S.C.R. 199, (1995) 127 D.L.R. (4th) 1, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1995/vol3/html/1995scr3_0199.html> at para. 28 [*RJR-MacDonald*].

123. *Ibid.* La Forest J found that the *Tobacco Control Act* in question was directed at an evil, that evil being the detrimental health effects caused by tobacco consumption. Professor Monahan characterizes *RJR-MacDonald’s* approach as being “sweeping and plenary in nature.” See Monahan, *supra* note 121 at p. 333.

As discussed above, there are criminal and quasi-criminal aspects to practices of spammers, and no doubt section 91.27 would confer authority on Parliament to enact legislation pertaining to discrete issues such as fraudulent content or perhaps even deceptive practices such as “spoofing.”¹²⁴ However, and despite the breadth of Justice La Forest’s comments, it is suggested that section 91.27 likely would not support a more general spam law, targeted in pith and substance at all emails that are sent without recipients’ consent. It is difficult to understand how such concerns—absent fraudulent conduct—could be construed as an “evil” warranting criminal law jurisdiction.

5.2.3.2.3. POGG (opening words to Section 91)

Section 91 of the *Constitution* opens with the following residual conferral of power on the federal Parliament:

...to make Laws for the Peace, Order, and good Government of Canada, in relation to all Matters not coming within the Classes of Subjects...assigned exclusively to the Legislatures of the Provinces...¹²⁵

The modern statement of the federal POGG power was formulated by Viscount Simon in *Ontario (A.G.) v. Canada Temperance Federation* as follows:

... the true test must be found in the real subject-matter of the legislation: *if it is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole ... then it will fall within the competence of the Dominion Parliament* as a matter affecting the peace, order and good government of Canada, though it may in another aspect touch upon matters specially reserved to the provincial legislatures. [emphasis added]¹²⁶

Parliament’s residual POGG power is most often described as having three sub-branches of power:¹²⁷

1. A “gap” power to cover lapses in the division of powers scheme.
2. A power to deal with temporary “emergencies” such as war or apprehended insurrection.

124. See Part 1 above. Clearly, the percentage of spam that contains fraudulent or pornographic content may already be subject to regulation under existing provisions of the *Criminal Code*, *supra* note 49.

125. *Constitution*, *supra* note 17, s. 91. The POGG power is thought to be residual in its relationship to the provincial heads of power on the grounds that it grants the federal Parliament all powers not coming within the classes of subjects assigned exclusively to the provincial Legislatures. See Hogg, *supra* note 104 at p. 17-1 to p. 17-2.

126. [1946] A.C. 193 at 205, (1946), 2 D.L.R. 1 (PC) [*Canada Temperance Federation* cited to A.C.]. This case ultimately rejected Viscount Haldane’s earlier and more narrow characterization of POGG as only an emergency power. See *Re Board of Commerce Act, 1919, and Combines and Fair Prices Act, 1919*, [1922] 1 A.C. 191, (1921), 60 D.L.R. 513 (P.C.); *Toronto Electric Commissioners v. Snider*, [1925] A.C. 396, (1925), 2 D.L.R. 5 (PC).

127. See Hogg, *supra* note 104 at p.17-5 to p. 17-18.1; Monahan, *supra* note 121 at p. 256.

3. A “national concern” power to deal with matters, though of local origin, which are of sufficient concern to the entire country to warrant federal jurisdiction.

It is suggested that only the third branch, and not the first two, is deserving of examination in the context of this article.¹²⁸

5.2.3.2.3.1. *What is a Matter of “National Concern”?*

The most authoritative pronouncement from the Supreme Court of Canada as to the meaning of “national concern” POGG power is that of Le Dain J in *R. v. Crown Zellerbach Canada Ltd.*¹²⁹ In this case, “marine pollution” was found to be a matter of sufficient national concern to warrant federal authority because of its “predominantly extra-provincial [and] international character and implications.”¹³⁰

Le Dain J also laid down four propositions that he considered to have been “firmly established” by earlier case law:¹³¹

1. The national concern doctrine is separate and distinct from any national emergency doctrine of the POGG power.
2. The national concern doctrine applies both to new matters which did not exist at the time of Confederation as well as to matters which, though originally falling under provincial jurisdictions, have since become matters of national concern.¹³²
3. A matter must have “a singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern and a scale of impact on provincial jurisdiction that is reconcilable with the fundamental distribution of legislative power under the Constitution” to qualify as a matter of national concern.¹³³

128. For a fuller understanding of the likely non-applicability of the first two branches, see Hogg, *ibid.* at p. 17-5 to p. 17-31.

129. [1988] 1 S.C.R. 401, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol1/html/1988scr1_0401.html>, (1988), 49 D.L.R. (4th) 161 [*Crown Zellerbach* cited to S.C.R.].

130. *Ibid.* at p. 436.

131. *Ibid.* at pp. 431-436.

132. It would nevertheless appear that federal authority is more likely to be sustained in relation to novel matters where the provinces have not yet attempted to assert a regulatory presence. See e.g. *Johannesson v. West St. Paul*, [1952] 1 S.C.R. 292, (1951), 4 D.L.R. 609 [*Johannesson*] (aeronautics); *Reference Re Regulation & Control of Radio Communication in Canada*, [1932] A.C. 304, (1932), 2 D.L.R. 81 (P.C.) [*Re Radio*] (radio); *Ontario Hydro v. Ontario (Labour Relations Board)*, [1993] 3 S.C.R. 327, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1993/vol3/html/1993scr3_0327.html>, (1993), 107 D.L.R. (4th) 457 (nuclear energy). See also Monahan, *supra* note 121 at pp. 267-268.

133. See e.g. *Reference re: Anti-Inflation Act*, [1976] 2 S.C.R. 373 at 457-458, (1976), 68 D.L.R. (3d) 452 [*Anti-Inflation Reference* cited to S.C.R.], where Beetz J stated that “inflation” was too diffuse a concept to fall within POGG.

4. It is relevant to consider what the effect on extra-provincial interests would be of a failure of any province to deal effectively with the intra-provincial aspects of the matter.¹³⁴

In at least two important cases, the national concern branch of POGG has been found to support exclusive federal authority over important new technologies: "aeronautics" in one,¹³⁵ and "radio broadcasting" in another.¹³⁶ It is not difficult to imagine arguments by proponents of federal legislative competency to the effect that the internet is a matter of nation-wide importance justifying federal jurisdiction.¹³⁷

The question is complicated somewhat by the fact that at least one important scholar (Professor Hogg) has argued that Parliament should not be permitted to invoke the national concern branch of POGG unless the provinces, either acting alone or in combination, would be unable to regulate the matter effectively.

