CAN WE CAN SPAM IN CANADA?

Written By: John Lawford, Janet Lo and Michael De Santis
Public Interest Advocacy Centre
1204 – ONE Nicholas St
Ottawa, Ontario
K1N 7B7

Published December 2010

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, Ontario
K1N 7B7

Canadian Cataloguing and Publication Data

Can We Can Spam in Canada?

ISBN

1-895060-98-2

PIAC received funding from Industry Canada's Contributions Program for Non-Profit Consumer and Voluntary Organizations to prepare the report. The views expressed in the report are not necessarily those of Industry Canada or the Government of Canada.

Executive Summary

"Spam" is the common term used by consumers to describe the practice of using electronic messaging systems to distribute large volumes of unwanted messages indiscriminately to users. For historical reasons, "spam" has been associated with unwanted electronic mail (e-mail) messages. However, the definition of spam has bedeviled efforts to corral it, as several factors are inputs to the concept without encompassing it totally. Thus consumers have various reactions to electronic messages that are unwanted or unsolicited; commercial in nature; arrive in bulk or are indiscriminately distributed; or those that are offensive, fraudulent or malicious.

Legal efforts to define spam most recently have attempted to encompass the entirety of these factors, in order to leave room for lawmakers to fashion exemptions elsewhere in spam laws for certain categories of messaging that are less offensive to consumers. One example is electronic messages from companies with which consumers have existing business relationships – where it appears users are more tolerant of such communications.

Spam remains a problem to over 70% of Canadian consumers. However, Canadians appear to find it less acute a problem than when it first appeared in the 1990s: 85% of Canadians say spam is a "minor problem" or even "no problem at all". Canadians have sensed, however, that spam now seems to be associated with spyware and "botnet" infections of their computers and can lead to computer takeover and fraud. Canadians state they have in large numbers taken steps to control spam, such as installing anti-virus and filtering programs, however, they have also benefitted from more filtering by and coordination between Internet service providers and third party electronic mail services.

Canada is now in the midst of passing an anti-spam law. The Canadian approach is to define spam widely and require prior consent to all commercial messages. The bill then adds exceptions for such categories as pre-existing business or charitable relationships, where consent is implied. Even in these cases, each electronic communication must provide clear directions on the e-mail about how to opt-out of future communications. Certain "transactional" activities are totally exempted from this regime, such as information from an airline about flight times. The bill also takes aim at botnets and phishing scams, which rely upon spam to deliver links to malware or highjacked webpages. To do so, the bill charges the: CRTC with basic complaints about spam not following the rules; the Competition Bureau with

pursuing fraudulent and misleading commercial messages and the Privacy Commissioner of Canada with ensuring rules against electronic mail address collection without consent.

Industry stakeholders and former Anti-Spam Task Force members were questioned about the likely impact of the law. They stated that Canada's anti-spam law appears to be comprehensive and a serious attempt to start to control a major consumer nuisance. However, to some extent the effort was viewed as "top heavy" and a major question with the new regime would be the level of enforcement that would be brought to the law's many prohibitions. Finally, the application of the new law to even newer communications platforms such as social networking sites and mobile phones was noted as a potential problem. PIAC believes the new law is written sufficiently widely to capture all such spam, however, the complexities of dealing with closed platforms and especially increased consumer trust of correspondents on social networking sites appears to make such new areas ripe for spamming.

Continuing non-legal efforts may dovetail in the future with the new Canadian legal framework. Some promising work in e-mail whitelisting is appearing. ISPs in Canada may have some room to implement more aggressive anti-spam measures, particularly against botnets, however, some incentives may be required to move them towards that course.

Given this environment, PIAC concludes that the new law should be given some time to operate under the control of the CRTC/Competition Bureau/Privacy Commissioner administration before radical changes are made to any aspect of the regime.

However, during this period, the Government of Canada should consider some or all of the following recommendations, which are based on the research in this report, including our survey, as well as our general consumer protection experience and specific electronic commerce experience.

1. **There should be intensive monitoring of spam volumes at the ISP/third party e-mailer level. Such data should be made available to researchers.**

2. **The Government of Canada should fund consumer polling and qualitative research on the effect on consumers of the law.**

3. **The Government of Canada should fund independent research into the effects of the law on e-mail providers and marketers (in particular on social networking sites, wireless platforms and other new means of communication).**

4. **The CRTC, Competition Bureau and Office of the Privacy Commissioner of Canada should undertake intense enforcement efforts under the new anti-spam law, in particular during its initial phases.**

5. **The CRTC, as primary administrator of the new anti-spam law should undertake widespread consumer education about the new regime, especially amongst younger Canadians.**

6. **The Government of Canada should strike a new Task Force on Spam to inform Parliamentarians of progress on the problem when the law is reviewed in three years.**

Acknowledgement

PIAC received funding from Industry Canada's Contributions Program for Non-Profit Consumer and Voluntary Organizations to prepare the report. The views expressed in the report are not necessarily those of Industry Canada or the Government of Canada.

Table of Contents

Introduction

Spam is a term that describes the practice of using electronic messaging systems to distribute large volumes of unwanted messages indiscriminately to users. The term "spam" is most commonly associated with unsolicited email messages, typically of a commercial nature. The early origins of the term "spam" point to a sketch from the popular television show "Monty Python's Flying Circus" where the word was repeated almost endlessly and very much out of context.[1] The term was first employed in the context of computers and technology in the 1980's when users of BBS and MUD systems would maliciously repeat the word "spam" to force other user's chat entries off of the screen. The term persisted through the late 1980's and 1990's when users posted excessive numbers of junk messages in Usenet forums. These messages were generally of a commercial nature. From these rather humble beginnings, spam evolved into veritable commercial enterprise, with some companies earning huge sums by sending out millions and even billions of unwanted messages via electronic mail services that became commonplace amongst users both at work and at home from the mid-1990s to today. However, the term now is applied, at least popularly, to a far broader scope of messages and now is thought to encompass social networking spam, search engine spam, spam on blogs, online forums (link spam) and instant messaging services and even SMS spam on mobile phones.

Report Methodology

PIAC approach to this report was to gather primary research from a national telephone survey of Canadians regarding unsolicited commercial e-mail[2] and to augment that quantitative research with qualitative research in the form of stakeholder interviews with former spam "Task Force" members (explained below). PIAC supplemented the primary research with a secondary source literature review. PIAC undertook its own review of materials on spam kept in house and tracked the progress of and interpreted draft spam legislation with its in-house and external counsel.

---

[1] S.M. Kierkegaard, "War Against Spam: A Comparative Analysis Of The US And The European Legal Approach" Communications of the IIMA (2005) Vol. 5, Issue 2 at 1. Online: http://www.iima.org/CIIMA/CIIMA%205.2%2047%20Kierkegaard-5.pdf

[2] A statement of the telephone survey methodology, confidence intervals and limitations is found in Appendix B of this report: "PIAC's Spam Survey."

Defining Spam is Difficult but Key

The definition of "spam" is probably the most important, yet bedeviling,[3] aspect of researchers', policy makers' and governments' approaches to the entire problem consumers have with unwanted electronic communications of all kinds.[4] As noted, for historical reasons, "spam" has generally been most closely associated with unwanted electronic mail messages. Yet even here there is controversy. One person's unwanted message is acceptable to another, and thus a key aspect of most legal definitions of spam is that it is, at the least, a communication that is "unsolicited". Most consumers, however, seem not to consider an unsolicited e-mail from a long lost friend or a new acquaintance suggesting having a coffee to catch up or get to know each other better as "spam". At worst, this is an unwanted communication but is not generally described by consumers as spam. Adding that the proposed meeting will include a discussion of the friend or acquaintance's business venture, however, may cause some consumers to consider the one-off invitation as a spam message. Thus it is not surprising to learn that most legal definitions of spam also include a requirement that the communication be for "commercial" purposes. Yet here also consumers will make practical judgments.

First, consumers judge on the quality or usefulness to them of the message or their general comfort with the sender of the message. Our survey indicates that consumers still have a high annoyance with commercial messages in general, however, they appear to be slightly less annoyed with commercial messages in general and will give significant leeway to commercial messages from trusted companies they do business with, especially when they view the message as at least in part helpful (that is, providing customer service or a relevant promotion).[5] This appears to be an area of spam that is in flux, as views of consumers and "reputable" companies appear to continue to be divergent but are converging in certain areas: some companies (and many more consumers now) may consider that some unsolicited communications, despite having at least one purpose as commercial are not ringing "commercial" alarm bells and thus are perhaps not even considered spam.

---

[3] See DAVID E. SORKIN, "Technical and Legal Approaches to Unsolicited Electronic Mail", (2001) 35 U.S.F. L. REV. 325 at 327: "The difficulties in addressing the problem of spam begin at the definitional stage: Internet users and providers differ widely in how they define spam and other forms of objectionable e-mail."

[4] Please see section below entitled "Is spam still a problem?".

[5] The answers to several questions in PIAC's survey of Canadians (see below) regarding spam does however make it clear that much annoyance emanates from known entities and companies with which the consumer already does business. See discussion of the survey, *infra*, and in particular note the percentage of Canadians desiring an "opt-in" system for receiving any commercial electronic mail, even for known companies consumers do business with or for special categories of e-mailers such as political parties and polling companies. Nonetheless, other answers clearly show a tolerance for companies the customer does business with and in particular for messages that provide a "benefit" (for example customer relationship management type functions or newsletters).

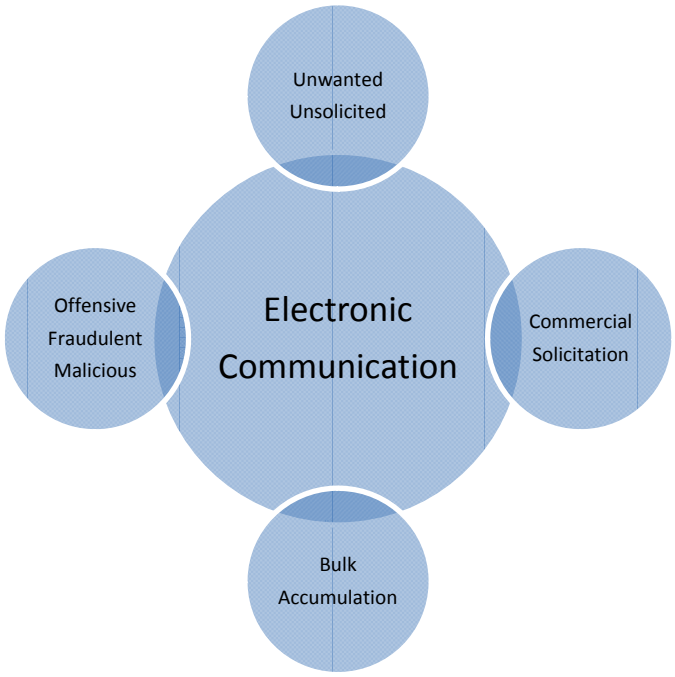

Figure 1 - Factors in Spam Calculus

Second, consumers judge messages not only on the quality but also the quantity of commercial communications. That is, where many commercial messages arrive either from varying sources or it is evident that the actual commercial message is not tailored to the consumer as an individual but likely sent in the same or slightly varied form (that is, it is a bulk message)[6] consumers almost invariably class this type of message as spam. The requirement that a message be a "bulk" e-mail raises definitional problems of how many messages must be sent, to whom and within what time period – and even if variations on a theme make the message in question part of a larger "bulk" e-mailing.[7]

Finally, much of the public disgust, concern or even fear associated with spam is that the content of the messages so often presents either content that is distasteful, illegal, a form of fraud, or presents an actual threat to the security of the recipient's own computer.[8] It appears

---

[6] The question of whether a commercial mailing must be a "bulk" mailing to be considered spam is one addressed in many legal systems. See Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail", supra, at pp. 330-2. Just to muddy the waters in Canada, the Task Force defined it in a Glossary at the close of the report as requiring a bulk component: "Spam: Although there is no internationally agreed-upon definition of "spam," many countries consider it to be any bulk commercial email sent without the express consent of recipients." "Stopping Spam", *supra*, at p. 59.

[7] Sorkin, "Technical and Legal Approaches to Unsolicited Electronic Mail", *supra*, at pp. 330-332.

[8] PIAC's survey of Canadians on spam indicated that 40% of respondents indicated that concern about e-mail delivery of a virus was their biggest concern with spam, with the remainder of the respondents indicating in

that the public considers nearly every message including such objectionable content to be spam, but that a majority of them think such objectionable content is not a *sine qua non* of spam and such objectionable messages do not comprise the whole of spam. Nonetheless, it appears that the public concern with this aspect of spam has increased and may outpace simple concern with unwanted commercial messages. In this, it turns out that consumers have sensed the seismic shift in the delivery method for spam from central servers to botnets (explained below) although they may not fully grasp the mechanics of how this happens or how they can stop it.

If these elements in various combinations are fair "inputs" to the spam equation, the next question becomes (assuming for the moment it is appropriate to pursue a policy of controlling spam) how does the law reflect these elements and define spam or how could a new law in Canada do so? As a result, we turn to the legal definitions of spam, with a view to approaches to controlling spam via legal methods, as opposed to self-regulation, changes in end-received (customer/consumer) behaviour or technical solutions, which we explore below.

Legal Definitions of Spam

The term "spam" generally is not a legal term of art and as noted it is often used as a quick and colloquial term to describe unwanted commercial electronic messages.[9] However, the word "spam" does appear in the title of the Australian *Spam Act of 2003* and also appears in the title of the CAN-SPAM Act in the United States (U.S.),[10] which is an acronym for the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*. Both of these laws provide definitions for unsolicited electronic messages. However, neither uses the term "spam" as a moniker for commercial electronic mail and instead both try to define commercial electronic messages or electronic mail.

---

tranches of around 15% that they were most concerned about offensive or illegal content (18%); spyware (15%) and phishing (14%). The remaining 10% rated all of the above, including viruses, as equally concerning.

[9] Kierkegaard, "War Against Spam: A Comparative Analysis Of The US And The European Legal Approach", *supra*, at 1.

[10] *The CAN-SPAM Act of 2003*, 15 U.S.C. §7701-§7713.

Australia – Spam Act 2003

Section 6 of the Australian *Spam Act of 2003* provides this careful definition of a commercial electronic message:

Basic definition
(1) For the purposes of this Act, a ***commercial electronic message*** is an electronic message, where, having regard to:

(a) the content of the message; and
(b) the way in which the message is presented; and
(c) the content that can be located using the links, telephone numbers or contact information (if any) set out in the message; it would be concluded that the purpose, or one of the purposes, of the message is:
(d) to offer to supply goods or services; or
(e) to advertise or promote goods or services; or
(f) to advertise or promote a supplier, or prospective supplier, of goods or services; or
(g) to offer to supply land or an interest in land; or
(h) to advertise or promote land or an interest in land; or
(i) to advertise or promote a supplier, or prospective supplier, of land or an interest in land; or
(j) to offer to provide a business opportunity or investment opportunity; or
(k) to advertise or promote a business opportunity or investment opportunity; or
(l) to advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or
(m) to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or
(n) to assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or
(o) to assist or enable a person to dishonestly obtain a gain from another person; or
(p) a purpose specified in the regulations.

(2) For the purposes of paragraphs (1)(d) to (l), it is immaterial whether the goods, services, land, interest or opportunity exists.[11]

It is notable that the Australian act clearly covers all of the "inputs" to the spam equation (unsolicited; commercial; fraudulent) with the exception of "bulk", which is arguably covered in subs. (b) "the way in which the message is presented". The Australian approach, unlike that in the U.S. or Europe, is to include fraudulent e-mails as well as commercial ones in its spam law, despite other laws dealing with fraud per se. By "overlapping" the definition in this manner, the Australians can deal with the phenomenon holistically. Note as well, the Australian lawmakers have left a power to deem any new innovative use of commercial electronic mail as part of this section by regulation.

[11] *Spam Act 2003* (Cth.). s.1-2.

U.S. – "CAN-SPAM Act"

Section 3 of the CAN-SPAM Act offers an older and simpler definition of a commercial electronic message:

> IN GENERAL- The term 'commercial electronic mail message' means 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).[12]

What is notable in comparison to the Australian definition is that the U.S. definition does not cover any message sent for the purpose of defrauding a consumer. The U.S. CAN-SPAM Act does not regulate such behavior because it has a well-established dedicated act that is regulating "mail fraud"[13]; a term which has been interpreted to include fraudulent spam in the U.S.

European Union – The Privacy Directive

Article 2(h) of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 provides yet another definition,[14] however, it separates the definition of electronic mail from the commercial aspect of unsolicited email, which is prohibited unless it comes from a company with which the consumer did business and that company has either express consent to send messages or if not, that all messages to the customer have a simple, costless opt-out option:

> 'electronic mail' means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.[15]

The Directive provides a clear prohibition for the misuse of email "for the purposes of direct marketing" at Article 13 entitled "Unsolicited Communications":

---

12 *The CAN-SPAM Act of 2003*, 15 U.S.C. §7701.

13 18 U.S.C. §1341.

14 Note, however, that many other EU Directives are relevant to the spam question in Europe, including the Data Protection Directive 95/46; Distance Selling Directive 97/7/EC; and Electronic Commerce Directive 2000/31/EC.

15 Directive 2002/58/EC of the European parliament and of the Council of 12 July 2002 (the "Privacy Directive").

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. [Emphasis added.]

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.[16]

Europe's approach to the definition of spam is from a data protection perspective that has had the effect of somewhat complicating matters, however, when the definition of spam is related to the rights of the "data subject" rather than being defined as an entity in and of itself, it can lead to more stringent consent requirements, which we discuss below.

Legal Definition of Spam in Canada?

Legislation recently has been introduced in Canada to control spam (discussed below) which includes a comprehensive definition of "commercial electronic message" very much along the lines of the Australian Spam Act of 2003, with some interesting additions. Prior to this time, however, there were no legal definitions of spam in Canada.[17]

Is Spam Still a Problem and if so, How?

Consumers have a number of problems with spam. The first is simple nuisance. Irrelevant and unwanted messages takes consumers time to sort through and delete. Installing and tending to anti-virus software can also take significant time. The second is the problem of lost or undelivered messages – what the industry calls "false positives" – where either ISP spam filters or home spam filter programs mistakenly characterize welcome incoming mail, even from

---

16 *Ibid.*

17 The Anti-Spam Action Plan for Canada, released by Industry Canada in May 2004, simply equated "spam" with "unsolicited commercial email." The final Report of the Task Force on Spam, Stopping Spam: Creating a Stronger, Safer Internet (May 2005), online http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/stopping_spam_May2005.pdf/$file/stopping_spam_May2005.pdf , simply adopted this definition for its work (at p. 1).

trusted personal correspondents or even the owner of the machine himself or herself, as spam. Lastly, spam often acts as a conduit to various forms of malware (including botnet creation) and acts as a solicitation to the gullible to correspond with a fraudster (phishing). We examine where consumers think spam stands on each of these problems now.