A full analysis as to whether the provinces would be unable to deal effectively with spam is beyond the scope of this article, although "provincial inability" might more likely arise where (as with spam) activities or harm may extend beyond the borders of a single province.¹³⁸ In any event, because spam pertains to a form of "communication," it is suggested that the foregoing POGG analysis is most likely only of secondary concern in light of the scope of the remaining federal head of power to be considered, which is discussed below.

5.2.3.2.4. Transportation and Communication (Subsection 92.10(a))

Subsection 92.10 is part of the enumeration of provincial powers and confers upon provincial Legislatures the power to make laws in relation to:

... local works and undertakings other than such as are of the following classes:

*Lines of Steam or other Ships, Railways, Canals, Telegraphs, and other Works and Undertakings connecting the Province with any other or others of the Provinces, or extending beyond the Limits of the Province...*¹³⁹

134. But note Hogg, *supra* note 104 at p. 17-12 to p. 17-14, who argues that provincial inability is a precondition that must be met for a matter to fall under "national concern."

135. *Johannesson*, *supra* note 132.

136. *Re Radio*, *supra* note 132, discussed in detail below.

137. Consider, for example, the claim that "the new [internet] economy has become the whole economy," concluded by the Canadian E-Business Opportunities Roundtable in Canadian E-Business Opportunities Roundtable, *Fast Forward 3.0: Maintaining the Momentum* (Ottawa: Canadian E-Business Opportunities Roundtable, 2002), <[http://tableronde.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/ff3.pdf/\\$FILE/ff3.pdf](http://tableronde.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/ff3.pdf/$FILE/ff3.pdf)> at p. 3. In the May 2003 report, the Canadian e-Business Initiative stated that over 60% of households in Canada were connected to the internet. Similarly, 93% of businesses with 20 or more employees were found to have used the internet in 2002. See Canadian e-Business Initiative, *Fast Forward 4.0: Growing Canada's Digital Economy* (May 2003), <<http://www.cebi.ca/Public/Team1/Docs/ff4.pdf>>.

138. *Supra* note 128.

139. *Constitution*, *supra* note 17, s. 92.10(a). [Emphasis added.]

Like all other listed exceptions from provincial power, these exceptions are deemed to be heads of exclusive federal legislative power by virtue of section 91.29, which includes those classes expressly exempt from provincial enumeration. As will be shown, the section 92.10 exceptions have been interpreted so as to confer undivided and unrestricted jurisdiction upon Parliament to regulate the facilities and communications of radio, television and telephone. Because of these decisions, it is suggested that a strong argument can be made that the federal Parliament would have exclusive jurisdiction to enact legislation targeting unsolicited email communications in Canada.

5.2.3.2.4.1. *The Facilities of Radio Communication*

The question of jurisdiction to regulate and control radio communication was put to the Privy Council on appeal from the Supreme Court of Canada in *Re Radio*.¹⁴⁰ Viscount Dunedin, writing for the Law Lords, affirmed that the entire undertaking of radio broadcasting fell within the exclusive sphere of federal power. That authority was stated to vest under *either* POGG (to facilitate giving national effect to treaty obligations recently undertaken by the federal government) or section 92.10(a).

Regarding the latter, it was noted that radio waves obey no borders (and thus can be considered inter-provincial). Viscount Dunedin then applied an extremely broad definition to the word “undertaking,” stating it “is not a physical thing but is an arrangement under which...physical things are used.”¹⁴¹ Under this definition, the Council had no doubt that the whole of the undertaking of radio fell within the meaning of an inter-provincial undertaking.¹⁴²

Although subsequent cases have attempted to narrow the scope of this definition, none have been successful.

5.2.3.2.4.2. *The Content of Radio Broadcasting*

The broad scope of federal authority as a result of the *Re Radio* decision was extended to include the content of radio broadcasting by the Ontario Court of Appeal’s decision in *Re C.F.R.B. and Canada (A.G.)*.¹⁴³ The issue before the Court of Appeal was whether *Re Radio* merely conferred exclusive federal authority over the facilities of broadcast communication, or whether it extended to include the content of broadcast communication as well.

The appellant argued that Viscount Dunedin’s definition of “undertaking” should be confined to physical equipment. The Court of Appeal was not persuaded, finding it to be:

140. *Supra* note 132.

141. *Ibid.* at p. 315.

142. Radio broadcasting was also considered to fall within the meaning of “telegraph”, which was defined as “an apparatus for transmitting messages to a distance, usually by signs of some kind.” *Ibid.* at p. 316.

143. [1973] 3 O.R. 819, (1973), 38 D.L.R. (3d) 335 (C.A.) [*Re CFRB* cited to O.R.].

...beyond doubt that...the whole of the undertaking of broadcasting is to be taken as within the exclusive field of Parliament as fully as if it had appeared in s. 91 as a separate head immediately after cl. 29.

...

[Moreover] it would be flying in the face of all practical considerations and logic to charge Parliament with the responsibility for the regulation and control of the carrier system and to deny it the right to exercise legislative control over what is the only reason for the existence of the carrier system, i.e., the transmission and reception of intellectual material.¹⁴⁴

5.2.3.2.4.3. Extension to Broadcast Television

Both *Re Radio* and *Re CRFB* concerned broadcasting technology in which information was communicated through radio waves travelling in the air, which obeyed no provincial borders. Subsequently, in *Capital Cities Communications v. Canadian Radio-Television and Telecommunications Commission*,¹⁴⁵ the Supreme Court of Canada determined that federal authority also extends to the regulation of the content of a cable re-transmission, occurring wholly within a province, of a television signal that originates from beyond the province.¹⁴⁶

Once again, the appellant in this case argued that *Re Radio* should be limited and not apply to circumstances where subscribers within a province are provided with signals sent through coaxial cable located entirely within the province. The Court (Laskin CJ for the majority) refused to narrow Viscount Dunedin's statements. The fact that a local distribution system transmits a signal originating extra-provincially means that the entire undertaking cannot be considered merely of a local nature.

Significantly, federal authority was found solely by virtue of subsection 92.10(a) in *Capital Cities*, without mention of an alternative POGG head of authority.¹⁴⁷

5.2.3.2.4.4. Extension to Telephone Communication

Finally, the case of *Alberta Government Telephones v. Canadian Radio-Television and Telecommunications Commission*¹⁴⁸ involved an entity created by an Alberta statute for the purpose of providing telephone communication services within that province. AGT's subscribers and physical equipment were located entirely within Alberta, although its equipment connected with the equipment of other communication companies at the Alberta border. Through this cooperating equipment, AGT was able to provide Albertans with telephone service to

144. *Ibid.* at p. 822 and p. 824.

145. [1978] 2 S.C.R. 141, (1977), 81 D.L.R. (3d) 609 [*Capital Cities* cited to S.C.R.].

146. *Ibid.* at p. 143.

147. As noted by Hogg, *supra* note 104 at pp. 22-26.

148. [1989] 2 S.C.R. 225, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1989/vol2/html/1989scr2_0225.html>, (1989), 61 D.L.R. (4th) 193 [AGT cited to S.C.R.].

anywhere in Canada as well as other parts of the world.¹⁴⁹

The Supreme Court began its analysis of legislative jurisdiction by confirming earlier case law that, under a subsection 92.10(a) analysis, the question of jurisdiction is an “all or nothing affair.” If a work or undertaking falls within subsection 92.10(a), then it is removed from the jurisdiction of the provinces, and that removal extends even to aspects of the undertaking which take place entirely within a province.¹⁵⁰

AGT attempted to argue that it was a local undertaking because it was located in Alberta, as was its equipment and subscribers. Once again, the Supreme Court refused to narrow the effect of *Re Radio*, focusing on the fact that AGT’s telecommunications system, taken as a whole, connected Alberta subscribers with the rest of Canada and other parts of the world.¹⁵¹

As a result of this case, all telephone operations that allow subscribers to send and receive inter-provincial or international communications, whether local or across provinces, fall exclusively within federal legislative competency.¹⁵²

5.2.3.3. Conclusions

It would appear that regardless of the technology employed, the medium in which information travels or is received, the location of physical equipment or the location of subscribers to a service, any undertaking which concerns an ability to communicate information to others beyond a provincial border can, arguably, be regulated only by the federal government under subsection 92.10(a). Moreover, once that jurisdiction is established, there is strong authority for the proposition that regulation extends to both the facilities as well as the content of communication.

If correct,¹⁵³ this analysis suggests that only the federal Parliament, and not each of the provincial Legislatures, is competent to enact spam legislation having a “pith and substance” that is substantially the same as has been characterized in this article.

149. *Ibid.* at pp. 243-244.

150. *Ibid.* at p. 257. See also *Ontario (A.G.) v. Winner*, [1954] A.C. 541, (1954) 4 D.L.R. 657 (PC); *Montreal (City of) v. Montreal Street Railway Co.*, [1912] A.C. 333, (1912), 1 D.L.R. 681 (PC).

151. AGT, *ibid.* at pp. 258-260.

152. Note, however, that AGT was ultimately found to be entitled to claim Crown immunity (*ibid.* at p. 301). This approach and analysis was affirmed by the Supreme Court of Canada more recently in *Téléphone Guèvremont Inc. v. Quebec (Régis des télécommunications)*, [1994] 1 S.C.R. 878, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1994/vol1/html/1994scr1_0878.html>, (1994), 112 D.L.R. (4th) 127 [*Téléphone Guèvremont* cited to S.C.R.]. Lamer CJC for the unanimous Supreme Court of Canada stated at p. 879:

We are all of the view that *Téléphone Guèvremont Inc.* is an interprovincial work and undertaking within the legislative authority of the Parliament of Canada by virtue of ss. 92(10)(a) and 91(29) of the *Constitution Act, 1867* by reason of the nature of the services provided and the mode of operation of the undertaking, which provides a telecommunication signal carrier service whereby its subscribers send and receive interprovincial and international communications...

153. There are two labour tribunals decisions which support the proposition that the internet falls within federal regulatory authority: *Re Island Telecom Inc.*, 2000 CIRB 59, <http://www.cirb-ccri.gc.ca/collections/publications/decisions/RD0059_b.pdf>, [2000] C.I.R.B.D. No. 12; *Re CITY-TV*, 1999 CIRB 22, <http://www.cirb-ccri.gc.ca/collections/publications/decisions/RD0022_b.pdf>, [1999] C.I.R.B.D. No. 22.

However, it is important to bear in mind that this exclusive federal authority would likely continue to be exercised “concurrently” with provincial power over “property and civil rights” in the provinces. For that reason, the provinces would likely remain competent to enact general legislation over provincial matters (e.g. defamation, commercial trade or advertising) which had an impact on internet communications, so long as regulation of the internet was not its dominant purpose.

For example, in *Irwin Toy Ltd. v. Québec (A.G.)*,¹⁵⁴ the Supreme Court of Canada found a Quebec statute regulating advertising to minors (including television advertising) was valid provincially, even though television broadcasting falls within federal regulatory authority.¹⁵⁵ The Quebec law was “in relation to” advertising within the province, although it had an “effect” on television.¹⁵⁶ The same might apply to many provincial laws which touch upon aspects of internet communications, so long as they do not purport to do so.

Having just considered the potential impact of federalism on a Canadian spam regime, the following section of this article proceeds to consider the equally important question of the impact of subsection 2(b) of the *Charter*.

★

6. SPAM LAWS AND SUBSECTION 2(B) OF THE CHARTER: A DEMONSTRABLY JUSTIFIED LIMITATION?

REGARDLESS OF WHETHER the regulation of spam falls with the authority of the federal Parliament or provincial Legislatures, in drafting any model of regulation, either level of government will have to bear in mind the supremacy of the *Charter* and the eminence of subsection 2(b), which guarantees everyone in Canada “freedom of expression.”

This section begins with an overview of the Canadian approach to freedom of expression and contrasts it with the approach taken in the United States. It then shifts to an analysis of whether spam communications can be considered a form of “expression” within the meaning of subsection 2(b) of the *Charter*. Thereafter, it considers the related issue of whether the regulation of spam involves a violation of that subsection. Finally, it considers the likelihood that a court would find any of the spam regulatory models discussed earlier to be a “demonstrably justified” limitation on subsection 2(b), under section 1 of the *Charter*.

154. [1989] 1 S.C.R. 927, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1989/vol1/html/1989scr1_0927.html>, (1989), 58 D.L.R. (4th) 577 [*Irwin Toy* cited to S.C.R.] at p. 930.

155. *Ibid.* at pp. 957-958.

156. *Ibid.* at p. 953.

6.1. Overview of Canada's Approach to Freedom of Expression

Freedom of expression, as a principle, pre-dates the *Charter*.¹⁵⁷ It has been called "the matrix, the indispensable condition of nearly every other form of freedom,"¹⁵⁸ and "little less vital to man's mind and spirit than breathing is to his physical existence."¹⁵⁹ Nevertheless, the history of *Charter* adjudication has demonstrated that freedom of expression is not absolute and must at times be reconciled against competing social objectives.