Nuisance and Loss of Productivity

Spam imposes direct financial costs on both consumers at home and employees of businesses. There has been considerable research on the monetary cost of spam to businesses. Much of this research focuses on the cost of employee productivity lost as a result of having to deal with spam. One research firm, Ferris Research projected the cost of spam in 2009 to be 130 billion U.S. dollars worldwide and 42 billion dollars in the U.S. alone.[18] These figures represent a 30% increase from 2007 figures and the figures from 2007 were 100% higher than the figures from 2005.[19] Ferris Research breaks down the costs of spam by lost user productivity, help desk costs and the cost of spam control technologies. User productivity costs which include the time spent deleting spam, looking for legitimate messages misdirected by spam filters and other similar lost time accounts for 85% of the cost of spam. Help desk costs which consist mostly of technical assistance for IT technicians to help users deal with the effects of spam account for 10% of the total costs of spam. The price of spam control technologies such as software, hardware, service as well as licensing fees and amortized capital costs account for 5% of the total costs of spam.

The problem of spam has become so pervasive that there are even tools to calculate the estimated financial impact on a business. Google offers one such tool for its users. Users must enter variables such as the number of employees with email, number of workdays per year per employee, average hourly salary per employee, average number of spam messages per day per employee and number of seconds of productivity wasted per spam message. Once these variables have been entered, the user receives figure that explains the overall financial cost to the company and for each employee, as well as how many hours per employee and in total are lost to spam.[20]

---

[18] Richi Jennings, "Cost of Spam is Flattening-Our 2009 Predictions" *Ferris Research* (January 28, 2009) online: < http://www.ferris.com/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions/>.

[19] *Ibid.*

[20] See the Google calculator for details: http://www.google.com/postini/roi_calculator.html

Some research, although less than for employees, has been done on the nuisance, inconvenience and loss of productivity to consumers at home who receive large amounts of spam. Epostmarks, a company selling a trusted email technology has calculated an estimated cost of spam to consumers using email for purposes not related to their careers. Here is their summary of their findings:

> Consumer spam cost the U.S. economy an additional $66.8 billion in productivity loss in 2007. This figure was estimated assuming an opportunity cost of $.04 to delete each of roughly 1.7 trillion annual unfiltered U.S. consumer spam messages received *during non-business hours*. The collective time spent deleting these messages could otherwise be allocated to non-primary work, volunteer work, education, or other activities that contribute to our overall economic and social development. Although the opportunity cost varies widely by person and is thus difficult to quantify, it is important to identify this problem and is reasonable to assume that the *potential value* of this lost time is as high as our primary working time.[21]

Regarding costs to consumers in dealing with spam and related problems delivered via spam, the International Telecommunication Union commissioned in 2008 a survey of 2,000 consumers living in the U.S., completed in 2006. According to this survey, 1 in 5 consumers reported problems with viruses, which caused U.S. $3.3 billion in damages.[22] Eliminating spyware and fixing the damage it causes cost consumers U.S. $1.7 billion and financial losses from phishing attacks cost U.S. $3.1 billion.[23] Another estimate for the U.S. aimed at quantifying the direct damages to repair or replace information systems infected with viruses and spyware. According to the report, consumers paid nearly US$ 7.5 billion over two years to repair or replace hardware.[24]

An important and largely unseen effect of spam is the environmental cost that it imposes. McAfee and ICF international conducted a study to determine the cost of spam in carbon emissions. The study determined that each spam message sent produced an average of 0.3 grams of green house gases.[25] The spam-relation action that has the greatest environmental

---

[21] "True Corporate and Consumer Costs of Spam" Epostmarks, online: <http://blog.epostmarks.com/team-blog/2009/3/21/the-true-corporate-and-consumer-costs-of-spam.html>.

[22] See page 23 of the ITU Study on the Financial Aspects of Network Security: Malware and Spam. Final Report 2008. International Telecommunication Union. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

[23] *Ibid.*

[24] *Ibid.*

[25] "The Carbon Footprint of Email Spam Report" *Macafee* (2009). p.1.

impact is the consumer manually viewing and deleting the spam.[26] This produces 52% of the total emissions. The process of manually sorting, viewing, deleting spam and searching for legitimate messages wrongly marked as spam produces 80% of the total emissions. While 0.3 grams of green house gas emissions per message may not seem like a significant threat, the report continues by stating that some 62 trillion spam messages were sent in 2008. This adds up to about 17 million metric tons of carbon emissions or 0.2% of the world's carbon emissions. If it were possible to stop all spam messages, the equivalent emissions of about 1.5 million U.S. homes or 2.2 million passenger vehicles would not be released into the earth's atmosphere.[27] These staggering figures help to illustrate the very significant environmental costs that spam imposes.

Given this fairly recent, large, documented inconvenience, cost and annoyance, it should be anticipated that consumer dissatisfaction with electronic mail and other forms of electronic messaging would remain high. However, we found a trend to less annoyance with spam.

PIAC's own survey on the effects of spam (detailed below) indicated that while a small minority of consumers continue to consider spam to be a major problem (15%), a large majority believe it is only a "minor problem" (58%) and a sizable minority, 27%, consider it "not a problem at all". Thus on one view, 85% of Canadians view spam as a minor problem, or no problem at all.[28] On the other hand, 73% of Canadians can be seen to still have a problem with spam.

This result contrasts with attitudes prevalent around the time of Canada's last major examination of the spam phenomenon in 2004. At that time, surveys indicated 86% of U.S. email users "reported some level of distress with spam". Pew Internet and American Life Project's March 2004 survey also reported 29% of email users said they reduced their overall use of email because of spam. At that time, the Canadian Task Force on Spam Stakeholder Background Paper warned darkly: "In the absence of successful means of reducing spam, the problem therefore threatens to undermine the use of email and the Internet as an effective platform for online commerce and general communications."

---

[26] *Supra*, p.3.

[27] *Supra*, p.2.

[28] Environics Survey, "PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010", question 2.

The answer as to why the apparent change in perception has occurred in the intervening years is multifaceted but likely includes free or low-cost end user virus and e-mail filtering software, but in particular filtering efforts by major ISPs and e-mail service providers such as Google and Hotmail. In short, Canadians may simply see the problem less: whereas they looked at a glacier of spam in the past, they now see only the tip of the iceberg as Internet service and e-mail providers responded to the problem by raising the initial level of filtering to drown out up to 95% of spam e-mails.[29]

False Positives, False Negatives

Spam filtering software may wrongly mark messages the intended recipient would like to receive as "spam" and take some action on them such as move them to a "spam" folder, which may or may not be locally stored or easy to retrieve. Even if easy to retrieve, if these marked messages are not displayed automatically, users may neglect them or forget they even are there. This is the problem of "false positives". Although ISPs take pains to reduce false positives, often the filtering at the ISP level is completely opaque to users.

Likewise, when spam gets through a spam filter program, it is a "false negative" as the program failed in its primary job of removing spam from view.

Consumers in PIAC's spam study still had a mean spam percentage of 25% of all e-mails, indicating likely some false negatives for those with filters.

Fraud and Malware

Invitations to enter into conversations with fraudsters still occur via electronic message. The Canadian Anti-Fraud Centre Annual Statistical Report 2009 indicates many types of such scams, including fake jobs, dating promises, inheritances, vacations and emergencies relating to loved

[29] See Microsoft, "Security Intelligence Report" 2010, Section 5.5.1 "Email Threats (Spam)", indicating "About 95.4 percent of all incoming messages were blocked at the network edge, which means that only 4.6 percent of incoming messages had to be subjected to the more resource-intensive content filtering process." Online: http://www.microsoft.com/security/sir/keyfindings/default.aspx#section_5_5_1 This was also the view of all of the individual interviewee stakeholders interviewed by PIAC (see below).

ones. These can all be delivered by simple e-mail solicitation. Although not broken down, the Centre indicates that over 10,000 complaints were delivered to victims by E-mail / Internet / Text Messaging.

Malware is any program that in surreptitiously installed and takes over functions of a user's computer. It may in turn be used to transform the users' machine into a "bot" to distribute more spam, or it may be a "keylogger" to record and report keystrokes (for example banking passwords) to fraudsters. Malware can be installed by clicking on an attached .exe file in an e-mail or even by visiting a script loaded webpage that the link in the e-mail directs the user to. [30] This latter attack is called a "drive-by" download but it is delivered to the user usually by e-mail.

Phishing

An example of a malicious form of spam is a phishing attempt via email. Phishing is a fraud technique wherein attackers pose as trustworthy organizations in electronic communications in order to acquire sensitive information such as account passwords for financial institutions, auction sites, online payment processors, IT administrators, communications accounts or social networking websites. Typically, phishing is carried out by email or instant messaging and often directs users to enter details at a fake website that matches the look and feel of the legitimate website by incorporating trademarks and brand names. In addition, authentication mechanisms may be spoofed adding another layer of sophistication. An example of authentication spoofing includes email spoofing, wherein the email address from which the phishing email appears to come from makes the sender look legitimate. The URL link in the email may also be spoofed or manipulated to appear legitimate.

Phishing relies on social engineering techniques to fool users. For example, a sense of urgency might be created by a warning that failure to respond will lead to account termination, penalties or other negative outcomes. Sometimes a phishing attempt may notify the user of a security breach and prompt the user to update their password or security settings. Disaster relief emails from phishers are becoming more common, leading users to a website that appears to belong to a genuine charity to prompt for a donation via credit card.

[30] See Tim Wilson, "Number Of malware-infected websites tops 1 million mark" DarkReading, September 17, 2010. Online: http://www.informationweek.in/Security/10-09-17/Number_Of_malware-infected_websites_tops_1_million_mark.aspx

Botnets

Botnets are often used by spammers to send spam email. A botnet is a collection of computers that have been infected with malicious code that exploits vulnerabilities on the system, giving the botnet "herder" or "master" remote control through commands sent through the internet. Botnet have been used to perform denial of service attacks against a remote target.[31] Spammers often leverage the pooled resources of a created or rented botnet distribution of spam email which are sometime referred to as "spambots", as botnet costs are low when compared to the financial loss and damages caused to businesses and end users. In a February 2010 technical article listing the top ten spam botnets, Daren Lewis of Symantec found that 80 percent of all spam is sent by the top 10 botnets. Furthermore, these botnets send 135 billion spam messages per day and five million computers belong to the ten botnets.[32]

Botnets are a problem for consumers as, although they are generally aware of the danger of viruses and even malware such as keyloggers, it appears many consumers continue to operate compromised computers with no real appreciation of the infection of their computers.[33] ISPs can often isolate users who may be running botnet computers but disinfecting these becomes a difficult job and ISPs may be reticent to undertake given possible liability for otherwise harming their user's home computer, as well as may not be able to afford to undertake the massive clean-up of all users in a competitive market.[34] Finally, it is now apparent that many botnets over-provision for botnet-infected computers, in order to release only a few spam e-mails a day

---

[31] For a complete and concise explanation of botnets, including technical information, see Microsoft® Security Intelligence Report, Volume 9, Jan-June 2010. "Battling Botnets for Control of Computers". Online: http://www.microsoft.com/security/sir/

[32] Michael Kassner, "The top 10 spam botnets: New and improved" TechRepublic (25 February 2010), online: http://blogs.techrepublic.com.com/10things/?p=1373.

[33] See MAAWG, "A Look at Consumers' Awareness of Email Security and Practices", Part 2, pp. 25-28. Although 80% of consumers say they are aware of botnets, 43% think their own computer is unlikely to become part of a botnet.

[34] van Eeten, M. et al. (2010), "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data", OECD Science, Technology and Industry Working Papers, 2010/5, OECD Publishing. doi: 10.1787/5km4k7m9n3vj-en at p. 16:

> A key factor is the cost of customer support. When an ISP contacts or quarantines infected customers, it will trigger incoming customer calls. The ISP incurs a certain cost to handle each call. Some ISPs have reported this cost to be around EUR 8 per incoming call, other estimates are substantially higher (Van Eeten and Bauer, 2008, Clayton 2010). There are indications that the cost of support can quickly outweigh the profit margin for a subscription. Clayton recently estimated that two customer calls in a year may be enough to consume the profits on that customer (Clayton, 2010).

from the infected computers in an attempt to avoid ISP monitoring for certain numbers of spam emanating from one IP or user address.[35]

PIAC's consumer spam survey

In January 2010, PIAC set out to explore how knowledgeable Canadian consumers were on the issue of spam and if it was still a problem for them and to determine what Canadian attitudes would be to an anti-spam law for Canada. PIAC thus conducted a national random telephone survey with Environics Research Inc.[36] The survey consisted of 12 questions asked to 1000 Canadian consumers across the country. The survey was administered to consumers from all walks of life: employed and self-employed people, students, homemakers, retirees and people looking for work. Consumers were also asked where they accessed the internet and the population of the community where they lived.

One important definitional question was answered in advance by the PIAC research team, namely, what definition of spam would be read to the survey participants, as it was thought to impractically lengthen the survey to poll Canadians on the several definitional factors listed above. As a result, the following introduction was used: "Now I would like to ask you some questions about unsolicited commercial e-mail, also known as "spam."" This clearly equates the common use of the term spam with "unsolicited commercial e-mail". As a result, the survey must be read in light of any limitations the presented definition imported.

Consumers were asked 12 important questions to elicit their opinions on spam. Those questions were as follows:

1. Do you have access to the internet?
2. Approximately what percentage of email messages that you receive would you consider spam?
3. How much of a problem is it for you personally to receive spam?
4. Generally, what do you do when you receive spam?
5. Which of the following particular types of spam concerns you most? Specific examples included viruses, offensive or illegal product marketing (such as erectile dysfunction drugs), spyware and phishing.

[35] Interview with Suzanne Morin, Bell Canada, *infra*. Ms Morin confirms that botnet infected computers often release only 3 spam e-mails a day.

[36] PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010. A full description of the survey methodology, confidence intervals and limitations is found in Appendix B of the report: "PIAC's Spam Survey."

6. Which steps have you taken in the past year to control and reduce spam? Step included were installing anti-spam/anti-virus software, never opening email from unknown or distrusted sources, setting up spam filters, updating one's web browser, changing passwords frequently, using more than one email address and turning off the email message preview pane.
7. If the federal government passed a law to control unsolicited emails or spam, which of the following would be the best way to penalize spammers? Examples include monetary fines, criminal charges, injunctions and allowing victims to sue spammers.
8. If the federal government passed a law to control unsolicited emails, which of the following should be exempt from the law, if any? Examples include businesses with whom you already do business, charities, political parties and candidates, newspapers and polling companies.
9. If the federal government passed a law to control spam whereby your consent was required before companies were allowed to send you unsolicited commercial emails, what would be the best way for that to work? Should it be that you must opt-out of receiving the company's emails, meaning companies can assume your consent until you ask them to stop or should it be that you must opt-in to receiving the company's emails, meaning companies may not send you emails unless you provide your prior consent.
10. If there were a way for you to make a complaint about getting spam, how likely would you be to complain?
11. Which of the following would be the most convenient way for you to complain about spam? Examples include forwarding the message to a "spam complaint centre" email address, clicking on a link in the email, calling a toll free number or filling out a form on a website.
12. Which of the following would be the way you would prefer to hear about how your complaint was handled? Examples include receiving an email notice when the complaint is resolved, obtaining a complaint tracking number and being able to track the complaint online and receiving an email acknowledgement of receipt of your complaint.

The results of the survey illustrate the difficulties that Canadian consumers experience because of spam. Remarkably, 11% overall of consumers surveyed reported receiving no spam in their inboxes. However, nearly one third of consumers surveyed overall (29%) stated that between 26 to 100 percent of the email messages they received were spam. This indicates that a sizable minority of Canadians as still dealing with large volumes of spam at the user level despite filters

of ISPs and third party e-mail providers, as well as their own spam filters. The mean percentage of spam e-mails of total e-mail volume (including those answering 0%) was about 25% of e-mails for the average Canadian with "access to the Internet". This is still very high.

As noted above, 73% of consumers surveyed stated that they believed that spam was a problem, with 58% stating it was a minor problem and 15% stating it was a major problem. However, 85% considered it a "minor problem" or "no problem at all." Consumers in Alberta seemed most affected by spam with 60% calling it a minor problem and 20% calling it a major problem. Consumers living in Manitoba and Saskatchewan seemed least affected by spam with 52% calling it a minor problem and 10% calling it a major problem. Disturbingly, in most of the higher percentage tranches, younger people reported higher spam levels, in particular those receiving 51%+ of spam in e-mails. This may reflect younger users' higher use of social networking sites and new communications platforms (described below) where innovative spam techniques are beginning to appear.

The survey results also reveal how Canadian consumers react to spam and what kind of behavior they engage in to deal with it. The survey examined what kind of action consumers took when they received spam. In general, over half of them used a filtering program to try and stop it (53%). A sizable minority simply ignore spam (36%). This indicates some inertia which could perhaps be leveraged if spurred to action. Alarmingly, some consumers (2% overall) chose to respond to the sender, which is risky behavior, as it confirms a working email address. One percent of consumers overall that were surveyed chose to complain to their ISP about receiving spam.

When asked about spam, many consumers had particular ideas about what kind of spam they perceived to be most harmful. Viruses or messages that contained malware were of the most concern to consumers with 40% of them overall stating that this type of spam concerned them the most. After viruses and malware, offensive or illegal product marketing messages, such as those promoting erectile dysfunction drugs, was the most troubling form of spam with 18% of consumers overall stating that it concerned them the most. Next was spyware with 15% of consumers overall stating it concerned them the most followed finally by phishing messages with 14% of consumers most concerned with that threat.

The survey also identified how consumers tried to prevent spam from affecting them. Overall, 88% of consumers had installed anti-spam, anti-virus or a firewall, 87% never open emails from unknown or distrusted sources, 72% have set up filtering option on their web browser or email client software, 70% performed updates on their web browser, 44% changed their passwords, 43% used more than one email address and 31% turned off the email message pane. It is interesting to note that of all the different groups divided by employment status, self employed people were the most aggressive in their measures to stop spam. 93% of them had anti-spam and anti-virus software and 91% never open messages from unknown or distrusted sources. These figures help to illustrate just how destructive spam can be on the operation of a business, even a small business employing a single person. The high percentages of action in all these categories also indicate consumers are willing to take action on spam, provided the actions are easy to understand and perform.