The US approach to this challenge is to grant a near absolute level of protection for expression deemed worthy of constitutional safeguarding, but to define such expression very narrowly.¹⁶⁰ In contrast, and perhaps owing to the availability of a section 1 analysis,¹⁶¹ the Supreme Court of Canada has stated that freedom of expression is to be given a virtually unlimited interpretation.¹⁶²

The full meaning of freedom of expression came to a head in Canada in 1988, when the Supreme Court heard two cases (*Ford* and *Irwin Toy*)¹⁶³ that have since established the approach of our courts. Both cases involved commercial advertising. *Ford* involved a challenge to a Quebec sign law that prohibited the display of any commercial signs not written in French.¹⁶⁴ The Attorney General for Quebec argued (in analogy to the US approach) that "commercial expression" is not within the core of expression intended to be protected by subsection 2(b). The Supreme Court rejected that limitation, stating that "there is no sound basis on which commercial expression can be excluded from the protection of subsection 2(b) of the *Charter*."¹⁶⁵ Rather, it found the concept embraced nearly all expressive human conduct.¹⁶⁶

157. Though rights such as freedom of expression have been enshrined in the *Charter*, such rights and freedoms did not spring from a vacuum in 1982. See e.g. *R. v. Big M Drug Mart Ltd.*, [1985] 1 S.C.R. 295, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1985/vol1/html/1985scr1_0295.html>, (1985), 18 D.L.R. (4th) 321; *Reference Re Provincial Electoral Boundaries (Saskatchewan)*, [1991] 2 S.C.R. 158, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1991/vol2/html/1991scr2_0158.html>, (1991), 81 D.L.R. (4th) 16.

158. *Palko v. Connecticut*, 302 U.S. 319, <<http://www.justia.us/us/302/319/case.html>> at p. 327, 58 S. Ct. 149 (1937) [*Palko* cited to U.S.], per Cardozo J.

159. *Switzman v. Elbling*, [1957] S.C.R. 285 at p. 306, (1957), 7 D.L.R. (2d) 337 [*Switzman* cited to S.C.R.], per Rand J.

160. See also Monahan, *supra* note 121 at p. 127.

161. Hogg, *supra* note 104, vol. 2 at p. 40-7.

162. See Robert J. Sharpe, Katherine E. Swinton & Kent Roach, *The Charter of Rights and Freedoms*, 2d ed. (Toronto: Irwin Law, 2002) at p. 127.

163. See *Ford v. Quebec (A.G.)*, [1988] 2 S.C.R. 712, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol2/html/1988scr2_0712.html>, (1988), 54 D.L.R. (4th) 577 [*Ford*]; *Irwin Toy*, *supra* note 154. The *Ford* decision resolved contradictory decisions by other Canadian courts on whether commercial expression qualifies for s. 2(b) protection under the *Charter*: contrasted with *Re Klein and Law Society of Upper Canada* (1985), 50 O.R. (2d) 118, (1985), 16 D.L.R. (4th) 489 (Div Ct) (excluding commercial expression from the *Charter* guarantee) and the Ontario Court of Appeal in *Rocket v. Royal College of Dental Surgeons of Ontario* (1988), 64 O.R. (2d) 353, (1988), 49 D.L.R. (4th) 641 (where this court reached an opposite conclusion).

164. Specifically, certain provisions of Quebec's *Charter of the French Language*, R.S.Q. 1977, c. C-11, <http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_11/C11_A.html>, were at issue.

165. *Ford*, *supra* note 163 at p. 767.

166. *Ibid.* at p. 716; and at p. 755, the Court suggested that the term "commercial expression" has no particular meaning or significance in Canadian constitutional law, unlike the corresponding "commercial speech" doctrine in the US. See also Allan C. Hutchinson, "Money Talk: Against Constitutionalizing (Commercial) Speech" (1990) 17 Canadian Business Law Journal 2. For a contrasting perspective, see Robert J. Sharpe, "Allan Hutchinson's 'Money Talk: Against Constitutionalizing Commercial Speech'" (1990) 17 Canadian Business Law Journal 35 at p. 39.

Argued just after *Ford*, *Irwin Toy* involved a challenge to Quebec's *Consumer Protection Act* which restricted advertising aimed at children.¹⁶⁷ Following substantially the same arguments as in *Ford*, the Supreme Court took the opportunity in *Irwin Toy* to lay out the applicable subsection 2(b) interpretive framework:¹⁶⁸

First, a court must determine if the party raising a subsection 2(b) claim is engaged in a protected form of expression.

If so, the court must then consider whether either the purpose or the effect of the impugned law is to limit that expression.

The following sections will apply this interpretative framework on the assumption that spam legislation of one form or another will eventually be considered in Canada.

6.2. Is Spam a Form of Protected "Expression"?

At the first stage of a subsection 2(b) analysis, a court must consider whether the conduct at issue constitutes protected expression. The applicable test is to ask whether the activity (which extends to both speech and conduct) conveys or attempts to convey a meaning.¹⁶⁹ With the exception of violent conduct,¹⁷⁰ if this question is answered in the affirmative, then the expression is protected under subsection 2(b). Given the breadth of this definition, nearly all forms of communication will qualify.¹⁷¹

For the purpose of the analysis herein, it is suggested that any court in Canada would likely consider all email communication, regardless of content, an "activity" that "conveys or attempts to convey a meaning."¹⁷²

167. S.Q. 1978, c. 9, as rep. by *Consumer Protection Act*, R.S.Q. 1980, c. P-40.1, <http://www2.publications.duquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FP40_1%2FP40_1_A.htm>.

168. *Irwin Toy*, *supra* note 154.

169. *Ibid.*

170. *Ibid.* at p. 970.

171. Subsequent cases confirmed that in addition to commercial expression, hate speech, deliberate lies and pornography are protected. See *R. v. Keegstra*, [1990] 3 S.C.R. 697 at 760, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol3/html/1990scr3_0697.html>, (1991), 2 W.W.R. 1 [Keegstra cited to S.C.R.] (hate speech); *R. v. Zundel*, [1992] 2 S.C.R. 731, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1992/vol2/html/1992scr2_0731.html>, (1992), 95 D.L.R. (4th) 202 (deliberate lies); *R. v. Butler*, [1992] 1 S.C.R. 452, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1992/vol1/html/1992scr1_0452.html>, (1992), 89 D.L.R. (4th) 449 [Butler] (pornography).

172. However, content-based issues which arise from deceptive or fraudulent spam practices may become relevant at a later stage of analysis.

6.3. Would Spam Legislation Violate Subsection 2(b)?

At the second stage of subsection 2(b) analysis, a court would be asked to determine whether the purpose or effect of the law in question is to limit protected expression.¹⁷³ Once again, it would appear exceedingly likely that any court would find spam laws to have as their purpose or effect the restriction of one or more forms of spam communication.