Consumers surveyed were also questioned about their attitudes concerning policy responses to the spam problem, in anticipation of anti-spam legislation. Consumers were asked how they would go about penalizing spammers. The most popular remedy was monetary fines for spammers, which was favoured by 33% of consumers overall. The second most popular remedy was criminal charges for spamming, which was favoured by 30% of consumers overall. Injunctions filed against spammers to make them stop spamming was favoured by 21% of consumers overall and 9% favoured a private right of action or the right to sue spammers. The comfort level with the administrative control of spammers by fining may indicate consumers' growing familiarity with the largely similar National Do Not Call List.

The survey also sought to determine what kind of exceptions should be written into the law, more specifically, what kind of organizations or businesses may contact consumers freely, unconstrained by spam laws. Overall, most consumers felt that businesses with whom they already do business should be exempt, with 43% of consumers supporting this idea. Registered charities had 31% support overall, political parties, candidates in elections and political riding associations had 21% support, newspapers of general circulation had 18% support and polling companies had 17% support. Again, as these categories are those that apply in the National Do Not Call List, it may be that consumers are becoming conscious of them. It also may reflect consumers' perceptions that electronic messages may be more tolerable if "useful" in some way to them, in particular, if they see the advantage in a regular communication as part of their customer (or donor) relationship.

The survey also asked a critical question concerning the consent of consumers to receive commercial messages. Consumers were asked to choose whether they wished for companies to assume their consent for receiving commercial messages, until told to stop (an "opt-out" regime) or whether they preferred to have companies and organizations to ask their consent first, before sending them commercial messages (an "opt-in" regime). An overwhelming 86% overall favoured an opt-in regime, compared to only 13% overall who favoured an opt-out regime. This was the strongest preference on the part of Canadian consumers in the survey and has obvious implications when crafting anti-spam legislation.

The survey also examined the question of how likely consumers were to complaint about receiving spam, if there was someone they were able to complaint to who would help them. Overall, 32% were very likely to complain, 39% were somewhat likely to complain, 18% were not very likely to complain and 10% were not at all likely to complain. With 71% of Canadian consumers likely or very likely to complain, it is clear that many consumers wish they had some form of recourse if they were abused by spammers. Consumers were also asked which method they would prefer to employ if they were able to complain about spam. Overall 50% chose to forward the email to a "spam complaint centre" email address, 26% chose to click on a link in the email, 14% preferred to call a toll free number, 8% wanted to fill a form on a website and 1% preferred all these options equally. Again, this result indicates a simply third party administrative system (akin to the National Do Not Call List) would be very popular amongst Canadians and might have an appreciable effect on gathering raw complaints about spammers.

Given the results of the survey, it is clear that while spam is a problem on the minds of Canadian consumers that they would like to see addressed, they are doing what they can to stem the tide (88% installed software to try and block spammers from reaching them) and they are willing to tolerate clearly relevant communications from certain senders, provided they retain control and any law quickly and effectively deters e-mail senders that abuse the system. When and if such legislation comes, a large majority of consumers surveyed wished any applicable spam legislation were opt-in, giving them control over who might contact them (86% of consumers surveyed said they wished for an opt-in regime). Given these figures, it is clear that Canadian consumers are rightly concerned about the effects of spam and that a legislated solution is required, but that it retain some flexibility for marketers but with the maximum of consumer control.

Stakeholder Interviews

PIAC also undertook stakeholder interviews to provide industry perspective as well as context and personal insight to the research. In particular, PIAC approached those persons who were originally on the Anti-Spam Working Group and still are key players in the debate over spam. References to these interviews are also made in footnotes where the stakeholders agree or disagree with a statement made or position taken in the rest of this report.

Jacob Glick, Google

Mr. Jacob Glick, Google's Canada Policy Counsel was not on the original Spam Task Force, the company he works for, Google, Inc. provides one of the world's largest third-party electronic mail service, Gmail.

Mr. Glick noted that much spam is *already* illegal under some other legislation, be that simple fraud, misleading advertising or phishing. He stated that many email systems provided by Google, and others already filter out most of these messages. His view was that the evidence from around the world has demonstrated the most effective solutions to spam were technological and not legislative.

Mr. Glick noted that most responsible businesses already give their customers the choice to unsubscribe from email lists.Market-based solutions have been effective in this regard.

Finally Mr. Glick pointed to a document in which Google explains, in broad terms, how it controls spam in Gmail, which techniques have proven highly effective for Gmail users.[37]

[37] See "Gmail: Google's approach to email", undated, online: http://mail.google.com/mail/help/intl/en/fightspam/spamexplained.html In effect, Google "crowdsources" its users' expertise to recognize and control spam.

Michael Geist, University of Ottawa

Professor Michael Geist is Canada Research Chair in Internet and E -commerce Law at the University of Ottawa. He also publishes a popular blog on Internet law and policy. He was a member of the original Spam Task Force.

Professor Geist noted that spam may be more or less noticeable now than in the mid-2000s depending on the consumer's own circumstances. This is because while the volume of spam has increased, there are far more and better spam filtering tools, both at the ISP and individual consumer level. He noted however that false positives are still a problem with filters and thus the reliability of email is still compromised by spam.

Professor Geist noted that spam now appears in more places than previously, including on mobile services such as SMS on cellphones – which can generate real costs for consumers. He also noted an increase in "real" harms from spam, in particular ID theft, phishing and malware.

Regarding Bill C-28, Professor Geist noted that although there were compromises made to ensure passage of the bill, that it was certainly better than the status quo. He praised the bill's "aggressiveness" in "flipping the presumption" that consumers should tolerate spam to instead provide control to consumers by assuming a stance of no unsolicited email without clear consent.

Professor Geist was asked whether Bill C-28 effectively reversed the finding made by the Privacy Commissioner of Canada in a complaint brought by him regarding unsolicited use of his work email, which found that such emails required explicit or implicit consent and that posting an email in a public space was not an invitation to spam. He acknowledged that Bill C-28, which allows such "business to business" e-mails (provided the recipient has not taken steps to note on their public webpages containing email addresses that he or she does not wish to receive such commercial emails) reversed his finding but noted that the investigation and enforcement regime proposed under Bill C-28 was vastly superior to proceeding before the Privacy Commissioner, who had no order making power to stop the spam. He expressed concern,

however, that the fines meted out under the new spam powers by the CRTC might mirror the small fines so far imposed under the Do Not Call legislation.

Regarding the future of spam, Professor Geist noted that wherever a popular new communications platform established itself, spam would follow. He cited Facebook, where, he stated, spam into Facebook groups was making running such groups as advocacy tools a chore, simply because the groups now had to be actively moderated to remove "link spam" (see "link spam" case study below). He also noted the emergence of spam on Twitter, in effect the creation of Twitterbot followers who simply spam (commercial link) tweets to popular tweeters.[38]

Regarding the spyware rules, Professor Geist noted that the result in Bill C-28 was again a compromise between privacy and the pressures exerted by copyright holders and law enforcement to probe consumers' computers for certain activities but at the least, full disclosure would be required for updates and other software controls on users.

Suzanne Morin, Bell Canada

Suzanne Morin is Senior Legal Counsel at Bell Canada. She is responsible for a wide range of advice on legal and policy matters, in particular in the consumer space. Ms. Morin was a member of the Task Force on Spam.

Ms Morin noted that much had changed since the Task Force in 2004-5. Then, service providers were struggling with spam. However, today, ISPs have become much better at identifying spammers within their own networks and denying them service. The problem in 2010 now is botnets, where the spam is coming from all of the ISPs users, not simply a small number of spammers. As a result, the problem, since there are strong filters at the ISP level, is more hidden from the customer and has become a greater burden on the ISP.

[38] We note that there has been for some time now a twitter commercial messages tool (as opposed to an underground hacker exploit) called "Tweettornado": see Dancho Danchev, "Commercial Twitter spamming tool hits the market" (4 February 2009) Zero Day blog. Online: http://www.zdnet.com/blog/security/commercial-twitter-spamming-tool-hits-the-market/2477

Ms. Morin noted however that ISPs and email providers have become better at delivering "legitimate" commercial email and that false positives for such messages (from the point of view of senders) have been virtually eliminated.

Thirdly, Ms. Morin noted that the ISP and email provider industry has in recent years built strong relationships in Canada and internationally to ensure the free flow of email and to avoid blacklisting of one another due to spam problems.

Fourthly, Ms Morin noted the higher use of anti-virus software to control spam by consumers.

Regarding the possible effect of Bill C-28 on spam in Canada, Ms Morin noted that the Task Force's original recommendations stressed applying existing laws to spam to catch the "bad guys". She questioned if the approach taken by Industry Canada had gone to far in "prohibiting everything" – with exceptions – thus pushing the cost of spam onto legitimate marketers. She noted that Bill C-28 is essentially an overlay – that Canada already has the Personal Information Protection and Electronic Documents Act, which requires consent to contact customers. Therefore the new spam law simply would require more "due diligence" for legitimate marketers. She cited the difficulties the new Act would impose on something as simple as software updates, ironically often to update consumer spam filters. She stated that spam has moved beyond nuisance and that this law would have been more effective 8 years ago.

Ms Morin also noted that ISPs and major marketers were concerned that the CRTC might adopt a "heavy-handed approach" to the fines permitted under the new spam law. She noted that since spammers not resident in Canada would be hard to catch, that it would possibly be Canadian marketers who made occasional mistakes who would bear the full brunt of enforcement, particularly if results were needed to justify the existence of the enforcement regime.

Regarding the future of spam and spam regulation, Ms Morin again noted that 95% of the "nuisance" spam was now dealt with by ISPs, and other internet intermediaries. She noted that

in certain spaces, such as SMS wireless spam, where the industry "got ahead of the curve" it is possible to set up rules making it more difficult for spammers to take over.

The real problem is not email marketing but "nasty stuff" and the law should be tuned to targeting the people doing real harm online. The law should focus on "following the money". The present law (C-28) does have the advantage of focusing law enforcement attention on the problem of spam, which Ms Morin noted was in the past held back by perception of the need for a new law specifically on spam, and she hoped the new law would lead to prosecution of fraudsters and increased scrutiny of ISPs harbouring such operations.

Ms Morin confirmed that it is difficult and expensive to quarantine infected users who are part of a botnet. It is not clearly an ISP responsibility and ISPs not only fear the immense cost but also potential liability for attempting to disinfect customers' computers. Ms Morin noted that botnets now rely on a larger number of infected machines to send out fewer spam emails a day (as few as three a day) making detection and action difficult. She confirmed that there are huge incentives to remove such botnets, but that the difficulties noted above cancel out such incentives. Finally, she noted that there are few efficiency gains likely for consumers in switching ISPs, as most use the same filtering software providers.

Spam legislation in Canada

Task Force on Spam, 2004

The debate regarding spam legislation in Canada began in 2004 when the Anti-Spam Action Plan for Canada was launched. The federal government wished to explore this issue further and assembled a group of industry representatives, scholars and experts to examine the problems created by spam in Canada and how to potentially address them. This initiative created a task force composed of representatives of parties from the private sphere such as marketing companies, telecommunications companies and academics. The task force was chaired by Industry Canada and the task force was seeking viable solutions to the problem of addressing spam in Canada. The Task Force on Spam held a round table meeting in December of 2004 to solicit the opinions and positions of stakeholders on the issue. This round table was announced in the *Canada Gazette* as well by using an online forum established especially for this purpose. In May of 2005, the task force released its report on spam. This report made 22

recommendations that could be effective in combating spam, including that legislation be enacted to help stop it. [39]

Despite the existence of the Task Force on Spam before the enactment of anti-spam legislation in other countries, Canada remained the last country in the G8 that does not have comprehensive spam legislation. There are *Criminal Code* provisions that were highlighted by the task force as being potentially useful in prosecuting spam cases, however, these provisions were not discussed in the task force report and these provisions have not been used to prosecute spammers.[40] Additionally, the Competition Bureau and the Privacy Commissioner have both received complaints from Canadians about receiving spam but there has never been any framework or legislation that allowed them to resolve these complaints.[41]

Private Member's Bill from the Senate

The first Canadian Bill directly addressing spam was Senator Yoine Goldstein's Bill S-202.[42] This Bill was introduced in 2008 and was a relatively short Bill that sought to prohibit unsolicited commercial messages and to require explicit consent from the recipient a message could be sent. The Bill excluded messages from political parties or candidates, charities, educational institutions and commercial messages from businesses that have an existing business relationship.[43] The Bill also forbade senders from misrepresenting themselves or impersonating another trusted sender.[44] The Bill died on the order paper.

Political Attention for Spam at Last

Perhaps sensing the political climate in advance of the election, responding to the policy issue in a proactive way, or seeing the interest in the Goldstein bill, Prime Minister Harper on

---

39 Note that Task Force member Suzanne Morin in her interview underlined that the thrust of the Task Force's recommendations was to amend existing laws to combat spam, not to create a "superstructure" law on top of it, as has been attempted with the ECPA and now FISA (see below).

40 Alysia Davies, "Bill C-27: The Electric Commerce Protection Act" *Parliamentary Information and Research Service, online:* <http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?lang=E&ls=c27&source=library_prb&Parl=40&Ses=2#fn04>.

41 *Ibid.*

42 Bill S-202, *An Act respecting commercial electronic messages*, 1st Sess., 40th Parl., 2008.

43 See section 8 for all of the permitted exceptions.

44 *Supra* note 45, cl.14-15.

September 25, 2008 announced the Conservative Party's intention to enact spam legislation as part of its consumer protection platform plank.

Electronic Commerce Protection Act, Bill C-27

Thus it came as little surprise that in April of 2009, the Minister of Industry, Tony Clement, introduced Bill C-27 or the *Electronic Commerce Protection Act* (ECPA). The Bill sought the creation of a new Act, as well as amending four existing Acts that regulate telecommunications, competition and privacy. An important change the Bill would have made was to designate the Canadian Radio-television and Telecommunications Commission to act as the main regulator for the ECPA.[45] The Commissioner of Competition and the Privacy Commissioner were also to take on smaller enforcement roles, had the Bill passed. Below is a chart outlining the proposed roles of the three agencies and the subject matter assigned to them.[46]

Roles of Agencies under Anti-Spam Bill (ECPA, now C-28 "FISA")

Administration	Violation	Addressing
CRTC	ECPA/FISA includes violations respecting: · The sending of unsolicited commercial electronic messages · The use of telecommunications to alter transmission data and download programs to computer systems and networks without authorization	· Spam · Malware & Botnets · Network re-routing
Competition Bureau	ECPA/FISA amends the *Competition Act* to include violations respecting: · Misleading and deceptive practices / representations, including false content, headers, subject lines	· False or misleading representations online (including websites and addresses)

[45] *Supra* note 43.

[46] PIAC expresses its thanks to Thomas Pentland, Competition Bureau, for permission to reproduce this chart.

OPC	ECPA/FISA amends *PIPEDA* to include contraventions involving: ・The collection and use of personal address information without consent by electronic or any other means ・The collection of personal information by illegally accessing, using or interfering with computer systems	・Address harvesting ・Dictionary attacks ・Spyware (Personal Information)

The ECPA was a lengthier and more complex than Bill S-202. In addition to stopping the propagation of spam, the Bill sought to empower the CRTC, the Competition Bureau and the Privacy Commissioner to work together and with international counterparts to deal with spam coming into Canada from outside the country. The government was clear about its intentions regarding spam when it published its backgrounder on the ECPA. It stated that the ECPA would "drive the most dangerous and damaging forms of spam from occurring in Canada and to help drive spammers out of Canada.[47]

The ECPA contained a variety of new definitions which do not appear in other federal laws, particularly in the context of technological concepts. For example, the nearest relative to spam laws in Canada is the federal Do Not Call List, which is governed by the Unsolicited Telecommunications Rules developed in proceedings before the Canadian Radio-television and Telecommunications Commission (CRTC).[48] It defines "telemarketing" as "the use of telecommunications facilities to make unsolicited telecommunications for the purpose of solicitation".[49] It was not entirely clear if the legal definition of "telecommunications facilities" included all elements of electronic messages like email. "Solicitation" is defined as "the selling or promoting of a product or service, or the soliciting of money or money's worth, whether directly or indirectly and whether on behalf of another person. This includes solicitation of donations by or on behalf of charitable organizations".[50] Adding to the uncertainty was the CRTC's regulatory forbearance stance with regard to

[47] Industry Canada, "Government of Canada Introduces the *Electronic Commerce Protection Act*," Backgrounder, Ottawa, 24 April 2009. Online: http://www.ic.gc.ca/eic/site/ic1.nsf/eng/04595.html

[48] CRTC Telecom Decision 2007-48. Online: http://www.crtc.gc.ca/eng/archive/2007/dt2007-48.htm

[49] *Ibid.,* at para. 79.

[50] *Ibid.*

retail internet services,[51] making the development of new rules solely for e-mail or extending the present Unsolicited Telecommunications Rules to Internet service providers difficult.

The ECPA therefore created a different standard to ground the new regulation: "commercial activity", presumably to ground the federal government's jurisdiction to regulate spam under the constitutional "trade and commerce" power rather than strictly telecommunications. The new definition for "commercial activity" proposed was different, however, from the definition included in the *Personal Information Protection and Electronic Documents Act* or PIPEDA (another act replying upon trade and commerce to ground its constitutionality). The ECPA took part of the wording from PIPEDA: "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character"[52] and added a new clause to it: "whether or not the person who carries it out does so in the expectation of profit."[53] This amended definition could be potentially linked to the some of the third party liability clauses included elsewhere in the ECPA. It also reflected an intention to widen the scope of which party is liable for spamming, which could possibly implicate ISPs or computers infected and harnessed by botnets.[54] The definition of commercial activity was also changed to exclude any action, conduct or message sent for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defense of Canada.[55] Actions or conduct could possibly include the installation of spyware on a user's computer to monitor their activities.

Also included in the ECPA was a very broad definition of "electronic address", unlike legislation elsewhere such as the U.S. CAN-SPAM Act. This definition[56] covered technology such as email, instant messaging, SMS messages sent from phones and messages sent from "any similar account" which would likely include social media such as Facebook or Twitter. A new definition was also provided for "electronic message" and this definition included any message sent over a means of telecommunication including a text, sound, voice or image.[57] This comprehensive definition appeared to have included voicemail messages, webcam messages, and the transmission of pictures or graphic files by methods of telecommunication.

---

51 See, Orders 97-471 and 99-592. See also Telecom Decision 98-9 in relation to cable ISPs.

52 *Personal Information Protection and Electronic Documents Act* S.C. 2000, c. 5, subs. 2(1).

53 Bill C-27, *The Electronic Commerce Protection Act*, 2nd Sess., 40th Parl., 2009 at subs. 2(1) ("ECPA").

54 *Supra*, note 47.

55 *ECPA* at subs. 2(4). Note that in Committee Marc Garneau, Liberal Party, attempted to exempt also communications with regulated professions thusly: "a body established by an Act of Parliament or a provincial or territorial legislature to regulate a profession, or an affiliated entity of such body". It was ruled out of order.