Any law that prohibits email from being sent without prior (or deemed) recipient consent necessarily restricts spammers' ability to communicate their messages to non-consenting recipients. Even a law which does nothing more than require that all email be sent with a valid return address and an accurate subject line would still prohibit non-conforming email.¹⁷⁴

Accordingly, it is suggested that any spam law drawing inspiration from the models reviewed earlier would very likely be found to violate subsection 2(b) of the *Charter* and require saving under a section 1 *Charter* analysis.

6.4. Analysis Under Section 1 of the Charter

As noted above, our courts have developed a framework for *Charter* adjudication that involves a broad definition of *Charter* rights, leaving the limitation of such rights to be determined under a section 1 analysis.¹⁷⁵ Section 1 states that the *Charter*:

...guarantees the rights and freedoms set out in it *subject to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.* [Emphasis added]

The test for saving an otherwise unconstitutional law under section 1 was laid down in the well-known case of *Oakes*,¹⁷⁶ and can be thought of as having the following elements:

First, the court is to consider whether the objective of the law relates to "concerns which are pressing and substantial in a free and democratic society," sufficient to warrant overriding a *Charter* right.

173. *Irwin Toy*, *supra* note 154. The effects test is completed in light of the principles and values underlying freedom of expression: a) as being essential to intelligent and democratic self-government; b) protects an open exchange of views, thereby creating a competitive marketplace of ideas; c) to value expression for its own sake. See Robert J. Sharpe, "Commercial Expression and the Charter" (1987) 37 *University of Toronto Law Journal* 229 at p. 232 [Sharpe, "Commercial Expression"]; Thomas I. Emerson, "Toward a General Theory of the First Amendment" (1963) 72 *Yale Law Journal* 877 at p. 878.

174. For example, in *Ford*, *supra* note 163, the law at issue prohibited signs not written in French. The Attorney General of Québec argued that advertisers could still communicate any message they wanted, as long as they did so in French. However, the court found that the requirement of exclusive use of French was necessarily a prohibition on the use of any other language, and therefore a violation of s. 2(b).

175. See generally John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (Cambridge: Harvard University Press, 1980); Patrick Monahan, *Politics and the Constitution: The Charter, Federalism and the Supreme Court of Canada* (Toronto: Carswell, 1987); Roland Penner, "The Canadian Experience with the Charter of Rights: Are there Lessons for the United Kingdom?" (1996) *Public Law* 104 at pp. 114-115.

176. *R. v. Oakes*, [1986] 1 S.C.R. 103, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1986/vol1/html/1986scr1_0103.html>, (1986), 26 D.L.R. (4th) 200 [Oakes]. The *Oakes* test is similar to the test established in the US for permitting restrictions on commercial speech. See *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557, 65 L. Ed. 2d 341 (1980) [Central Hudson].

If so, the court will next undertake a three-part “proportionality” exercise, asking in turn:

- whether there is a “rational connection” between the law and the legislative objective;
- whether the law limits the right at issue to no greater an extent than is necessary to accomplish the government objective; and
- whether there is otherwise a proportionality between the government objective and the deleterious effects of the law.¹⁷⁷

6.4.1. The Burden on the State

While the language of section 1 could be construed as imposing a heavy burden on the state in attempting to justify otherwise unconstitutional legislation, the Supreme Court has mandated that a contextual approach is to be taken and a fair degree of deference is to be shown to law makers.¹⁷⁸ This approach has come to be described as offering law makers “a zone of discretion” or a “margin of appreciation.”¹⁷⁹ Nevertheless, it has been noted that of all *Charter* rights, this margin of appreciation is at its narrowest when considering a violation of subsection 2(b).¹⁸⁰ As will be reviewed below, it also appears that the margin of appreciation extended to lawmakers varies depending on the class of expression being restricted.

6.4.2. Pressing and Substantial Objective

It is not a simple task for a court to identify the objective of a challenged law and any governmental purpose can be expressed with either generality or specificity. Defining a law’s objective broadly (e.g. “improving the safety of Canadians”) naturally tends to increase the likelihood that the objective will pass a “pressing objective” test. However, this same broad characterization has an opposite effect in later section 1 analysis, in that it tends to make it less difficult for a court to envision a “less restrictive” alternative for the government to have adopted. In contrast, the government’s minimal impairment argument may become very persuasive when the law’s objective is defined narrowly (e.g. “decreasing wasted internet bandwidth in Canada”), although this tends to make the objective itself

177 Of these criteria, experience suggests that it is nearly always the “least drastic means” inquiry which is at the centre of the debate. See Peter W. Hogg & Allison A. Bushell, “The *Charter* Dialogue Between Courts and Legislatures (or Perhaps the *Charter* of Rights Isn’t Such a Bad Thing After All)” (1997) 35 *Osgoode Hall L.J.* 75 at p. 85 [Hogg, “*Charter* Dialogue”].

178. See e.g. *Rocket v. Royal College of Dental Surgeons of Ontario*, [1990] 2 S.C.R. 232 at pp. 246-247, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol2/html/1990scr2_0232.html>, (1990), 71 D.L.R. (4th) 68 [Rocket cited to S.C.R.]. This approach has been subjected to academic criticism. See Keith Dubick, “Commercial Expression: A ‘Second-Class’ Freedom?” (1996) 60 *Saskatchewan Law Review* 91; Christopher D. Bredt & Adam M. Dodek, “The Increasing Irrelevance of Section 1 of the *Charter*” (2001) 14 *Supreme Court Law Review* (2d) 175 [Bredt]; Richard Moon, “Justified Limits on Free Expression: The Collapse of the General Approach to Limits on *Charter* Rights” (2002) 40 *Osgoode Hall Law Journal* 337.

179. See Hogg, *supra* note 104, vol. 2 at p. 35; *Irwin Toy*, *supra* note 154 at p. 999.

180. Bredt, *supra* note 178.

appear less constitutionally substantial.¹⁸¹

Bearing this in mind, the Supreme Court has stated that an impugned law's objective is to be defined in relation to the *Charter* infringement at issue, rather than in relation to other goals. A statement of the law's objective should therefore answer the question: *Why was the Charter right infringed?*¹⁸²

Any proposed spam regulation could have several policy objectives. For example, it could be characterized narrowly as seeking to decrease wasted bandwidth in Canada. Perhaps at its broadest, it could be said to be intended to "make the internet more secure, efficient and economical in Canada." However, I suggest the "pith and substance" characterization of spam laws provided earlier remains a reasonable statement of government objective; namely: *to protect the rights of recipients not to receive email (either all or those of a limited class) against their wishes, and to prescribe the circumstances in which recipient consent can reasonably be presumed to exist.*

Proceeding on the assumption that this represents a reasonable statement of objective, the question becomes whether this objective is constitutionally "pressing and substantial." For the following reasons, I believe a court would most likely answer that question in the affirmative:

First, a court would likely have regard for the fact that spam regulation is considered important in several other countries such as the United States, the European Union and Australia.¹⁸³ An argument can be raised that, without spam legislation, Canada risks being seen as an international haven for spammers.

There is also support in US case law and journals for the proposition that the state has a substantial interest in restricting unsolicited facsimile advertisements (in order to prevent cost shifting and other interference to recipients).¹⁸⁴ These arguments could be analogized in the context of spam, including in the Canadian context.

Finally, Canadian courts tend to show deference to government action at this initial stage of analysis and, therefore, rarely conclude that a law's objective is constitutionally insubstantial.¹⁸⁵

For these reasons, it is suggested a court would most likely find that any proposed spam regime model has a "pressing and substantial" objective, necessitating a review of its overall "proportionality."

181. See Hogg, *supra* note 104, vol. 2 at p. 35-18.

182. *RJR-MacDonald*, *supra* note 122 at p. 204.

183. See "Declaring a World War on Spam" *Wired.com* (1 July 2003), <<http://www.wired.com/news/politics/0,1283,59459,00.html>>.

184. *Missouri ex rel. Nixon v. American Blast Fax, Inc.*, 323 F. 3d 649 (8th Cir 2003); *Destination Ventures v. FCC*, 46 F. 3d 54 at 57 (9th Cir 1995); David Sorkin, "Unsolicited Commercial E-mail and the Telephone Consumer Protection Act of 1991" (1997) 45 *Buffalo Law Review* 1001 at p. 1013, <<http://www.sorkin.org/articles/buffaloarticle.html>>.

185. Monahan, *supra* note 121 at p. 62.

6.4.3. Proportionality Analysis

6.4.3.1. The “Rational Connection” Branch

At the first stage in a proportionality examination, a court would be required to satisfy itself that there is a rational, non-arbitrary, non-capricious connection between the legislative objective in question and the law that is challenged.¹⁸⁶

It is very rare for a court to find an absence of any rational connection because there is no requirement for the government to establish this connection by way of scientific proof. For example, in *RJR-MacDonald* the Supreme Court found a rational connection existed between limits on tobacco advertising and the objective of reducing tobacco use, even though the evidence of a link between the two was “inconclusive.”¹⁸⁷

Once again, it is suggested that spam legislation would pass this threshold and thus the applicable section 1 analysis would continue.

6.4.3.2. The “Minimal Impairment” Branch

The question of minimal impairment is considered to be one of the “core elements” of the overall proportionality review.¹⁸⁸ Originally in *Oakes*, Dickson CJ had written for the Supreme Court that the onus on the government was to demonstrate that its law impaired the right at issue “as little as possible.”¹⁸⁹ However, the Chief Justice refined his language shortly thereafter, re-stating the test to require the government to establish only that its law limits the freedom at issue “as little as is reasonably possible.”¹⁹⁰

In relation to subsection 2(b) decisions, the case law suggests that a different standard of reasonableness may apply depending on the expression at issue. It seems that the closer the expression at issue comes to the courts’ understanding of the “core” meaning of freedom of expression, the higher the degree of scrutiny to which any restriction will be subjected.¹⁹¹

The Supreme Court of Canada recently summarized the core values promoted by free expression as including “self-fulfilment, participation in social and political decision-making, and the communal exchange of ideas.”¹⁹² This statement accords with earlier decisions in which laws restricting expression with

186. The standard is low and the rational connection test is used largely to prevent the attempted justification of laws based on discriminatory assumptions. Monahan, *ibid.* at p. 64.

187. *RJR-MacDonald*, *supra* note 122 at p. 207.

188. Hogg, “Charter Dialogue,” *supra* note 177.

189. *Oakes*, *supra* note 176 at p. 139.

190. *R. v. Edwards Books and Art Ltd.*, [1986] 2 S.C.R. 713 at p. 772, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1986/vol2/html/1986scr2_0713.html>, (1986), 35 D.L.R. (4th) 1 [Edwards cited to S.C.R.].

191. See Dubick, *supra* note 178; Neil Finkelstein, “Section 1: The Standard for Assessing Restrictive Government Actions and the Charter’s Code of Procedure and Evidence” (1983) 9 Queen’s L.J. 143 at p. 169; Sharpe, “Commercial Expression,” *supra* note 173.

192. *Retail, Wholesale and Department Store Union, Local 558 v. Pepsi-Cola Canada Beverages (West) Ltd.*, 2002 SCC 8, <http://www.lexum.umontreal.ca/csc-scc/en/pub/2002/vol1/html/2002scr1_0156.html>, [2002] 1 S.C.R. 156 at para. 32.

low social utility (such as hate speech)¹⁹³ were saved more often than laws restricting “core” speech, such as political expression.¹⁹⁴

The Supreme Court has decided a number of cases regarding commercial speech,¹⁹⁵ the results of which make it difficult to discern any bright lines of analysis. The early cases of *Ford* and *Irwin Toy* both involved challenges to Quebec advertising laws and, in both cases, the commercial speech at issue was found to be “expression” protected by subsection 2(b). However, different results were reached in those cases under section 1.

The law in *Ford* was not saved by section 1. It involved a near total ban on all signs written in a language other than French. The Supreme Court found that this ban went further than was necessary to protect and enhance the French language.¹⁹⁶ In contrast, the law in *Irwin Toy* was saved under section 1. It prohibited commercial advertising from being directed at persons under the age of 13. Therefore, while this law also involved a ban, it was more targeted and directed than the limitation at issue in *Ford*.¹⁹⁷

From these and other decisions,¹⁹⁸ it appears that commercial expression is considered to occupy a middle-ground in the hierarchy of protected expression.¹⁹⁹ Overt commercial solicitation is not considered to lie at the core of the guarantee of freedom of expression,²⁰⁰ but total bans may not be upheld as minimal impairments.²⁰¹ In contrast, section 1 may be permitted to save an otherwise unconstitutional restriction on commercial expression if the government has focussed its efforts as reasonably as possible in the circumstances.