56 *ECPA* at subs. 2(1).

57 *Ibid.*

Another new definition provided by the ECPA was a definition for "commercial electronic message" which considers the content of the message. The definition considers not only the content but also any hyperlinks present in the message and also any commercial traits in the contact information provided for the message.[58] Therefore, if some inference of commercial activity may be drawn from links or contact information present in the message, it may be considered a commercial electronic message (see our "case study" on link spam below). Commercial activity was also defined to include any solicitation to purchase, sell, barter or lease products or services, land or an interest or right in land in addition to offers to provide a business, investment or gaming opportunity.

The ECPA also provided a definition of "transmission data". The definition encompasses any data which deals with "the telecommunications functions of dialing, routing, addressing or signaling".[59] This definition included telecommunications by phone, internet and wireless and involved all the steps of transmitting the message electronically outside of the actual substance of the message itself. The intention of this particular definition appeared to be to regulate all of the steps needed to transmit a message electronically, preventing a spammer from misusing a network to transmit spam or to assume a false identity to perpetrate offences such as phishing or identity theft.

An important exception was provided by clause 6(7) of the ECPA. This clause exempted two way voice communications between business and consumers. On its surface this clause appears to have the effect of exempting commercial solicitations over the telephone. Industry Canada officials testified before the Industry Committee in hearings about the ECPA that technological obsolescence could make the National Do Not Call List inapplicable to voice communications.[60] This was due to the transition from traditional telephone networks to Voice over Internet Protocol, which transforms telephone service into a form of electronic message. PIAC in discussions with CRTC employees responsible for the telemarketing rules confirmed that the intention is to leave the two systems (anti-spam and the Do Not Call list) separate but under one roof at CRTC for their administration until such time as both are well-functioning. Then the exemption in subs. 6(7) would be repealed.[61] The effect of this would be to update the consent

---

58 *Ibid.*

59 *Ibid.*

60 Testimony of André Leduc and Philip Palmer, Industry Canada, to the House of Commons **Standing Committee on Industry, Science and Technology**, 26 October 2009, at 16:45–17:10.

61 *ECPA*, s. 64; s. 69 of Bill C-28.

rules in the National Do Not Call list to the slightly higher standards under the ECPA/Bill C-28 framework and then administer all commercial electronic messages, whether by voice or other communications facility, under one set of rules and one enforcement mechanism.

This holistic approach is consistent with the expressed purpose and constitutional underpinning of the proposed anti-spam law, which is based upon encouraging electronic commerce. The ECPA defined its purpose at clause 3 of the Bill:

> The purpose of this Act is to promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct
>
> (*a*) impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities;
>
> (*b*) imposes additional costs on businesses and consumers;
>
> (*c*) compromises privacy and the security of confidential information; and
>
> (*d*) undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities in Canada and abroad.[62]

The ECPA also contained provisions at clause 4 that made it binding on any corporation either federally or provincially incorporated.[63] The ECPA was not binding on broadcasters in relation to their broadcast undertakings, however,[64] only to their telecommunications (ISP) services.

The ECPA died on the order paper in December 2009 when the bill had cleared the House of Commons committee charged with studying it and was before the Senate Transportation and Communications Committee.

Fighting Internet and Wireless Spam Act (FISA), Bill C-28

However, the ECPA was quickly re-introduced in nearly identical form in the new Parliament on May 25, 2010 as the *Fighting Internet and Wireless Spam Act*, Bill C-28 ("FISA") – a name that

---

62 *ECPA*, s. 3.
63 *ECPA*, s. 4.
64 *ECPA*, s. 5.

more closely reflected the original political message of the Conservative Party of Canada. Jumping ahead to the present, C-28 was examined briefly by the House of Commons and reported out to the Senate on November 2, 2010 with only one amendment – namely the deletion of the short title, FISA, which was judged too politically charged by the opposition parties which united against the Conservative party members to remove the short title.[65]

The discussion of C-28 (we defer to the direction of the Committee not to use the short title proposed) is somewhat difficult, in that amendments were made to the ECPA that were of note but, as noted, the ECPA was, in amended form, largely recapitulated in the form of Bill C-28. As a result, our discussion of Bill C-28 will be through the ECPA and its numbering of sections, as these have not substantively changed. To assist the reader, we append a chart with a comparison of all key sections of the ECPA and Bill C-28 in Appendix 1. Where confusion might arise or there are substantive differences in the two bills, we also reference the Bill C-28 numbering.

How the Proposed Anti-Spam Bill Works

Most of the substantive clauses of the ECPA (now Bill C-28) may be found at clauses 6 through 9. Clause 6 forbids the transmission of a commercial electronic message unless there is express or implied consent on the part of the recipient.[66] Any commercial message sent must also conform to a prescribed form which identifies the person who sent the message and the person on whose behalf it was sent, if applicable, the message must provide accurate details to contact the sender and also a mechanism to unsubscribe from future messages. There are exceptions to the prohibitions set out by clause 6. Family members are excepted as are messages sent that are solely inquiries or applications relating to commercial services.[67] There was also a clause that exempted intermediary ISPs from liability.[68]

Two other exemptions of note were the exemption of messages from charities to whom one has donated or worked for, and exemption of messages from political parties or candidates for office, within 2 years of the e-mail being sent.

---

[65] Standing Committee on Industry, Science and Technology, Tenth Report, C-28. Online: http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4747972&Language=E&Mode=1&Parl=40&Ses=3

[66] *ECPA*, s. 6; Bill C-28, s. 7.

[67] *ECPA*, subs. 6(5).

[68] *ECPA*, subs. 6(6).

As the ECPA passed through the House of Commons, various other exemptions were added after committee meetings and debates. Clause 6(5.1) provided an exception to messages sent for the purpose of providing quotations or estimates of commercial good or services, but only if this was explicitly requested by the consumer.[69] Another exception would have provided an exception that applied to messages that facilitate, complete or confirm a transaction that has already been consented to by the consumer.[70] A different exception provides warranty, product service or safety or recall information on a product or service that a consumer has purchased.[71] These are referred to as "transactional" exemptions (see below).

The effects of hackers were addressed by clause 7 of the ECPA. Clause 7 forbids anyone from altering transmission data along a network or to cause a message to be copied or sent anywhere other than where the sender intended it to go.[72] Any such alteration or misdirection required the consent of the sender. Thus the common spam technique of masking the actual sender of the message was forbidden. There was an exception for service providers who may need to alter transmission data for "network management".[73]

A provision at clause 8 prevents the installation of a computer program to be installed on a consumer's computer and also prevents any electronic messages to be sent from any installed program on a consumer's computer.[74] This provision would have stopped malicious code such as spyware and malware from being installed on a consumer's computer.

These measures are clearly aimed at stopping users' computers from being turned into "zombies" for a "botnet" (see below). A botnet is a vast, distributed system of computers used for disseminating spam messages.

Additionally, however, the wording would also prevent software similar to Sony's infamous rootkit from being installed on a consumer's system. The Sony rootkit was a piece of software

69 *ECPA*, subs. 6(5.1)(a).
70 *ECPA*, subs. 6(5.1)(b).
71 *ECPA*, subs. 6(5.1)(c).
72 *ECPA*, subs. 7.1.
73 *ECPA*, subs. 7(2).
74 *ECPA*, s. 8.

that automatically installed itself on a consumer's computer after it was inserted in a computer's CD-ROM drive. The disc would then install software on the consumer's computer without their knowledge or consent to prevent the disc from being copied. This software then left the computer very vulnerable to malicious attacks. The provisions afforded by clause 8 have been opposed by media companies who have already implemented monitoring software (spyware) to control copyright infringement or plan to do so in the future, especially if such "technical protection measures" are permitted under upcoming copyright act reform.[75]

Clause 9 designates the causing or procurement of any of the activities in clauses 6 through 8 to be a violation of the ECPA. Any actions identified under clause 6 are violations only if the computer used to send or access the offending message in question is located in Canada.

Consent

The issue of consent is critical to any law regulating spam, since consumers react differently to different e-mails and different senders, however, overall they appear to dislike unsolicited communications. Clauses modifying the basic rule on consent (s. 6, ECPA) are found at clauses 10, 11 and 13. Clause 6 permits electronic communications either where there is express and implied consent. It reads:

> 6. (1) No person shall send or cause or permit to be sent to an electronic address a commercial electronic message unless
>
> > (a) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and
> >
> > (b) the message complies with subsection (2).

Express consent or "opt-in" consent requires that commercial messages may not be sent to a consumer unless that consumer has first consented to receiving such messages. Such "express" consent, it appears, can be a specific opt in box or typing of a word to signify consent, or it can be contained in another document, such as an account opening application, or a privacy policy

[75] See M. Geist, "The Copyright Lobby's Secret Pressure On the Anti-Spam Bill" (19 October 2009). Online: http://www.michaelgeist.ca/content/blogsection/0/126/

for a service, provided the customer has signed or assented to the application or acknowledged the privacy policy as a term of service.[76]

Implied consent or "opt-out" consent does not require explicit consent before a commercial message may be sent to a consumer. Commercial messages may be sent under an opt-out regime if the senders believe the consumer wants to receive messages from them based on past behaviour. If they do not, they must be provided a way to opt out of receiving further communications. Under the ECPA, if there is an existing relationship between the sender and the recipient, consent may be presumed; that is, there is implied consent. The most common use of this existing relationship will be an "existing business relationship". Clause 10(4) defines the parameters for existing business relationship as such:

> In subsection (3), "existing business relationship" means a business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from
>
> > (*a*) the purchase or lease of a product, goods, a service, land or an interest or right in land, within the two-year period immediately preceding the day on which the message was sent, by the person to whom the message is sent from any of those other persons;
> >
> > (*b*) the acceptance by the person to whom the message is sent, within the period referred to in paragraph (*a*), of a business, investment or gaming opportunity offered by any of those other persons;
> >
> > (*c*) the bartering of anything mentioned in paragraph (*a*) between the person to whom the message is sent and any of those other persons within the period referred to in that paragraph;
> >
> > (*d*) a written contract entered into between the person to whom the message is sent and any of those other persons in respect of a matter not referred to in any of paragraphs (*a*) to (*c*), if the contract is currently in existence or expired within the period referred to in paragraph (*a*); or
> >
> > (*e*) an inquiry or application, within the six-month period immediately preceding the day on which the message was sent, made by the person to whom the message is sent to any of those other persons, in respect of anything mentioned in any of paragraphs (*a*) to (*c*).[77]

---

[76] This is to be contrasted with the new Dutch anti-spam law, discussed below. This assumption comes from a review of the findings of the Privacy Commissioner of Canada, who has held that such documents can be operative as express consent. See, for example, PIPEDA Case Summary 2003-243.

[77] *ECPA*, subs. 10(4).

Clause 10(6) also defines the parameters for an "existing non-business relationship":

> In subsection (3), "existing non-business relationship" means a non-business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from
>
> > (*a*) a donation or gift made by the person to whom the message is sent to any of those other persons within the two-year period immediately preceding the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization, or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office;
> >
> > (*b*) volunteer work performed by the person to whom the message is sent for any of those other persons, or attendance at a meeting organized by that other person, within the two-year period immediately preceding the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; or
> >
> > (*c*) membership, as defined in the regulations, by the person to whom the message is sent, in any of those other persons, within the two-year period immediately preceding the day on which the message was sent, where that other person is a club, association or voluntary organization, as defined in the regulations.[78]

While consumers overwhelmingly favoured an opt-out regime for spam (our survey, question 8, had 86% of consumers preferring opt-in to opting out of receiving commercial electronic messages), they also expressed a strong minority opinion that commercial messages from businesses they do business with be exempted from the law completely (43%, our survey question 7). Likewise 31% of Canadians would exempt charities from the consent requirement.

Thus it appears the bill attempts to satisfy both desires. It does not provide a full express consent requirement, however, it does not provide pure exemptions from the regime (as with the Do Not Call List) but rather allows those entities that a large group of Canadians will tolerate most mesages from the lesser standard of implied consent, which may always be withdrawn by a consumer who changes his or her mind. This compromise appears to be a brilliant solution to the seemingly contradictory desires of the Canadian population to both control spam, but be flexible in its use when it is legitimately useful to them as consumers.

---

[78] *ECPA*, subs. 10(6).

Spyware

As noted above, as the anti-spyware aspects of the ECPA progressed through the House, a variety of amendments were proposed for the consent clauses to such "monitoring". Clause 10(2) saw a number of amendments, rendering the clause far more complex. The Parliamentary Information and Research Service summed up the proposed changes nicely:

> The new clauses 10(2), and clauses 10(2.1)–10(2.5), state that only the function and purpose need to be stated, along with some additional details that depend on the type of installation. These details may include a description of the material elements that perform the program function and their reasonably foreseeable impact on the operation of the recipient's computer system (clause 10(2.1)(***a***) and (***b***)). These extra details must be provided if the installation will do one of the following: collect personal information stored on the computer system; interfere with the recipient's control of the computer system; change or interfere with the recipient's existing settings, preferences or commands; change or interfere with data that affects the recipient's lawful access to it; cause the recipient's computer system to communicate with another computer system or device without the recipient's consent; or install a computer program that may be activated by a third party without the knowledge of the recipient. Further criteria requiring the extra information to be provided for consent may be specified in the regulations (clause 10(2.2)). Exceptions to these requirements include the collection, use and communication of transmission data only, a program upgrade or update (provided the recipient has consented to receive updates and upgrades), cookies, HTML code, Java scripts, an operating system, any other program executable only through a program for which consent has already been given, any program to be specified in the regulations, and situations where it is reasonable to assume implicit consent from the recipient's conduct clauses 10(2.3)–10(2.5)).[79]

The result of these changes was essentially to provide the authority for rights holders and law enforcement agencies to spy on consumers for copyright enforcement or law enforcement, provided they made some indication to consumers that such monitoring would occur and state why. The theory appears to be that such disclosure will not be undertaken by "bad actors", namely those persons using spyware for purposes of keylogging or other frauds, while permitting "good actors" to remotely monitor consumers to alert them when the consumer him or herself does "bad things". The trade-off for consumers seems rather dubious; certainly the present anti-spam bill would have been more transparent to consumers had these

[79] Alysia Davies, "Bill C-27: The Electric Commerce Protection Act", *supra*, note 40.

exceptions not been stuffed into this bill but rather added to the copyright[80] and lawful access[81] bills and debated there.

Phishing

Phishing, is a major source of consumer concern (in our survey, it was the fourth highest rated threat, most concerning to young Quebecers). The Canadian Anti-Fraud Centre (formerly "Phonebusters") estimates phishing costs Canadian consumers over $1 million dollars annually (2009 figures)[82].

Phishing is indeed prohibited by Bill C-28, but in a confusing and multi-part way. First, it is important to note the misleading links would be covered under the definition of "commercial electronic message" in s. 2.(2), which encompasses not only the content of the email message, but also any hyperlinks contained in the message and the contact information of its sender. Since the "phisher" is likely unknown to the consumer, then under s. 7 of Bill C-28 (consent) the phisher will have no permission to send an e-mail, as they have no business or non-business relationship with the recipient and no other exemption. Also, subs. 8(1) refers to altering transmission data, so that if the message is delivered to another or a different destination, arguably this section applies if there is a reasonable disconnect between what the link appears to suggest the consumer will be led to and the actual site led to.

[80] See Bill C-32, An Act to amend the Copyright Act, Third Session, Fortieth Parliament, 59 Elizabeth II, 2010.

[81] See Bills C-50, An Act to amend the Criminal Code (interception of private communications and related warrants and orders) (Improving Access to Investigative Tools for Serious Crimes Act); C-51 An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (Investigative Powers for the 21st Century Act); and C-52, An Act regulating telecommunications facilities to support investigations (Investigating and Preventing Criminal Electronic Communications Act), Third Session, Fortieth Parliament, 59 Elizabeth II, 2010.

[82] In 2009, phishing was the 7th most reported scheme/pitch used to defraud Canadians, according to Phonebusters (it followed, in order: service, merchandise, sale of merchandise by complainant, prize, personal info, job). There were 1205 phishing complaints reported in Canada in 2009, about 1/10th of all "E-mail / Internet / Text Messaging" type complaints. The top solicitation method in 2009 was indeed "E-mail, Internet, Text Messaging," with a total dollar loss of over $14 million (this is more than double the next highest solicitation method, being "in person" with a dollar loss of under $6 million). Thus we calculate losses of over $1 million for phishing based upon this percentage. In a meeting of PIAC with the Canadian Anti-Fraud Centre, they confirmed they did not have a more detailed breakdown of E-mail vs Internet vs Text Messaging losses.

In addition, there is a regime which prohibits misleading statements or advertising and is handled by the Competition Bureau. In the amendments to the *Competition Act* found in Bill C-28, misleading links would be covered by the newly added definitions of locator and sender information. "Locator" means a name or information used to identify a source of data on a computer system, and includes a URL; "sender information" means the part of an electronic message — including the data relating to source, routing, addressing or signaling — that identifies or purports to identify the sender or the origin of the message; Locator and sender information are both referred to in the newly added ss. 52.01 (referring to telemarketing and competition), and 74.011 (deceptive marketing practices).

Finally, the phishing will not be allowed under exceptions to consent in PIPEDA: s. 83 of C-28, by creating new PIPEDA s. 7.1, removes that potential defence from the phisher. See in particular new s. 7.1(3) of C-28 which disallows collection of personal information by this method, no matter what is tried by the phisher with reference to implied consent, consent in privacy policies, etc., unless the collector described the process of collection by referring the person to the unexpected site and provided an opt-out (see s. 12(6) of C-28). Although complicated, the phishing sections appear to contemplate all known types of phishing attacks to prohibit them.

Business to Business Communications

The definition of "implied consent" provided by clause 10(3) also changed to include a "conspicuous publication" exception. This concept has been employed by Australia and New Zealand.[83] With this new exception, if a person publishes their email contact information in a place visible to others without explicitly stating that their email may not be used to send them unsolicited commercial messages, then that person may be contacted regarding matters connected to their business or official capacity. Once again, this solution represents a well-thought-out compromise between the problem of employee loss of productivity at work, and the company's desire to remain open to business offers that may advantage it – leaving the decision (and control) about how much commercial mail a business will accept up to the management of the company, not the views of other companies wishing to send unsolicited offers.

[83] Alysia Davies, "Bill C-27: The Electric Commerce Protection Act", *supra*, note 40.

Sale of a Business

Clause 10(4) sets out the criteria for implied consent that must be met for an existing business relationship to qualify. The question of whether this consent survived a sale or transfer of business was not clear in the original text of the Bill. Another clause that was added as the Bill passed through the House was clause 10(5.1).[84] This clause allows a business that purchases another business to inherit its existing business relationships without having to re-seek consent of all customers. We question if in all cases the blanket transfer of consent in this situation is appropriate, however, we note that customers still will be able to opt-out of future e-mails should they dislike the management of the new company, which company must, due to the disclosure requirements of the bill, set out its correct legal title and contact information.