6.4.3.2.1. Minimal Impairment Analysis Applied in the Context of Spam

As discussed, international models of spam regulation attempt to deal with spam, broadly speaking, in two ways:

-
193. See *Keegstra*, *supra* note 172 (hate speech), where the majority Supreme Court concluded that the minimal impairment test was to be applied less rigorously in connection with this class of speech. See also *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol3/html/1990scr3_0892.html>, (1990), 75 D.L.R. (4th) 577.
194. See e.g. *Thomson Newspapers Co. (c.o.b. Globe and Mail) v. Canada (A.G.)*, [1998] 1 S.C.R. 877, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1998/vol1/html/1998scr1_0877.html>, (1997), 38 O.R. (3d) 735.
195. A commercial expression has been defined as “... one which has as its purpose the proposal of an economic transaction. See Sharpe, “Commercial Expression”, *supra* note 173 at p. 230. In *Ford*, *supra* note 163 at p. 756, the Supreme Court of Canada defined the commercial speech doctrine as “business advertising which merely solicits a commercial transaction.”
196. For example, it was suggested that a law which permitted other languages in advertising so long as French was also included might be a reasonable limitation. *Ford*, *supra* note 163 at pp. 779-780.
197. It was also aimed at protecting a vulnerable group (children), which could not be said about the legislation in *Ford*.
198. See e.g. *Rocket*, *supra* note 178; *RJR-MacDonald*, *supra* note 122.
199. Dubick, *supra* note 178 at p. 92.
200. *Reference re ss. 193 and 195.1(1)(c) of the Criminal Code (Canada)*, [1990] 1 S.C.R. 1123 at p. 1136, <http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol1/html/1990scr1_1123.html>, (1990), 109 N.R. 81 [*Prostitution Reference* cited to S.C.R.].
201. See e.g. *Rocket*, *supra* note 178.

First, by mandating that spammers receive recipients' consent before sending an email (adopting either an "opt-in" or an "opt-out" model of obtaining consent).

Second, by mandating that spammers provide their recipients with a valid return address and an accurate subject line description of the nature of their email.

Arguably, the latter measure should be considered a lesser restriction on spammers' actions than the former, because under it spammers would remain free to send any emails they wished, so long as they met the mandated standards of truth and accuracy.²⁰² However, it is equally arguable that such regulations may not, by themselves, have the desired impact on spam in Canada.

For example, while such measures should make it easier for spam to be blocked by filtering technologies (e.g. by targeting messages with the word "Advertisement" in the subject line), filtering software offer imperfect solutions. They sometimes catch emails that recipients would rather have passed through, meaning an expensive process of review and sorting still remains.²⁰³ These costs would ultimately continue to be borne by ISPs and their customers.²⁰⁴ Moreover, as long as some percentage of spam is able to bypass whatever filters exist, it is conceivable spammers will find a way to make a profit and also torment recipients.

6.4.3.2.2. Mandating Consent

It is suggested, therefore, that any effective form of spam legislation must include some requirement of recipient consent as part of its overall scheme.²⁰⁵ The constitutional question therefore becomes how to balance the recipient's right not to receive spam against the spammer's freedom of expression.

Here it is suggested that the government must recognize that all spam is not created equal. Any proposed legislation should be drafted to avoid encroaching on forms of expression touching on core social values, meaning that such legislation should be limited to regulating unsolicited *commercial* email,²⁰⁶ as opposed to all unsolicited emails in general.²⁰⁷ It is suggested that a very fair

202. Only communications that had been falsified in relevant respects would be prohibited.

203. Indeed, increasingly broad filtering techniques run the risk of generating an unacceptably high percentage of false positives (legitimate emails that are blocked or deleted as filters incorrectly identify the email as spam) and blocking of legitimate unsolicited emails from known sources. See *supra* note 51.

204. Similarly, accurate return addresses may allow recipients to reply directly to spammers to vent frustration (perhaps in a concerted way) and to locate spammers to sue them. Spammers, however, may simply switch ISPs routinely.

205. Recognition of the right of recipients to determine which emails they receive seems to be a primary motivating factor in most proposed anti-spam measures. See e.g. Anti-Spam Bill of 2003, *supra* note 89, s. 2.

206. For the purpose of this discussion, commercial is meant to include distasteful commercial email such as pornography and fraud. While the government could further narrow its efforts by focusing on commercial spam which also contains pornographic or fraudulent content, it is suggested that such a law would be too focused to have the impact that is needed.

207. Though arguably a more effective method of combating spam, efforts to ban all unsolicited emails runs the risk of catching expression which is considered to be at the core of s. 2(b) protection (i.e. political, religious or social in nature).

argument can be made that it is commercial spam which causes most of the problems discussed earlier,²⁰⁸ and also that the foregoing regulation schemes are reasonably necessary in the circumstances to address it. The idea that the problem of spam cannot be addressed other than by mandating some form of recipient consent is also consistent with approaches taken most often in other countries.²⁰⁹

Bearing these factors in mind, it is suggested the final question for a court to consider would be whether there is overall proportionality between the effect of this proposed spam model (which targets commercial spam) and the public benefit of the objectives sought.

6.4.3.3. The "Overall Proportionality" Branch

The following passage represents the seminal statement by the Supreme Court of Canada, in *Oakes*, as to the context of this final branch of proportionality:

Some limits on rights and freedoms protected by the Charter will be more serious than others in terms of the nature of the right or freedom violated, the extent of the violation, and the degree to which the measures which impose the limit trench upon the integral principles of a free and democratic society. Even if an objective is of sufficient importance, and the first two elements of the proportionality test are satisfied, it is still possible that, because of the severity of the deleterious effects of a measure on individuals or groups, the measure will not be justified by the purposes it is intended to serve. *The more severe the deleterious effects of a measure, the more important the objective must be if the measure is to be reasonable and demonstrably justified in a free and democratic society.*²¹⁰

In other words, at the end of the day, there must also be proportionality between the effects of the Charter limitation and the government objective, which is a highly contextual investigation.

What are the deleterious effects of our proposed law? Clearly, it is to reduce the ability of corporations and spammers to communicate even genuine and legitimate commercial messages. Can it be said that the circumstances of spam are exceptional enough to justify this regulation?

I believe a fair argument can be made that the circumstances surrounding spam are, in fact, sufficiently exceptional. As discussed earlier, spam reverses the normal cost burden of advertising, placing that burden on recipients rather than spammers.²¹¹ A spammer's right to freedom of expression should not

208. 2003 Spam Paper, *supra* note 4.

209. See e.g. European Directive, *supra* note 28. All bills in the US also propose to address commercial spam (whether in bulk or not). *Supra* note 89. To the knowledge of this author, there are no proposed models that broadly prohibit all forms of unsolicited email. See also Steven Miller, "Washington's 'Spam-Killing' Statute: Does it Slaughter Privacy in the Process?" (1999) 74 Washington Law Review 453.

210. As *per* Dickson, C. in *Oakes*, *supra* note 176 at pp. 139-140. [Emphasis added.]

211. See Part 2 above, "Overview of the Rise of Spam, its Problems and its Costs."

include the right to force Canadians to pay to read it.²¹² Moreover, because spam contains a higher percentage of questionable content than traditional advertising, the spam industry has the potential to undermine consumer confidence in the internet as a whole.²¹³

Contextually, I believe it is also important to bear in mind that the act of spamming does not involve expressive conduct taking place on public property or on a spammers' private property. It involves unsolicited communication that is transmitted onto or into another's property—their computer. In this way, spam can be analogized to an uninvited guest who attempts to exercise freedom of expression in someone else's home. The following statement from the US Supreme Court appears apt:

The basic issue in this case is whether respondents, in the exercise of asserted [freedom of expression] rights, may distribute handbills on Lloyd's private property contrary to its wishes....