Loans, Subscriptions and Memberships

Another special area is business and non-business relationships involving loans, subscriptions, memberships and similar arrangements. These have different rules governing existing business relationships. For these, clause 10(7) stipulates that a 2 year relationship period where the merchant may contact the consumer begins on the date that the loan, subscription, membership or other, ends.[85] This clause ensures that the consent implied to send messages does not end, for example, on the last day payment of a subscription was made, but rather on the last day of the subscription, presumably to allow re-contacting the individual within a reasonable time to renew. This again appears to be a compromise that accounts for a "transactional"-type arrangement (at least on the view of the marketer). Although consumers may not appreciate the 2 year window to try to draw them back into a subscription, the consumer can in this period always formally withdraw consent to these post-subscription solicitations.

Enforcement

The ECPA makes the CRTC the primary enforcement agency responsible for its anti-spam clauses. The CRTC may do this through the pursuit of administrative penalties.[86] The CRTC would also have been granted the power to require a person to produce a document or file in

---

84 *ECPA*, subs. 10(5.1).

85 *ECPA*, subs. 10(7).

86 *ECPA*, s. 14.

his or her possession for the purposes of an investigation.[87] The CRTC may apply for a warant from a justice of the peace to enter a place of business, examine anything there, test or use any means of communication there, examine or use any communication systems there, examine or use any computer systems, documents and copying equipment found there. It may also remove anything found on the premises for examination or restrict or forbid access to the premises as well.[88] Major monetary penalties may be imposed by the ECPA up to one million dollars for an individual or up to ten million dollars for a corporation, per violation. A violation occurs each day that an offence occurs and these maximum penalties may therefore be imposed for each day a violation is committed.[89] The CRTC also has powers similar to an injunction whereby they can force an offending party to stop contravening the law.[90] Any penalties recovered for ECPA violations are to be paid to the Receiver General for Canada.

One last, and key difference between the Anti-spam bills and the changes to the Telecommunications Act that created the National Do Not Call list, is that these bills both made an appropriation from government monies to run the administration. In short, the CRTC will, for the anti-spam administration, actually be funded directly by taxpayers. It can be expected that this financial freedom will permit more enforcement to be undertaken than the limited enforcement so far evidenced with the DNCL, however, with the money comes the responsibility to justify the expenses before Parliament. The latest bill, C-28, has a requirement for Parliament to review the Act within 3 years.[91] As a result, it appears important that monitoring of consumer complaints to the spam centre at the CRTC, the recording of enforcement actions, and the gathering of other primary information about the functioning of the various agencies under the new law should be compiled from the first day it is proclaimed and should be made available to the public for study.

Enforcement may well be the key differentiator between successful implementation of the anti-spam law in Canada and a dead letter law. Given that results likely will be demanded by Parliament when the Act comes up for review in 3 years, there may be pressure to have fined someone, and Canadian-based retailers and marketers may well be concerned that attention will fall upon them (since they are Canadian-based and subject to all administrative penalties under the Act), rather than foreign spammers who will only be investigated in Canada with a

87 *ECPA*, s. 17.
88 *ECPA*, s. 19.
89 *ECPA*, s. 20.
90 *ECPA*, s. 26.
91 Bill C-28, s. 66.

view to sharing this information with international partners. Nonetheless, the National Do Not Call list has shown that there is a considerable variation in size and type of non-conforming telemarketers in Canada (indeed, no large telecommunications company nor retailer has yet been fined) and it is likely that the new regime will reveal such spammers in Canada. Finally, PIAC's survey indicated a very high number of Canadians would make complaints to an anti-spam website about spam (71% were "very likely", or "likely" to make such a complaint), provided that such reporting were easy (see answers to question 10, the easiest method being simple forwarding to a spam complaints address, favoured by 50% of respondents). Should Canadians undertake the effort to complain about spam, it is very likely that they will expect concomitant enforcement of complaints.[92]

New Developments in Spam

Social networking and spam

Though spam typically refers to unwanted email messages, it is increasingly prevalent in other forms of electronic communication, such as social networking. All of the stakeholder experts consulted agreed that spammers were now targeting most of their energy upon social networking sites and new communications platforms, or soon would be. Social networking is rapidly becoming the most popular application for the internet. Social networking captures messages, comments, URLs, tags and other media generated by users and makes it available to other users on the network. The use and prevalence of applications such as instant messaging, social bookmarking pages and social networking sites has increased dramatically in a few short years. In March of 2010, the popular social networking site Facebook had eclipsed Google, the web's most popular search engine, in the number of visits by users.[93] Facebook today now has over 500 million registered users and expects to top 1 billion users.[94] With impressive figures such as these, it is difficult to deny the influence social networking is having on the online world.

---

[92] Although we are unaware of research directly on consumer satisfaction with the National DO Not Call List, there have been numerous press articles decrying the lack of enforcement under the DNCL, which quote frustrated Members of Parliament, who do, after all, have the power to continue or cancel such schemes. See, for example, Richard J. Brennan, "Enforcement of do-not-call list far too weak, critics say", (21 May 2010) Toronto Star. Online: http://www.thestar.com/news/canada/article/812831--enforcement-of-do-not-call-list-far-too-weak-critics-say

[93] Chris Nuttall and David Gelles: "Facebook become a bigger hit than Google" *The Financial* Times (March 16th, 2010) online: <http://www.ft.com/cms/s/2/67e89ae8-30f7-11df-b057-00144feabdc0.html>.

[94] Mark Sweeney, "Mark Zuckerberg: Facebook 'almost guaranteed' to reach 1 billion users" (23 June 2010) The Guardian. Online: http://www.guardian.co.uk/media/2010/jun/23/mark-zuckerberg-facebook-cannes-lions

Unfortunately, as social networking and media becomes more popular, it is also increasingly the target of spam. Their focus on user-generated content makes them more vulnerable to spam attacks. This spam can take many forms as well. Whereas conventional spam is usually an email message, social networking spam can take the form of a document, message, hyperlink, user profile or automated vote, among other forms. Additionally, the intentions behind social network spamming may also be different from conventional spam. Spammers may manipulate social networks for the purposes of self-promotion, disruption, attacking competitors or opponents and even simple curiosity.[95] This unwanted interference has the effect of undermining the network and reducing the confidence of its users.

Social networking spam differs from conventional spam in four important respects: [96]

1. *One controlling entity*: A single entity or owner manages the system's content and maintenance. This contrasts with email where a single message may pass over a variety of networks and servers all owned or administered by different parties.

2. *Well defined interactions*: The entity or owner in control of the network can constrain the ways users may interact by setting its own rules for its site or application. For example: social networking site may allow users to share comments, links and photos but nothing else. Traditional email is not constrained in the same way and email users can write whatever they wish and attach all kinds of different files.

3. *Identity*: On a social networking site or application, all of the content and actions on the system can be traced back to particular users. With conventional email, this is not possible and it is trivially easy to mask one's identity or impersonate another user.

4. *Multiple interfaces*: Social networking users enjoy different ways to access content on sites or applications. The way this content is organized can vary greatly. One example is the most frequently occurring data or content (a "tag cloud") or most recent contribution from a particular member. How and when this data is organized depends on an algorithm determined by the provider and this can vary from user to user. Therefore, a spammer can have different effects on different users with the same content or message, depending on how the site or application sorts it. In contrast, most email is usually organized and displayed to users chronologically. It is possible to organize email in different ways, but this is generally the default sorting method.

---

[95] Fighting spam on social websites; a survey of approaches and future challenges. Paul Heymann, Georgia Koutrika and Hector Garcia-Molina, *IEEE Computer Society (November 2007)*. Online: http://ilpubs.stanford.edu:8090/818/1/2007-34.pdf

[96] *Ibid.*

These characteristics make the relationship between service providers and spammers much different than in the case of traditional email. The social networking site or application administrator has much more control over how to enforce spammers using their service, as it remains under their sole control.[97] They are also able to determine what the past behaviour of their users might have been and may take their perceived intention into account when deciding how to react to them. On the other hand, spammers are able to attack social networking sites and applications in a variety of different ways, as opposed to a single one with traditional email spam. This means that social networking service providers have to protect multiple angles of attack and employ multiple strategies to have any hope of success. This means that while social networking providers have more control over their facilities, they are less able to predict how they will be compromised and have to consider many more possibilities.

Spam occurring on social networks is generally addressed using three possible strategies. Those strategies are identification-based (spam detection), rank-based (spam demotion) and interface or limit based (spam prevention).[98] These strategies may be used individually or in concert to try to combat the effects of spam over social networks. Not all of these strategies are applicable to all social networks and some may impose convenience or usability costs to social network users.

Identification-based strategies rely on detecting spam as it enters onto a social network. These strategies work in two steps. In the first step, content believed to be spam is identified either by pattern-based classification software or by the social networking users themselves. Individual users can flag messages suspected of being spam for inspection. Similarly, classification software can be programmed to analyze content and remove spam automatically, using the principles of statistical analysis and machine learning.[99] Classification software for social networking sites or applications will have to test several kinds of inputs such as comments, photos, URLs or tags and determine whether they constitute spam or not. This software looks for patterns or attributes that could indicate spam:[100]

[97] Supra note 3
[98] SpamClean: Towards Spam-free Tagging Systems. Ennan Zhai, Huiping Sun, Sihan Qing, Zhong Chen. 2009 International Conference on Computational Science and Egineering.
[99] Ibid.
[100] Supra note 3

Source Analysis: this examines the identities of the party who contributed the content

Text Analysis: this examines content for words or phrases that are commonly used by spammers such as names of pharmaceuticals commonly sold online or sexually explicit terms.

Link or Behaviour Analysis: this strategy examines the networks of content or users and tries to determine if it may constitute spam.

In addition to these forms of analysis, administrators can also examine the IP addresses of users and see if some particular IP addresses have a demonstrated association with spam. Also, unnatural behavior by particular users is often a sign of spam, as many spammers rely upon automated processes for distributing their material.

Rank-based spam detection strategies rely upon the ordering of content within a social network to reduce the visibility of content believed to be spam. This method of sorting is popular for web searches performed on the internet. The most popular results are displayed first, with the order of results descending with sequentially less popular content. In the case of social networking, rank based methods like TrustRank do not eliminate spam but rather, lower its rank so that it is effectively invisible to users.[101] Automatic ranking systems can be configured in a variety of ways to determine the most popular list. Content can be ranked by a user's reputation with the network, number of legitimate contributions, geographical location or any number of variables. The rank of content can also be controlled manually be users in addition to automatic means. If content appears on a social network that users believe to be spam, they can manually vote it down, lowering its rank and likelihood of being noticed. These methods do not eliminate spam on social networks but they are effective at minimizing its effect on the network users.

Interface or limit-based strategies attempt to make spamming on a social network more difficult in the first place.[102] They act as a sort of pre-emptive barrier to spammers. Social network designers can make spamming difficult by concealing some of the ways the network operates or by designing it in such a way as to make automated spamming more difficult. There are two common ways of blocking spammers; interface-based methods and limit-based

[101] Ibid
[102] Ibid

methods. Interface based methods make the process of spamming difficult over the social network. One popular method for doing so on social networks is the CAPTCHA. CAPTCHA stands for "completely automated public Turing test". The CAPTCHA is a type of challenge-response test to ensure that content entered into a social network is not generated by a computer. This usually consists of a user being required to decipher an obscured word or set of characters and enter them into the system in order to be allowed to proceed with posting something to a social network. Limit-based strategies work by imposing limits to user behavior that could be characteristic of spam.[103] Limits are typically imposed upon creating multiple accounts or logins, sending a large number of messages in a short period of time or posting links in some forms of social networking. These limits can be hard limits, such as forbidding more than one login per user or soft limits, such as imposing a 1 minute delay between messages.

All of these 3 strategies are useful for preventing spam from infiltrating social networks. However, the weak link, as always, is not so much the system but the user. One problem with enforcement of the proposed spam law to new platforms, in particular social networking sites, is that it will require that both the CRTC administrators become familiar with spam on these services and that users of these services become sensitized to recognizing and complaining about spam received on these platforms. It appears that since such websites are "semi-closed" and their users theoretically "known" to other users (simply because of the requirement to log in and in particular if a "friend" of a correspondent), that consumers may be more vulnerable to spam e-mails that have been engineered to appear to come from such a friend, but in fact are installing spyware such as keyloggers or other malware.

This vulnerability was exploited by the operators of the "Koobface" malware that highjacked, among other services, Facebook accounts to send messages apparently from a "friend" to others.[104] These messages contained links that, once clicked on, installed software that then nagged customers to solve CAPTCHAs (images of words meant to require real human interaction) which the attackers then used to create new accounts. The software installed also sent out new spam messages to friends of the infected users, tempting them to follow links and likewise become infected. New accounts and compromised accounts were then used to direct

[103] Supra note 3

[104] See Nart Villeneuve, "Koobface: Inside a Crimeware Network" (Toronto: Canada Centre for Global Security Studies and the Citizen Lab Munk School of Global Affairs, University of Toronto), at p. 6, Fig, 1. (November 12, 2010). Online: http://www.infowar-monitor.net/reports/iwm-koobface.pdf

users to pay per click advertising and nag them to install pay per installation software (itself spyware).[105]

The Koobface example indicates that investigation and enforcement of the new Canadian anti-spam law in the social networking environment may require acute technical skill, high cooperation with social networking site operators (who may be reticent to have government knowledge of the inner workings of their advertising networks, account operating details and number of users) and intensive interaction with international anti-spam and anti-fraud agencies (Koobface for example had command and control (central brain) servers and proxy servers for their botnet operating in several countries.

Nonetheless, the availability of a spam law and a will to pursue spammers in the enforcement end of the administration may prove effective in social networking spam. An example is the experience of the U.S.

The U.S. CAN-SPAM Act provides some useful protections to consumers regarding the propagation of unwanted commercial email, however, the law is largely a product of its time and does not seem to account for content other than email messages that could be considered spam. Social networking was nascent in 2003. There is no mention of social networking or any other technology in the definitions included in the CAN-SPAM Act.[106]

Despite the lack of specific provisions, U.S. judges have interpreted the CAN-SPAM act to apply to spammers who exploit social networks. The first such decision occurred in 2007 when a California federal court judge ruled in case between the social networking site MySpace and noted spammer Sanford Wallace. The judge applied the CAN-SPAM Act to instances of spam that did not occur over email, widening its interpretation. Wallace was found to have sent nearly 400,000 messages and left over 890,000 comments on MySpace from 320,000 “hijacked” accounts which had been stolen from legitimate users.[107] The court reasoned that:

[105] Ibid., at
[106] 15 USC 7702
[107] http://www.spamsuite.com/webfm_send/106

> The Plain language definition of "electronic mail address" entails nothing more specific than "a destination…to which an electronic mail message can be sent" and the references to "local part" and "domain part" and all other descriptors set off in the statute by commas represent only one possible way in which a "destination" can be expressed…As the Defendant himself points out, at the time the Act was passed in 2003, electronic messages could be sent in many ways including through "instant messaging" and the Court must presume that Congress was well of these various forms of electronic communications when it drafted the Act. The plain language of "electronic mail address" encompasses these alternate forms while also recognizing that the most commonly used form of electronic address was the traditional email address…To interpret the Act in the limited manner as advocated by Defendant would conflict with the express language of the Act and would undercut the purpose for which it was passed.[108]

The CAN-SPAM Act was applied again in 2008 when another Federal Court judge in California awarded $873 million in damages to Facebook, another social networking site, against a spammer who was exploiting the site.[109]

The wide interpretation given by the courts to the CAN-SPAM Act has helped it become a useful tool for combating spam on social networks. However, having clearer wording in the law which is technology neutral, but easily applicable to technologies such as social networking will help stop spam more effectively. If the law is written in an inclusive way, it becomes easier to interpret for law enforcement official and other non-lawyers who are trying to determine whether a particular practice is legitimate or not. This principle appears to have been applied to the new law forbidding spam in Canada, however, as noted, the other challenges of technical knowledge to investigate, cooperation with social networking website owners (who may often be U.S.-based) and the need for close international cooperation will make such work a chore.

Case Study: Could link spam be covered under Bill C-28?

Is link spam a "commercial activity" as per ss. 2.(1) and 2.(2) and thereby covered by Bill C-28?

More mundanely, perhaps, than social networking spam, there is a question regarding whether simple links left as "comments" on blogs would be considered "spam" and covered by Bill C-28, since this is not a message delivered to a particular recipient. To gauge the power and flexibility

[108] http://www.spamsuite.com/webfm_send/106. See pages 8 and 9.
[109] Please see the Facebook blog for more details: http://blog.facebook.com/blog.php?post=40218392130

of the new law, it is useful, therefore, to consider if this "link spam" would be caught by the new law.

There is an argument to be made that link spam is not commercial in character because increasing a site's search engine ranking (the goal of dropping URL-containing comments on opn blog comment pages) is not, in and of itself, profitable. Arguably, only after people click on the link or visit the site ranked in the search engine, then either purchase a product or click on an advertisement, is any profit is made. However, profit and commercial activity are not synonymous in the Act. Section 2(1) specifically mentions "any transaction, act or conduct whether or not the person who carries it out does so in the expectation of profit." While ranking high in a search list is not profitable in and of itself, it is still commercial in character because it is analogous to advertising. Link spam is a type of advertising that potentially increases traffic to a site, increases sales profits, and increases advertising profits. The expansive definition of commercial activity in the Act likely captures link spam even if link spam itself merely increases a search engine rank, because link spam promotes commercial activity by means of increased traffic, sales, and advertising.

Section 2(2) also seems to subsume link spam under its definition of "commercial electronic message." This section specifies that the content of the message, the hyperlinks, and the contact information can make it reasonable to conclude that the purpose is to encourage participation in a commercial activity. Regarding content, link spam is usually absent any meaningful content, relating minimally, if at all, to the blog, wiki, guestbook or discussion board in which it is posted; this makes apparent the self-serving, commercial nature of the link spam's content. Regarding the hyperlink, as discussed above, the posting of the hyperlink will itself increase the linked site's rank in search engines, whether or not people click the link within the blog or comment, making the posting of the hyperlink a form of advertising (a commercial activity).

Section 2(2) also includes the words "has as its purpose, or one of its purposes, to encourage participation in a commercial activity." This opens the definition to include messages that are somewhat related to the blog or discussion board in which they're posted, but that, by including a hyperlink, have as one of their purposes to encourage participation in a commercial activity.

Bill C-28 states that a commercial electronic message is one meant "to encourage participation in a commercial activity, including an electronic message that….a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land; b) offers to

provide a business, investment or gaming opportunity; c) advertises or promotes anything referred to in paragraph a) or b); or d) promotes a person….who does anything referred to in… a) to c), or who intends to do so." There is an argument to be made that this wording covers only the specific categories of electronic messages listed in subsections a), b), c) and d) , and that link spam may not fall directly under any of these categories. However, a stronger argument is that the listing of these categories simply means that these categories are included, not that only these are included. The purpose of s. 2(2) is to allow the recognition of commercial messages based on their content, their use of hyperlinks, and their contact information; this requires a purposive approach to interpreting "commercial electronic messages," as opposed to a limited, categorical approach.

In any case, it is probable that link spam would fall under the specific categories listed in one or more ways. First, link spam could be an offer to purchase a good under s. 2(2)(a) in the sense that it is promoting traffic to sites where visitors can purchase goods or view ads (a product or service that advertisers and webhosts profit from). Second, and more likely, link spam could be interpreted to be an "advertisement" or "promotion" of offers to purchase a product, good or service under s. 2(2)(c), as it promotes traffic to sites where products, goods, and services are advertised.

Is link spam the type of conduct the Act is meant to address?

Section 4 states that the Act is meant to discourage conduct that "impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities." In the digital age, ranking higher on a search engine is an extremely important advertising tool. Link spam distorts search engine results, hurting the reliability, efficiency and optimal use of search engines for online advertising, shopping, and other commercial activity.

Link spam also imposes additional costs on businesses and consumers by reducing people's use of blogs, wikis, guestbooks and discussion boards. Webpage hosts and advertisers make less money from their websites because people use blogs and discussion boards less when they are frustrated and confused by the presence of link spam on their pages. Webpage hosts and advertisers can invest in filters and programs to limit link spam, but this is at an additional cost to them.

Further, link spam undermines the confidence of Canadians in the use of electronic means of communication to carry out commercial activities in general. First, link spam distorts search engine rankings, which people passively rely on as an indicator of the reliability and popularity of the sites ranked. Canadians will lose confidence in shopping online when they have to scroll past several spam sites in the search engine list before coming to "real" websites where they can shop. Second, link spam blurs the lines between commercial and non-commercial activities online, confusing and frustrating consumers. When people use blogs and websites "for free," meaning not for their own commercial purposes, they will see link spam as a form of unwanted advertising, one that they can't control and one that violates their "personal" space, be it their blogs, discussions, social networking pages or the like. Canadians will lose confidence in the internet as a safe space to conduct personal and commercial activities without threat of being intruded upon by spam in general.

Does link spam fall under the requirements and prohibitions of s. 7(1), as understood using the definitions in s. 2(1)?

Although s. 7(1) seems to speak to the more traditional concept of "email" spam - a commercial electronic message sent to an electronic address where a person has not given prior consent, there is a strong argument that the terminology could equally apply to link spam. As discussed above, link spam is a "commercial electronic message" in that it is a message sent by means of telecommunication (text, sound, voice or image message – a typed URL address) for a commercial, advertising purpose. It is being "sent" the same way email spam is sent, using software that distributes messages en masse to lists of harvested addresses. A blogspot, wiki, guestbook, or social networking site is an "electronic address" in the sense that it is an electronic mail account or any similar account. "Any similar account" is a broad term and would likely include most online accounts like social networking accounts, blog accounts, online profiles and the like, where an account must be created and identified with a user, email, or computer account.

Further, the prohibited activity is sending the message without express or implied consent. Users of blogs and discussion boards may be said to impliedly consent to receive messages from others, as per the terms of service or reasonable expectations of using such sites. However, consenting to receiving messages does not mean consenting to receiving messages that have as their purpose, or one of their purposes, the promotion of commercial activity.

Thus "link spam" will mostly likely be captured by the purposes, definitions, requirements, and prohibitions in the Fighting Internet and Wireless Spam Act. The Act seems to be written broadly enough to encompass this type of spam, and new, unforeseen spam technologies as well. Hopefully, a purposive approach to interpreting the legislation will ensure that overseers use this act to fight link spam in the same way as other forms of spam.

The Canadian dimension to spam?

Canada is a well developed country and a member of the G8 group of nations. It is, to date however, the only G8 country without a dedicated anti-spam act. Canada has a world class economy and a sophisticated and modern internet network that is integral to its economy. As such, it is important that Canada do all that it can to protect its network and shield itself from the harmful effects of spam. It is because of these advantages Canadians enjoy and the lack of such laws that it has been alleged that Canada is a desirable spot for spammers to set up their operations.

There have been some prominent stories in the Canadian media that paint Canada as a haven for spammers. One such story involves Facebook and a lawsuit against a spammer who used the Facebook platform to distribute his commercial messages. Noted internet law professor, Michael Geist wrote an article about the case that appeared in the Toronto Star, Ottawa Citizen and the Tyee. This article entitled "Canada emerges as haven for spam" examines the case against the spammer who used Facebook to distribute very large numbers of spam messages.[110] The spammer targeted by the $873 million judgment operated out of Montreal. In Professor Geist's view, this case served as an important example of how Canada's laws are completely inadequate to address the problem of spam. At the time the article was written in 2008, there was no comprehensive law prohibiting spam in Canada and the ECPA had not yet been introduced.

The Facebook case demonstrates that spam is an issue facing Canada and action on the part of the federal government is required. Professor Geist's article mentions a study that demonstrates how significant spam originates from web-based email services like Hotmail or Gmail. The study in question finds that up to 80% of spam originates from web-based email

[110] Michael Geist, "Canada emerges as haven for spam" *The Toronto* Star (December 1, 2008) online: <http://www.thestar.com/sciencetech/article/546213>.

services and that Canada is ranked 5th among countries that send the most web-based email spam. Only Iran, Nigeria, Kenya and Israel send more web-based email spam than Canada does.

Canada has also been singled out as having a potential complication in dealing with spam in that it has a well-developed "hosting" market. Hosting providers allow domain name owners to "host" their domain with the hosting provider, who buys bulk bandwidth from ISPs and provides the computing resources to maintain webpages for a domain and, crucially, to act as a relay for electronic mail delivered to email addresses associated with the hosted domain. The allegation is that many such hosting companies may be less diligent in filtering spam and also may inadvertently host spammers, being run as lean operations. PIAC was unable to find sufficient research documenting this supposed phenomenon, although security researchers noted that Canada was a special case in spam research due to its large hosting community.[111]

Since Bill C-28 applies to all internet intermediaries, including ISPs and hosting companies, it may be that the hosting phenomenon will be reduced once the enforcement of the new act comes into being. It is worth studying this market further, however, in order to help the CRTC decide where to allocate scarce enforcement resources.

Technical, practical, non-legal solutions to spam

Several technical innovations resulting from work of private email providers and the Internet Engineering Task Force have been rolled out recently in efforts to control spam at the ISP and other internet Intermediary level. All are variants of some form of sender authentication. Sender authentication is required and an obvious solution because the original electronic mail delivery protocols (SMTP – simple mail transfer protocol, and various later iterations) on the Internet allowed the "mail transfer agent" – the entity doing the actual email transfer – to be different from the actual sender.[112]

---

[111] Van Eeten et al., The Role of Internet Service Providers in Botnet Mitigation, supra, at p. 24, noting that up to 90% of spam originates within ISPs in certain countries, but in Canada is under 50%, perhaps due to hosting: "On the low end, we find Canada, with around 47%, which might be explained by the fact that Canada has a large hosting provider industry that contributes a significant number of spam sources."

[112] See http://www.wikipedia.org/wiki/Dkim Note that SMTP permitted use of "standard" port 25 to relay outgoing email messages, meaning a user could use any mail server with port 25 open to send mail. Such "open relays" have been all but eliminated in commercial email and ISP situations, and the rest blacklisted by spam filter companies, meaning a user must authenticate himself or herself on the new standard "submission" port, 587.

These methods include Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Whitelisting.

Sender Policy Framework

With Sender Policy Framework or SPF, internet intermediaries can specify which hosts are permitted to send email from their domains in a policy statement. This stops forged sender addresses or "return-paths". The recipient machines check any mail claiming to be from the domain against the SPF policy of the domain at the domain name servers. This requires recipients to be configured to do the actual checking. If they do not, and just accept email from the domain without checking, then SPF is ineffective. Likewise, SPF can pose a problem to users of the domain if they try to forward legitimately received messages to another domain. This latter problem can be solved if the domain the forwarded message is coming from is whitelisted by the receiver system (see "Whitelisting" below).

Domain Keys Identified Mail

Domain Keys Identified Mail relies upon public key encryption to digitally sign the message and to associate it with a particular domain. In this way, both the message source and the contents can be verified as originated from a particular domain and thus be "genuine". The public encryption key required to unlock the signature is stored at the DNS server and is downloaded along with the email carrying the additional email header field "DKIM-signature". DKIM is particularly effective in reducing phishing emails, as phishers theoretically cannot generate signed messages claiming to be from particular domains. Thus providers like Gmail use DKIM especially to ensure that only legitimate e-mails from, for example, Ebay or PayPal are delivered, but not phishing attempts.

DKIM's vulnerabilities are the same as most other public key encryption, that is, if a fraudster infiltrates the sender and gets the digital key, they can sign spam if they are able to send it from within the domain. DKIM also requires additional processing power at the DNS server and client end, as well as the sender.

Whitelisting

Whitelisting can be used to address spam. An e-mail "whitelist" can be created to define a list of "safe" e-mail senders and recipients to control spam.[113] Most e-mail whitelists currently exist to certify "good" bulk e-mail marketers to improve e-mail marketing delivery rates, not necessarily to filter out commercial electronic mail for an individual user.

Spamhaus launched anti-spam whitelists of known benign internet mail servers in October 2010.[114] The concept and policy of the Spamhaus whitelist is radically different to that of existing whitelists, in that it approaches whitelisting from the perspective of the recipient, which means trusting a sending server to never deliver spam. The only way Spamhaus trusts a server is where the server owner knows all of the server's users, hence the Spamhaus mantra "Know Your User."

The Spamhaus whitelists allow mail servers to separate incoming e-mail traffic into three categories: good, bad and unknown. Bad e-mail is blocked while the good e-mail traffic passes through safely. Any unknown e-mail is heavily filtered. For e-mail recipients, Spamhaus claims that their whitelists will end false positives from scoring systems, content filters, local blacklists or poor filtering choices. For e-mail senders, the Spamhaus whitelists will end important mail delayed, lost in junk filters or wrongly filtered as spam.

According to Spamhaus, one driver for the new service is the arrival of IPv6 spam, the next-generation protocol that will allow more addresses on the internet:

> Once IPv6 mail starts flowing in earnest, the volume of IPv6 spam -- in particular the potential volume of sources that can send spam in IPv6 -- risks overwhelming current filter technologies. … Blocklists designed to store millions of bad IP addresses suddenly need to cope with potentially billions of bad IP addresses. Yet legitimate mail servers in the world number only a few hundred

[113] Noncommercial and commercial e-mail whitelisting solutions are discussed in PIAC's report, "Whitelisting for Cyber Security: What It Means for Consumers" (November 2010). Online: http://www.piac.ca/files/whitelisting_final_nov2010.pdf

[114] The Spamhaus Whitelist: http://www.spamhauswhitelist.com/en/.

> thousand. It thus becomes sensible to identify and single out the few hundred thousand to let past unimpeded.[115]

The Spamhaus whitelist is designed for transactional e-mail such as from ecommerce systems, banks, automated billing and travel booking systems and important mail such as from medical centers, known corporations, organizations and government agencies. Marketing or soliciting bulk e-mail of any sort are not allowed. Notably, Spamhaus defines transactional e-mail as "relationship e-mail" and fits into a narrow category of business-to-client messages that:

> 1. Facilitate or confirm a commercial transaction that the recipient already has agreed to;
> 2. Gives warranty, recall, safety, or security information about a product or service the recipient has obtained;
> 3. Gives information about a change in terms or features or account balance information regarding a membership, subscription, account, loan or other ongoing commercial relationship;
> 4. Provides information about an employment relationship or employee benefits;
> 5. Delivers goods or services as part of a transaction that the recipient already has agreed to. [116]

Where a message combines commercial or marketing with transactional content and the recipient would reasonably interpret the subject line of the e-mail to conclude that the message contains an advertisement or promotion for a commercial product or service, the Spamhaus whitelist considers that e-mail to be a commercial e-mail. Where an organization sends both transactional and bulk mail, in order to be eligible for the Spamhaus whitelist, the organization must separate their mail streams.

In the context of the legislative framework for spam currently contemplated by the Canadian Parliament, the Spamhaus whitelisiting solution will fit well as eligibility for the Spamhaus whitelist is limited to transactional e-mail, which is defined even more narrowly than the "existing business relationship" exception in the Bill. In fact, it appears to cover the entirety of the "transactional" exception found in (Bill C-28) subs. 7(6) which reads:

---

[115] Search Security, "Spamhaus launches antispam whitelist to end spam false positives" (7 October 2010), online: http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci521551,00.html.

[116] Spamhaus Whitelist FAQ: "What is 'transactional email'?" online: http://www.spamhauswhitelist.com/en/faq.php.

7. (6) Paragraph (1)(a) [which requires explicit or implicit consent of the recipient for sending of commercial electronic messages] does not apply to a commercial electronic message that solely

(a) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land, if the quote or estimate was requested by the person to whom the message is sent;

(b) facilitates, completes or confirms a commercial transaction that the person to whom the message is sent previously agreed to enter into with the person who sent the message or the person — if different — on whose behalf it is sent;

(c) provides warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased;

(d) provides notification of factual information about

(i) the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or the person —if different—on whose behalf it is sent,

or

(ii) the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent;

(e) provides information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved, is currently participating or is currently enrolled;

(f) delivers a product, goods or a service, including product updates or upgrades, that the person to whom the message is sent is entitled to receive under the terms of a transaction that they have previously entered into with the person who sent the message or the person — if different — on whose behalf it is sent;

or

(g) communicates for a purpose specified in the regulations.

The Spamhaus whitelist may provide a more useful whitelisting e-mail solution than transitional whitelists because only transactional e-mail desired by the consumer will be delivered safely and unknown e-mail will need to pass through filters, eliminating bulk e-mail passing through as "safe". As such it may complement the regulatory framework envisaged by Bill C-28 perfectly.

While there are a whole host of technical solutions to slowing the flow of spam, many of them are rapidly outdone and overridden by spammers. Any technical solution offered here today risks becoming obsolete tomorrow in the rapid arms race between spammers and spam counter-measures. Nonetheless, certain of the technical measures adopted can make it harder for spammers to ply their trade and should be pursued in the provider community. Certain solutions, such as whitelisting, may play a larger role where their function can be complementary to a particular exception in a comprehensive spam law, such as the Spamhaus whitelisting service and the "transactional" exceptions allowed to companies doing business with consumers.

Consumer Awareness and Education

A significant percentage of consumers are ignorant of the risks posed by spam. In spite of many high-profile cases of spam in the media, many consumers continue to open spam messages, exposing themselves to different risks. The Ipsos Messaging Anti-Abuse Working Group (MAAWG) produced a study that examined the behaviour of consumers who had opened spam messages from their email inbox. Almost half of the people surveyed (46%) admitted they had deliberately opened a spam message.[117] Of these consumers, 15 percent said they were interested in the product or service being offered, 18 percent wanted to "see what would happen" and a surprising 4 percent even forwarded spam messages to other people.[118] These figures demonstrate a lack of understanding that opening of spam e-mails can lead to malware installation and following links can lead to "drive-by downloads" on infected websites – both of which can lead to threats not only to a consumer's computer but those of others. More surprising still, is the fact that 44 percent of the consumers surveyed said they considered themselves "somewhat experienced" in protecting themselves from online security threats

[117] Jacqui Cheng, "Idiot users still intentionally opening, clicking on spam" *Ars Technica* (April 2010) online: <http://arstechnica.com/business/news/2010/03/idiot-users-still-intentionally-opening-clicking-on-spam.ars>.

[118] ibid

while an additional 20 percent of those surveyed considered themselves as "experts"[119] The bulk of users that engage in "risky e-mail behavior" consists of males under the age of 35.[120] This is also surprising as it is more likely that members of this group that consider themselves to be more experienced when dealing with internet security threats. This study demonstrates that despite considerable public awareness and education, spam is still able to pose a significant risk to consumers, even those that consider themselves savvy computer and internet users. What amount of such recklessness is due to behavioural factors (and thus outside of the scope for much education) and what amount simple ignorance of how spam works is unclear and would seem an area ripe for study. Consumers need to be better educated about the risks posed by spam. Even seemingly innocuous actions such as replying to a spam message can pose risks to them, in this case by confirming that a consumer has read a spam message and that their account is active to receive more spam.

The issue of better consumer education was raised in the Spam Taskforce's Report on Spam. The federal government initiated a project called "Stop Spam Here", which is a program that seeks to educate consumers on the risks posed by spam and spammers. However, it is not clear that there was any structured evaluation of the effectiveness of this campaign. The website currently contains information on "Bill C-27", the ECPA, which has been replaced by Bill C-28.

The new anti-spam administrators, the CRTC, should encourage renewed participation in the campaign by providers and update and host all materials. Future efforts in this campaign should be monitored and reported by the new anti-spam administration to Parliament upon review of Bill C-28 in three years time (provided the Bill is proclaimed into law).

Enforcement

Bill C-28 has a a range of penalties that may be imposed upon offenders. They also grant the CRTC powers of investigation which are necessary for the enforcement anti-spam provisions. Some of our expert stakeholders feared this power would be wielded unfairly, while others thought it would be used very leniently. What is the right mix?

[119] Ibid

[120] Interestingly, in PIAC's study, for one risky action "reply to sender", women were three times more likely to reply to spam than men (but this was a small sample, 3% as opposed to 1%). PIAC survey, question 3.

There is evidence that a public and active approach to strong penalties can dissuade all spammers. Holland very recently introduced anti-spam legislation in October 2009. Dutch internet security experts SpamExperts examined the effect of the law 5 months after it was introduced. They recorded a drop of 85% in "semi-legitimate" spam messages, which were in part advertisements from business to business but also included business to consumer spam.[121] Additionally, the Dutch OPTA (Independent Mail and Telecommunication Authority) quickly investigated over 10,000 complaints concerning spam and in those 5 months issued 39 official warnings to businesses engaged in spamming. OPTA can impose fines that are comparable to those in Bill C-28, namely, up to 45,000 Euros.