...

Although...the courts properly have shown a special solicitude for the guarantees of [freedom of expression], this Court has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.²¹⁴

6.5. Charter Summary

Admittedly, the foregoing discussion has been largely theoretical. Nevertheless, it may reasonably be assumed that any Canadian anti-spam legislative model would find substantial inspiration in the models proposed elsewhere. In regard to those models, a likely conclusion is that a court would consider any such regimes to violate subsection 2(b) of the *Charter*, requiring justification under section 1.

Assuming that a contextual analysis is applied, I believe a fair argument can be made that legislation directed at commercial spam that is sent without recipient consent may be saved as a reasonable limitation under the applicable section 1 analysis, bearing in mind that the problems of spam require prohibition measures and also that commercial expression does not lie within the core of expression protected by subsection 2(b) of the *Charter*.

212. Dianne Plunkett Latham, "Electronic Commerce in the 21st Century: Article Spam Remedies" (2001) 27 *William & Mitchell Law Review* 1649 at p. 1658. As discussed above, this is particularly true in the context of devices for which users pay a fee based on content downloaded. *Supra* note 35, see also discussion in Part 2.2.1 above.

213. See e.g. FTC Study, *supra* note 5.

214. *Lloyd Corp. v. Tanner*, 407 U.S. 551 at 567-568, 33 L. Ed. 2d 131 at 142 (1972), *per* Powell J (also cited as introductory quote at beginning of this paper).

★

7. CONCLUSIONS AND SUGGESTIONS FOR A MODEL CANADIAN LAW

THE PROSPECT OF SPAM LEGISLATION in Canada raises an interesting and complicated division of powers issue, and history has indicated that new means of communication usually give rise to important litigation over constitutional jurisdiction. I have concluded that a court seized with the issue of regulatory authority over the facilities and content of internet communication would most likely determine both to be within the sphere of exclusive federal competency, pursuant to subsection 92.10(a) of the *Constitution*. Nevertheless, the efforts of the provincial Legislatures to regulate “property and civil rights” in their provinces may be permitted to have a “concurrent” impact on internet communications.

As spam legislation very likely represents a limitation on spammers’ freedom of expression, several challenging issues of *Charter* analysis have also been raised. I have concluded it may be possible to conceive of an effective model of spam legislation which also represents a demonstrably justified limitation on subsection 2(b), able to be saved by section 1 of the *Charter*.

7.1. Model Law Checklist

Bearing in mind the entirety of the foregoing analysis, this article ends by suggesting a checklist of elements that a model Canadian spam law should include to address the constitutional and other practical issues noted above. These suggestions are offered with recognition of the fact that spam is a worldwide problem that needs to be pursued through as many domestic and international enforcement mechanisms as possible.

7.1.1. Constitutional Issues

The law should be directed at “commercial” spam, with “commercial” being defined so as to ensure that the law would not act as a limitation on communication that is at or near the core of the concept of freedom of expression.

The law should be enacted by the federal Parliament and not the provincial Legislatures.

7.1.2. Practical Issues

The law should mandate that entities who transmit commercial email first acquire recipient consent. Either an opt-in or an opt-out model could be considered. Canada should begin this policy debate quickly, but with an awareness of international developments so that some measure of international harmony and consistency is achieved.²¹⁵

Recipient consent should be obtained genuinely. Accordingly, the law should also mandate that commercial spam:

- be sent with a valid and undisguised return address; and
- clearly identify itself to recipients as a “Commercial Advertisement” or else provide such other description as the law may be deemed appropriate.

Other practices such as “spoofing” and “hijacking” may also be addressed, or perhaps could be dealt with as amendments to the *Criminal Code*.

The law should allow violators to be pursued by both the appropriate government agency and by private parties (ISPs and recipients) through civil actions.

The law should contain provisions intended to make it easier, quicker and less expensive for private parties to pursue spammers in the civil courts. The following suggestions are offered:

Summary applications should be readily available (instead of actions) to minimize the costs of litigation.

The applicant should have the burden only of establishing that it received a commercial email. The spammer should then have the evidential burden to prove that it had acquired whatever level of recipient consent is mandated by the law.

Parties should be able to recover damages for any actual loss suffered. In addition, a regime of “statutory damages” should be available, in which a non-nominal sum is awardable without proof

215. For example, the US has signed a Memorandum of Understanding dealing with cooperative enforcement assistance in matters dealing with spam with Australia and the United Kingdom. See *Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters*, United States, United Kingdom and Australia, 2 July 2004, <<http://www.ftc.gov/os/2004/07/040630spammoutext.pdf>>. Australia has also signed a Memorandum of Understanding with Korea and Thailand. See respectively *Memorandum of Understanding Concerning Cooperation in the Regulation of Spam*, Australia and Korea, 20 October 2003, <http://www.dcita.gov.au/ie/spam_home/spam_international/korea_mou> and *Joint Statement Concerning Cooperation in the Fields of Telecommunications and Information Technology*, Australia and Thailand, 5 July 2004, <http://www.dcita.gov.au/__data/assets/pdf_file/21621/MOU-joint-statement_thailand_final.pdf>. Such statements of bilateral or trilateral cooperation may mean increased pressure to harmonize legislation, with international recognition of the importance of global cooperation and regulation of spam.

216. For example, see the statutory damages regime encapsulated in *Copyright Act*, R.S. 1985, c. C-42, <<http://laws.justice.gc.ca/en/C-42/text.html>>, s. 38.1.

of actual loss.²¹⁶ Such award might be multiplied for each unsolicited spam email received from the same entity.²¹⁷

Broad permanent injunctive relief should be available. Any injunction granted against a defendant spammer should extend to any other entities with an internet presence that are related to the defendant, its officers or its directors, whether or not those other entities were in existence, had an internet presence or were related to the defendant at the time that legal proceedings were commenced.²¹⁸

Finally, if a lesson could be learned from the US experience, any Canadian legislation should include strong enforcement mechanisms that are rigorously enforced by the appropriate authorities.

217. Similar provisions are also suggested in some of the US bills currently before Congress. See e.g. *REDUCE Spam Act of 2003*, *supra* note 89, s. 6(b) which provides that "In determining the per-violation penalty...the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, the extent of economic gain resulting from the violation, and such other matters as justice may require."

218. Inspiration for this suggestion has been drawn from *Copyright Act*, *supra* note 216, s. 39.1, prescribing "wide injunctions."