There is some reason to be concerned that Canada will not take such a proactive approach as the Netherlands in enforcement of Bill C-28. The enforcement of the similar regime under the National Do Not Call List legislation has been somewhat erratic owing in part to the requirement that the CRTC Commissioners must approve all administrative monetary penalties (AMPs). Bill C-28 has a similar requirement. In addition, the Commissioner of the CRTC, in hearings before the Industry Committee on Bill C-27, the ECPA, noted that the Commission will likely favour asking violators to give an undertaking to comply with the Act, rather than reach automatically for a notice of violation. Finally, there is an appeal mechanism, even on a question of fact, with leave, to the Federal Court of Appeal.[122]

One new tool is the power to apply to a court for a civil injunction top halt a particular spammer.[123] This tool was favoured by 21% of respondents to PIAC's spam survey as the most effective method for stopping spammers. Given that much spam, especially of the phishing and other fraud-based types is sent over long weekends, when consumers may be at their home computers and more vulnerable to such pitches, it may be wise for the CRTC to consider launching such an injunction application early that week, given the section requires at least 48 hours notice of the application.

One last method for enforcement is the inclusion of a private right of action open to both consumers as recipients of spam and to network and email operators to sue spammers for statutory damages of up to $200 a message to a maximum of $1,000,000 a day.[124] While this

[121] SpamExperts Press release, April 13, 2010
[122] Bill C-28, s. 28.
[123] Bill C-28, s. 42.
[124] Bill C-28, s. 48.

right appears to be a large stick, if the CRTC accepts an undertaking or issues a notice of violation in respect of the spammer and incident, the action is not permitted to proceed. It is hard to imagine a situation where such a notice will not be issued nor an undertaking given, unless the CRTC voluntarily chooses not to proceed in this manner or takes the position that there is no violation. Thus it is possible this threat will not materialize often. The intent appears to leave discretion in the CRTC to quash any private actions against "reputable" companies that can be disciplined with fines or undertakings, leaving actions to proceed against "bad" spammers who are supported by their spamming business rather than running a business with occasional marketing lapses. This saw-off may be appropriate, depending upon the attitudes of "responsible" companies caught spamming and, crucially, the frequency and especially the scale of AMPs the CRTC may require of companies that claim to make mistakes in spamming. It is of note that this posture may be a fair reflection of public attitude: only 9% of Canadians saw a private right of action as the best way to control spam,[125] however, it was still a significant minority.

Conclusions

Canada's long-awaited anti-spam law may well see the day it is implemented. Canadian consumers have too long suffered from the lack of a clear, enforceable legal framework to assist in the control of spam. One effect of Canada lagging in bringing this framework forward only in 2010 is that it has permitted the law to be tailored to realities of the present age regarding spam, including the seismic shift from centrally distributed spam to distributed sending via botnets that are themselves in control of consumers' computers. Consumers appear aware vaguely of their role in spam propagation and perhaps in denial regarding it. However, they appear very supportive of an anti-spam law and indeed, on all major points where the proposed bill had to take a policy direction, such as express consent and opt-outs, with some exceptions, they appear to agree almost entirely with the approach of the bill.

Challenges remain, including the move of spam into new platforms as fast as they appear, such as social networking sites and the question of the administration and especially enforcement of the new act. However, provided the new framework is appropriately administered and enforced, it may well be that Canada has turned a corner on the spam problem and there may be brighter and cleaner days ahead. Can we can spam in Canada? Maybe we can.

[125] See PIAC survey, question 6.

Recommendations

Despite the optimism that developments on the legal front may have in Canada, there are still a number of areas where the manner of the implementation of anti-spam legislation may make a huge difference to consumers' actual experience with spam over the coming few years. The new law should be given some time to operate under the control of the CRTC/Competition Bureau/Privacy Commissioner administration before radical changes are made to any aspect of the regime, however, implementation issues will be the key to success.

Based on the research in this report, including our survey, and our general consumer protection experience and specific electronic commerce experience, PIAC therefore makes the following recommendations.

1. **There should be intensive monitoring of spam volumes at the ISP/third party e-mailer level. Such data should be made available to researchers.**

   Much of the spam that is filtered out by ISPs is unseen by customers. Although it does not reach consumers for the most part, it causes significant costs to ISPs and email providers, who may have to pass on such costs to consumers. Since this metric is so large and is generally consistent, any positive effects of the new spam law in Canada may be detectable by researchers. Since individual ISPs usually do not share such data, measurement of effects is difficult. CRTC as administrator of the new regime may be best placed to attempt to compile this data from ISPs and email providers and will be able to compare it to the spam reporting centre data forwarded by consumers. Such compiling and comparing of data will also ensure consumers' efforts in reporting spam will not be in vain.

2. **The Government of Canada should fund consumer polling and qualitative research on the effect on consumers of the law.**

   There also will be a lack of data and research on the qualitative and quantitative on the actual effect upon consumers of the new anti-spam law unless polling and focus group research is funded by governments. Given the superstructure of administration and enforcement to pursue spam, it is necessary to carefully monitor the actual experience of users with spam once the regime is in place.

3. **The Government of Canada should fund independent research into the effects of the law on e-mail providers and marketers (in particular on social networking sites, wireless platforms and other new means of communication).**

   When the present law comes up for review in 3 years from its passage, the government must have independent assessments of the effect upon ISPs, email providers and in

particular online marketers in order to make a balanced assessment of the law's real impact upon the Internet economy in Canada. Given the stated purpose of this regime, to grow Canadian e-commerce, it is responsible for the government to have such information for analysis rather than relying upon colourable reports by marketers.

Research into the effects of the law in new spaces such as wireless and social networking will assist the CRTC in applying the Act in these areas and also will permit Parliament to determine if the Act as written is capable of functioning in these new areas to protect consumers.

4. **The CRTC, Competition Bureau and Office of the Privacy Commissioner of Canada should undertake intense enforcement efforts under the new anti-spam law, in particular during its initial phases.**

   Serious enforcement of the new spam rules will send an immediate message to those marketing by electronic means in Canada that there are, after many years, new rules in Canada. The general public will be impatient for some evidence of spam reduction or at least reduction in the most harmful spam in the short term. Anemic enforcement, such as that that has taken place so far with the Do Not Call list will be the subject of both negative press and questioning by federal politicians. Such a poor start would potentially jeopardize the anti-spam law when it comes up for review in the very short time period suggested in Bill C-28 of only 3 years. Given that Canada may indeed be a "haven" for at least certain types of spam or spammers, there should be egregious examples which can be more easily pursued in the short term, which will also help signal to good actors as well as bad that Canada no longer intends to tolerate spammers.

5. **The CRTC, as primary administrator of the new anti-spam law should undertake widespread consumer education about the new regime, especially amongst younger Canadians.**

   Knowledge of this law amongst users will once again put spam on the consumer radar. Since consumers, when asked, do have opinions on spam and clearly dislike it, they also have made accommodations to use email as part of their lives despite its many failings. Giving them hope that email may actually improve as a communications method, while assuring them of the application of the law to new platforms such as social networking and wireless, should indeed encourage electronic commerce with consumer protection, which has been somewhat absent in Canada. Younger Canadians have grown up without a regime in place to control spam; as a result, they must be told that spam is not a reality they must "live with" while attempting to navigate the Internet and run their lives.

6. **The Government of Canada should strike a new Task Force on Spam to inform Parliamentarians of progress on the problem when the law is reviewed in three years.**

The many technical efforts of ISPs and email providers to halt spam will need to be integrated with the new Canadian spam law. Marketers will have problems with it and adapt. Retailers will either be comfortable with it or not, depending on enforcement. Consumers may or may not benefit from the law. Academics may have new insights into spam in the new environment. All of these parties need to sit down to discuss these matters prior to the review of the anti-spam regime by parliament. The spirit that drove the initial Task Force report would be valuable in making that review a positive experience for all players, instead of a chance to square off in the usual corners, with the only possible knockout being Canada's nascent spam law.

Appendix 1 – ECPA (Bill C-27) versus Bill C-28 ("FISA")

Item	**ECPA Provisions**	**C-28 "FISA" Provisions**
Definitions	**2.** (1) The following definitions apply in this Act. "commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada. "computer program" has the same meaning as in subsection 342.1(2) of the *Criminal Code.* "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "electronic address" means an address used in connection with the transmission of an electron- ic message to (*a*) an electronic mail account; (*b*) an instant messaging account; (*c*) a telephone account; or (*d*) any similar account. "electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message. (2) For the purposes of this Act, a commercial electronic message is an electronic	**2.** (1) The following definitions apply in this Act. "commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada. "computer program" has the same meaning as in subsection 342.1(2) of the *Criminal Code.* "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "electronic address" means an address used in connection with the transmission of an electron- ic message to (*a*) an electronic mail account; (*b*) an instant messaging account; (*c*) a telephone account; or (*d*) any similar account. "electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message. (2) For the purposes of this Act, a

	message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that (*a*) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land; (*b*) offers to provide a business, investment or gaming opportunity; (*c*) advertises or promotes anything referred to in paragraph (*a*) or (*b*); or (*d*) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (*a*) to (*c*), or who intends to do so. (3) An electronic message that contains a request for consent to send a message described in subsection (2) is also considered to be a commercial electronic message. (4) An electronic message described in subsection (2) or (3) that is sent for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada is not considered to be a commercial electronic message. (5) For the purposes of this Act, a reference to the person to whom an electronic message is sent means the holder of the account associated with the electronic address to which the message is sent, as well as any person who	commercial electronic message is an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that (*a*) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land; (*b*) offers to provide a business, investment or gaming opportunity; (*c*) advertises or promotes anything referred to in paragraph (*a*) or (*b*); or (*d*) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (*a*) to (*c*), or who intends to do so. (3) An electronic message that contains a request for consent to send a message described in subsection (2) is also considered to be a commercial electronic message. (4) An electronic message described in subsection (2) or (3) that is sent for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada is not considered to be a commercial electronic message. (5) For the purposes of this Act, a reference to the person to whom an electronic message is sent means the holder of the account associated with the electronic address to

	it is reasonable to believe is or might be authorized by the account holder to use the electronic address.	which the message is sent, as well as any person who it is reasonable to believe is or might be authorized by the account holder to use the electronic address.
Spam	**6.** (1) No person shall send or cause or permit to be sent to an electronic address a commercial electronic message unless (*a*) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and (*b*) the message complies with subsection (2). (2) The message must be in a form that conforms to the prescribed requirements and must (*a*) set out prescribed information that identifies the person who sent the message and the person — if different — on whose behalf it is sent; (*b*) set out information enabling the person to whom the message is sent to readily contact one of the persons referred to in paragraph (*a*); and (*c*) set out an unsubscribe mechanism in accordance with subsection 11(1) (3) The person who sends the commercial electronic message and the person — if different — on whose behalf the commercial electronic message is sent shall ensure that the contact information referred to in paragraph (2)(*b*) is valid for a minimum of 60 days after the message has been sent.	**7.** (1) It is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless (*a*) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and (*b*) the message complies with subsection (2). (2) The message must be in a form that conforms to the prescribed requirements and must (*a*) set out prescribed information that identifies the person who sent the message and the person — if different — on whose behalf it is sent; (*b*) set out information enabling the person to whom the message is sent to readily contact one of the persons referred to in paragraph (*a*); and (*c*) set out an unsubscribe mechanism in accordance with subsection 12(1). (3) The person who sends the commercial electronic message and the person — if different — on whose behalf the commercial electronic message is sent must ensure that the contact information referred to in paragraph (2)(*b*) is valid for a minimum of 60

		days after the message has been sent.
	(4) For the purposes of subsection (1)	(4) For the purposes of subsection (1)
	(*a*) an electronic message is considered to have been sent once its transmission has been initiated; and	(*a*) an electronic message is considered to have been sent once its transmission has been initiated; and
	(*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination.	(*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination.
	(5) This section does not apply to a commercial electronic message	(5) This section does not apply to a commercial electronic message
	(*a*) that is sent by or on behalf an individual to another individual with whom they have a personal or family relationship, as defined in the regulations;	(*a*) that is sent by or on behalf of an individual to another individual with whom they have a personal or family relationship, as defined in the regulations;
	(*b*) that is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity; or	(*b*) that is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity; or
	(*c*) that is of a class, or is sent in circumstances, specified in the regulations.	(*c*) that is of a class, or is sent in circumstances, specified in the regulations.
	(5.1) Paragraph (1)(*a*) does not apply to a commercial electronic message that solely	(6) Paragraph (1)(*a*) does not apply to a commercial electronic message that solely
	(*a*) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land, if the quote or estimate was requested by the person to whom the message is sent;	(*a*) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land, if the quote or estimate was requested by the person to whom the

	(*b*) facilitates, completes or confirms a commercial transaction that the person to whom the message is sent previously agreed to enter into with the person who sent the message or the person — if different — on whose behalf it is sent; (*c*) provides warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased; (*d*) provides notification of factual information about (i) the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or the person — if different — on whose behalf it is sent, or (ii) the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent; (*e*) provides information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved, is currently participating or is currently enrolled; (*f*) delivers a product, goods or a service, including product updates or upgrades, that the person to whom the message is sent is entitled to receive under the terms of a transaction that they have previously entered into with the person	message is sent; (*b*) facilitates, completes or confirms a commercial transaction that the person to whom the message is sent previously agreed to enter into with the person who sent the message or the person — if different — on whose behalf it is sent; (*c*) provides warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased; (*d*) provides notification of factual information about (i) the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or the person — if different — on whose behalf it is sent, or (ii) the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent; (*e*) provides information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved, is currently participating or is currently enrolled; (*f*) delivers a product, goods or a service, including product updates or upgrades, that the

	who sent the message or the person — if different — on whose behalf it is sent; or (*g*) communicates for a purpose specified in the regulations. (6) This section does not apply to a telecommunications service provider merely because the service provider provides a telecommunications service that enables the transmission of the message. (7) This section does not apply to a commercial electronic message (*a*) that is, in whole or in part, an interactive two-way voice communication between individuals; (*b*) that is sent by means of a facsimile to a telephone account; or (*c*) that is a voice recording sent to a telephone account.	person to whom the message is sent is entitled to receive under the terms of a transaction that they have previously entered into with the person who sent the message or the person — if different — on whose behalf it is sent; or (*g*) communicates for a purpose specified in the regulations. (7) This section does not apply to a telecommunications service provider merely because the service provider provides a telecommunications service that enables the transmission of the message. (8) This section does not apply to a commercial electronic message (*a*) that is, in whole or in part, an interactive two-way voice communication between individuals; (*b*) that is sent by means of a facsimile to a telephone account; or (*c*) that is a voice recording sent to a telephone account.
Altering Transmission Data	**7.** (1) No person shall, in the course of a commercial activity, alter or cause to be altered the transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender, unless the alteration is made with the express consent of the sender or in accordance with a court order.	**8.** (1) It is prohibited, in the course of a commercial activity, to alter or cause to be altered the transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender, unless (*a*) the alteration is made with the express

	(2) Subsection (1) does not apply if the alteration is made by a telecommunications service provider for the purposes of network management.	consent of the sender or the person to whom the message is sent, and the person altering or causing to be altered the data complies with subsection 12(4); or (*b*) the alteration is made in accordance with a court order. (2) Subsection (1) does not apply if the alteration is made by a telecommunications service provider for the purposes of network management.
Installation of a computer program	**8.** (1) No person shall, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system, unless the person has obtained the express consent of the owner or an authorized user of a computer system or is acting in accordance with a court order. (2) A person contravenes subsection (1) only if the computer system is located in Canada at the relevant time or if the person either is in Canada at the relevant time or is acting under the direction of a person who is in Canada at that time.	**9.** (1) A person must not, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system, unless (*a*) the person has obtained the express consent of the owner or an authorized user of the computer system and complies with subsection 12(5); or (*b*) the person is acting in accordance with a court order. (2) A person contravenes subsection (1) only if the computer system is located in Canada at the relevant time or if the person either is in Canada at the relevant time or is acting under the direction of a person who is in Canada at the time when they give the directions.
Contravention	**9.** No person shall procure or cause to be procured the doing of any act contrary to any of sections 6 to 8.	**10.** It is prohibited to aid, induce, procure or cause to be procured the doing of any act contrary to any of sections 7 to 9.
Express consent	**10.** (1) A person who seeks express consent for the doing of an act described in any of sections 6 to 8 must, when requesting consent, set out clearly and simply the following	**11.** (1) A person who seeks express consent for the doing of an act described in any of sections 7 to 9 must, when requesting consent, set out clearly and simply the following

	information:	information:
	(*a*) the purpose or purposes for which the consent is being sought;	(*a*) the purpose or purposes for which the consent is being sought;
	(*b*) prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies that other person; and	(*b*) prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies that other person; and
	(*c*) any other prescribed information.	(*c*) any other prescribed information.
	(2) A person who seeks express consent for the doing of any act described in section 8 must, when requesting consent, also describe clearly and simply the function, purpose and impact of every computer program that is to be installed if the consent is given and set out any other prescribed information.	(2) Despite paragraph (1)(*b*), for the purposes of section 7, if a person is seeking express consent on behalf of a person whose identity is not known,
	(3) Consent is implied for the purpose of section 6 only where the person who sends the message, the person who causes it to be sent or the person who permits it to be sent has an existing business relationship or an existing non-business relationship with the person to whom it is sent, or in the circumstances set out in the regulations.	(*a*) the only information that is required to be provided under that paragraph is prescribed information that identifies the person seeking consent; and (*b*) the person seeking consent must comply with the regulations in respect of the use that may be made of the consent and the conditions on which the consent may be used.
	(4) In subsection (3), "existing business relationship" means a business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from	(3) A person who seeks express consent for the doing of any act described in section 9 must, when requesting consent, also, in addition to setting out any other prescribed information, clearly and simply describe, in general terms, the function and purpose of the computer program that is to be installed if the consent is given.
	(*a*) the purchase or lease of a product, goods, a service, land or an interest or right in land, within the 18-month period immediately preceding the day on which the message was	(4) In addition to the requirements set out in subsections (1) and (3), if the computer program that is to be installed performs one or more of the functions described in subsection

	sent, by the person to whom the message is sent from any of those other persons; (*b*) the acceptance by the person to whom the message is sent, within the period referred to in paragraph (*a*), of a business, investment or gaming opportunity offered by any of those other persons; (*c*) the bartering of anything mentioned in paragraph (*a*) between the person to whom the message is sent and any of those other persons within the period referred to in that paragraph; (*d*) a written contract entered into between the person to whom the message is sent and any of those other persons in respect of a matter not referred to in any of paragraphs (*a*) to (*c*), if the contract is currently in existence or expired within the period referred to in paragraph (*a*); or (*e*) an inquiry or application, within the six-month period immediately preceding the day on which the message was sent, made by the person to whom the message is sent to any of those other persons, in respect of anything mentioned in any of paragraphs (*a*) to (*c*). (5) For the purposes of subsection (4), the following organizations are considered to be businesses: (*a*) a cooperative as defined in subsection 2(1) of the *Canada Cooperatives Act*; (*b*) a cooperative corporation as defined in section 2 of the *Cooperative Credit Associations Act*; and	(5), the person who seeks express consent must, when requesting consent, clearly and prominently, and separately and apart from the licence agreement, (*a*) describe the program's material elements that perform the function or functions, including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system; and (*b*) bring those elements to the attention of the person from whom consent is being sought in the prescribed manner. (5) A function referred to in subsection (4) is any of the following functions that the person who seeks express consent knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system: (*a*) collecting personal information stored on the computer system; (*b*) interfering with the owner's or an authorized user's control of the computer system; (*c*) changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system; (*d*) changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts or interferes with lawful

	(*c*) any similar organization incorporated under an Act of Parliament or the legislature of a province. (6) In subsection (3), "existing non-business relationship" means a non-business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from (*a*) a donation or gift made by the person to whom the message is sent to any of those other persons within the 18-month period immediately preceding the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization, or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; (*b*) volunteer work performed by the person to whom the message is sent for any of those other persons, or attendance at a meeting organized by that other person, within the 18-month period immediately preceding the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; or (*c*) membership, as defined in the regulations, by the person to whom the message is sent, in any of those other persons, within the 18-month period immediately preceding the day on which the message was sent, where that other person is	access to or use of that data by the owner or an authorized user of the computer system; (*e*) causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system; (*f*) installing a computer program that may be activated by a third party without the knowledge of the owner or an authorized user of the computer system; and (*g*) performing any other function specified in the regulations. (6) Subsection (4) does not apply in respect of a computer program that performs a function described in subsection (5) if that function only collects, uses or communicates transmission data or performs an operation specified in the regulations. (7) Subsections (1) and (3) do not apply in respect of the installation of an update or upgrade to a computer program the installation or use of which was expressly consented to in accordance with subsections (1) and (3) if the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and the update or upgrade is installed in accordance with those terms. (8) A person is considered to expressly consent to the installation of a computer program if (*a*) the program is

	a club, association or voluntary organization, as defined in the regulations.	(i) a cookie, (ii) HTML code, (iii) Java Scripts, (iv) an operating system, (v) any other program that is executable only through the use of another computer program whose installation or use the person has previously expressly consented to, or (vi) any other program specified in the regulations; and (*b*) the person's conduct is such that it is reasonable to believe that they consent to the program's installation. (9) Consent is implied for the purpose of section 7 only if (*a*) the person who sends the message, the person who causes it to be sent or the person who permits it to be sent has an existing business relationship or an existing non-business relationship with the person to whom it is sent; (*b*) the person to whom the message is sent has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the

		electronic address and the message is relevant to the person's business, role, functions or duties in a business or official capacity; (*c*) the person to whom the message is sent has disclosed, to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity; or (*d*) the message is sent in the circumstances set out in the regulations. (10) In subsection (9), "existing business relationship" means a business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from (*a*) the purchase or lease of a product, goods, a service, land or an interest or right in land, within the two-year period immediately before the day on which the message was sent, by the person to whom the message is sent from any of those other persons; (*b*) the acceptance by the person to whom the message is sent, within the period referred to in paragraph (*a*), of a business, investment or gaming opportunity offered by any of those other persons; (*c*) the bartering of anything mentioned in paragraph (*a*) between the person to whom the

		message is sent and any of those other persons within the period referred to in that paragraph; (*d*) a written contract entered into between the person to whom the message is sent and any of those other persons in respect of a matter not referred to in any of paragraphs (*a*) to (*c*), if the contract is currently in existence or expired within the period referred to in paragraph (*a*); or (*e*) an inquiry or application, within the six-month period immediately before the day on which the message was sent, made by the person to whom the message is sent to any of those other persons, in respect of anything mentioned in any of paragraphs (*a*) to (*c*). (11) For the purposes of subsection (10), the following organizations are considered to be businesses: (*a*) a cooperative as defined in subsection 2(1) of the *Canada Cooperatives Act*; (*b*) a cooperative corporation as defined in section 2 of the *Cooperative Credit Associations Act*; and (*c*) any similar organization incorporated under an Act of Parliament or the legislature of a province. (12) If a person has an existing business relationship with another person in accordance with subsection (10), and the business is sold, the person who purchases the business is considered to have, in respect of that business, an existing business relationship with that other person.

		(13) In subsection (9), “existing non-business relationship” means a non-business relationship between the person to whom the message is sent and any of the other persons referred to in that subsection — that is, any person who sent or caused or permitted to be sent the message — arising from (*a*) a donation or gift made by the person to whom the message is sent to any of those other persons within the two-year period immediately before the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization, or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; (*b*) volunteer work performed by the person to whom the message is sent for any of those other persons, or attendance at a meeting organized by that other person, within the two-year period immediately before the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; or (*c*) membership, as defined in the regulations, by the person to whom the message is sent, in any of those other persons, within the two-year period immediately before the day on which the message was sent, where that other person is a club, association or voluntary organization, as defined in the regulations. (14) Where a period is specified in subsection (10) or (13) in relation to the purchase or lease of a product, goods, a service, land or an interest or right in land, or in relation

		to a donation, gift or membership, (*a*) in the case of a purchase, lease, donation or gift, if it involves an ongoing use or ongoing purchase under a subscription, account, loan or similar relationship, the period is considered to begin on the day that the subscription, account, loan or other relationship terminates; and (*b*) in the case of a membership, the period is considered to begin on the day that the membership terminates.
Unsubscribe mechanism	**11.** (1) The unsubscribe mechanism referred to in paragraph 6(2)(*c*) must (*a*) enable the person to whom the commercial electronic message is sent to indicate, using the same electronic means by which the message was sent, that they do not wish to receive any commercial electronic messages, or any specified class of such messages, from the sender or the person — if different — on whose behalf the message is sent; and (*b*) specify an electronic address to which the indication may be sent or provide a hyperlink by means of which the indication can be given. (2) The person who sends the commercial electronic message and the person — if different — on whose behalf it is sent shall ensure that the electronic address or hyperlink referred to in paragraph (1)(*b*) is	**12.** (1) The unsubscribe mechanism referred to in paragraph 7(2)(*c*) must (*a*) enable the person to whom the commercial electronic message is sent to indicate, at no cost to them, the wish to no longer receive any commercial electronic messages, or any specified class of such messages, from the person who sent the message or the person — if different — on whose behalf the message is sent, using (i) the same electronic means by which the message was sent, or (ii) if using those means is not practicable, any other electronic means that will enable the person to indicate the wish; and (*b*) specify an electronic address, or link to a page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent. (2) The person who sends the commercial electronic message and the person — if different — on whose behalf it is sent must

	valid for a minimum of 60 days after the message has been sent. (3) The person who sent the commercial electronic message and the person — if different — on whose behalf the message was sent shall ensure that effect is given to an indication sent or given in accordance with paragraph (1)(*b*) without delay, and in any event no later than 10 days after the indication has been sent or given, without any further action being required on the part of the person who so indicated. (4) A person who has the express consent of the sender to do any act described in section 7 shall (*a*) for the period covered by the consent, ensure that the sender is provided with an electronic address to which they may send, or a hyperlink by means of which they can give, notice of the withdrawal of their consent; and (*b*) ensure that effect is given to a notice of withdrawal of consent sent or given in accordance with paragraph (*a*) without delay, but in any event no later than 10 days after receiving it. (5) A person who has the express consent of an owner or authorized user to do any act described in section 8 shall (*a*) for a period of one year after any computer program is installed under the consent, ensure that the person who gave their consent is provided with an electronic address to which they may, if they believe that the function, purpose or impact of the	ensure that the electronic address or World Wide Web page referred to in paragraph (1)(*b*) is valid for a minimum of 60 days after the message has been sent. (3) The person who sent the commercial electronic message and the person — if different — on whose behalf the message was sent must ensure that effect is given to an indication sent in accordance with paragraph (1)(*b*) without delay, and in any event no later than 10 business days after the indication has been sent, without any further action being required on the part of the person who so indicated. (4) A person who has the express consent of the sender or the person to whom a message is sent to do any act described in section 8 must (*a*) for the period covered by the consent, ensure that the person who gave their consent is provided with an electronic address to which they may send notice of the withdrawal of their consent; and (*b*) ensure that effect is given to a notice of withdrawal of consent sent in accordance with paragraph (*a*) without delay, but in any event no later than 10 business days after receiving it. (5) A person who has the express consent of an owner or authorized user to do any act described in section 9 must (*a*) for a period of one year after any computer program that performs one or more of the functions described in subsection 11(5) but not referred to in subsection 11(6) is installed under the consent, ensure that the person who gave their consent is provided with an electronic address to which they may, if they believe that the function, purpose or impact of the computer program installed under the consent was not accurately described when

	computer program installed under the consent was not accurately described when consent was requested, send a request to remove or disable that computer program; and (*b*) if the consent was based on an inaccurate description of the function, purpose or impact of the computer program, on receipt within that one-year period of a request to remove or disable that computer program, without cost to the person who gave consent, assist that person in removing or disabling the computer program as soon as feasible.	consent was requested, send a request to remove or disable that computer program; and (*b*) if the consent was based on an inaccurate description of the material elements of the function or functions described in subsection 11(5), on receipt within that one-year period of a request to remove or disable that computer program, without cost to the person who gave consent, assist that person in removing or disabling the computer program as soon as feasible.
Amendments	AMENDMENT TO THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION ACT **65.** Subsection 12(2) of the *Canadian Radio-television and Telecommunications Commission Act* is replaced by the following: (2) The full-time members of the Commission and the Chairperson shall exercise the powers and perform the duties vested in the Commission and the Chairperson, respectively, by the *Telecommunications Act* or any special Act, as defined in subsection 2(1) of that Act, or by the *Electronic Commerce Protection Act*. AMENDMENTS TO THE COMPETITION ACT **66.** (1) The definition "record" in subsection 2(1) of the *Competition Act* is replaced by the following: "record" means any information that is recorded on any medium and that is capable of being understood by a person or read by a computer system or other device;	AMENDMENT TO THE CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION ACT **70.** Subsection 12(2) of the *Canadian Radio-television and Telecommunications Commission Act* is replaced by the following: (2) The full-time members of the Commission and the Chairperson shall exercise the powers and perform the duties vested in the Commission and the Chairperson, respectively, by the *Telecommunications Act* or any special Act, as defined in subsection 2(1) of that Act, or by the *Fighting Internet and Wireless Spam Act*. AMENDMENTS TO THE COMPETITION ACT **71.** (1) The definition "record" in subsection 2(1) of the *Competition Act* is replaced by the

	(2) Subsection 2(1) of the Act is amended by adding the following in alphabetical order: "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*; "data", other than in Part III, means signs, signals, symbols or concepts that are being prepared or have been prepared in a form suitable for use in a computer system; "electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message; "information" includes data; "locator" means a name or information used to identify a source of data on a computer system, and includes a URL; "sender information" means the part of an electronic message — including the data relating to source, routing, addressing or signalling — that identifies or purports to identify the sender or the origin of the message; "subject matter information" means the part of an electronic message that purports to summarize the contents of the message or to give an indication of them; **67.** Subsection 16(6) of the Act is repealed. **68.** Subsection 20(2) of the Act is replaced by the following: (2) Copies of any records referred to in subsection (1), made by any process of reproduction, on proof orally or by affidavit that they are true copies, are admissible in evidence in any proceedings under this Act and have the same probative force as the original. **69.** Subsections 33(1) to (7) of the Act are	following: "record" means any information that is recorded on any medium and that is capable of being understood by a person or read by a computer system or other device; (2) Subsection 2(1) of the Act is amended by adding the following in alphabetical order: "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*; "data", other than in Part III, means signs, signals, symbols or concepts that are being prepared or have been prepared in a form suitable for use in a computer system; "electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message; "information" includes data; "locator" means a name or information used to identify a source of data on a computer system, and includes a URL; "sender information" means the part of an electronic message — including the data relating to source, routing, addressing or signalling — that identifies or purports to identify the sender or the origin of the message; "subject matter information" means the part of an electronic message that purports to summarize the contents of the message or to give an indication of them; **72.** Subsection 16(6) of the Act is repealed. **73.** Subsection 20(2) of the Act is replaced by the following: (2) Copies of any records referred to in subsection (1), made by any process of

	replaced by the following: **33.** (1) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, a court may issue an interim injunction forbidding any person named in the application from doing any act or thing that it appears to the court could constitute or be directed toward the commission of an offence under Part VI — other than an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53 — or under section 66, pending the commencement or completion of a proceeding under subsection 34(2) or a prosecution against the person, if it appears to the court that (*a*) the person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; and (*b*) if the offence is committed or continued, (i) injury to competition that cannot adequately be remedied under any other provision of this Act will result, or (ii) serious harm is likely to ensue unless the injunction is issued and the balance of convenience favours issuing the injunction. (1.1) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, a court may issue an injunction forbidding any person named in the application from doing any act or thing that it appears to the court could constitute or be directed toward the commission of an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53, if it appears to the	reproduction, on proof orally or by affidavit that they are true copies, are admissible in evidence in any proceedings under this Act and have the same probative force as the original. **74.** Subsections 33(1) to (7) of the Act are replaced by the following: **33.** (1) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, a court may issue an interim injunction forbidding any person named in the application from doing any act or thing that it appears to the court could constitute or be directed toward the commission of an offence under Part VI — other than an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53 — or under section 66, pending the commencement or completion of a proceeding under subsection 34(2) or a prosecution against the person, if it appears to the court that (*a*) the person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; and (*b*) if the offence is committed or continued, (i) injury to competition that cannot adequately be remedied under any other provision of this Act will result, or (ii) serious harm is likely to ensue unless the injunction is issued and the balance of convenience favours issuing the injunction. (1.1) On application by or on behalf of the Attorney General of Canada or the attorney

	court that (*a*) the person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; (*b*) if the offence is committed or continued, serious harm is likely to ensue unless the injunction is issued; and (*c*) the balance of convenience favours issuing the injunction. (1.2) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, a court may issue an injunction ordering any person named in the application to refrain from supplying to another person a product that it appears to the court is or is likely to be used to commit or continue an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53, or to do any act or thing that it appears to the court could prevent the commission or continuation of such an offence, if it appears to the court that (*a*) a person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; (*b*) if the offence is committed or continued, serious harm is likely to ensue unless the injunction is issued; and (*c*) the balance of convenience favours issuing the injunction. (2) Subject to subsection (3), at least 48 hours' notice of an application for an injunction	general of a province, a court may issue an injunction forbidding any person named in the application from doing any act or thing that it appears to the court could constitute or be directed toward the commission of an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53, if it appears to the court that (*a*) the person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; (*b*) if the offence is committed or continued, serious harm is likely to ensue unless the injunction is issued; and (*c*) the balance of convenience favours issuing the injunction. (1.2) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, a court may issue an injunction ordering any person named in the application to refrain from supplying to another person a product that it appears to the court is or is likely to be used to commit or continue an offence under section 52 involving the use of any means of telecommunication or an offence under section 52.01, 52.1 or 53, or to do any act or thing that it appears to the court could prevent the commission or continuation of such an offence, if it appears to the court that (*a*) a person has done, is about to do or is likely to do any act or thing constituting or directed toward the commission of the offence; (*b*) if the offence is committed or continued, serious harm is likely to ensue unless the

	under subsection (1), (1.1) or (1.2) shall be given by or on behalf of the Attorney General of Canada or the attorney general of a province, as the case may be, to each person against whom the injunction is sought.	injunction is issued; and (*c*) the balance of convenience favours issuing the injunction.
	(3) If a court to which an application is made under subsection (1), (1.1) or (1.2) is satisfied that subsection (2) cannot reasonably be complied with, or that the urgency of the situation is such that service of notice in accordance with subsection (2) would not be in the public interest, it may proceed with the application *ex parte* but any injunction issued under subsection (1), (1.1) or (1.2) by the court on *ex parte* application has effect only for the period, not exceeding 10 days, that is specified in the order.	(2) Subject to subsection (3), at least 48 hours' notice of an application for an injunction under subsection (1), (1.1) or (1.2) shall be given by or on behalf of the Attorney General of Canada or the attorney general of a province, as the case may be, to each person against whom the injunction is sought. (3) If a court to which an application is made under subsection (1), (1.1) or (1.2) is satisfied that subsection (2) cannot reasonably be complied with, or that the urgency of the situation is such that service of notice in accordance with subsection (2) would not be in the public interest, it may proceed with the application *ex parte* but any injunction issued under subsection (1), (1.1) or (1.2) by the court on *ex parte* application has effect only for the period, not exceeding 10 days, that is specified in the order.
	(4) An injunction issued under subsection (1), (1.1) or (1.2) (*a*) shall be in the terms that the court that issues it considers necessary and sufficient to meet the circumstances of the case; and (*b*) subject to subsection (3), has effect for the period that is specified in the order.	(4) An injunction issued under subsection (1), (1.1) or (1.2) (*a*) shall be in the terms that the court that issues it considers necessary and sufficient to meet the circumstances of the case; and (*b*) subject to subsection (3), has effect for the period that is specified in the order.
	(5) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, as the case may be, or by or on behalf of any person to whom the injunction is directed, on at least 48 hours' notice of the application to all other parties to the injunction, a court that issues an injunction under subsection (1), (1.1) or (1.2) may, by order, (*a*) despite subsections (3) and (4), continue the injunction, with or without modification, for any definite period that is specified in the order; or	(5) On application by or on behalf of the Attorney General of Canada or the attorney general of a province, as the case may be, or by or on behalf of any person to whom the injunction is directed, on at least 48 hours' notice of the application to all other parties to the injunction, a court that issues an injunction under subsection (1), (1.1) or (1.2) may, by

		order,
	(*b*) revoke the injunction.	
	(6) If an injunction is issued under subsection (1), (1.1) or (1.2), the Attorney General of Canada or the attorney general of a province, as the case may be, shall proceed as expeditiously as possible to institute and conclude any prosecution or proceedings arising out of the acts or things on the basis of which the injunction was issued.	(*a*) despite subsections (3) and (4), continue the injunction, with or without modification, for any definite period that is specified in the order; or
		(*b*) revoke the injunction.
	(7) A court may punish any person who contravenes an injunction issued by it under subsection (1), (1.1) or (1.2) by a fine in the discretion of the court or by imprisonment for a term not exceeding two years.	(6) If an injunction is issued under subsection (1), (1.1) or (1.2), the Attorney General of Canada or the attorney general of a province, as the case may be, shall proceed as expeditiously as possible to institute and conclude any prosecution or proceedings arising out of the acts or things on the basis of which the injunction was issued.
	70. (1) Subsection 52(1.2) of the Act is replaced by the following:	(7) A court may punish any person who contravenes an injunction issued by it under subsection (1), (1.1) or (1.2) by a fine in the discretion of the court or by imprisonment for a term not exceeding two years.
	(1.2) For greater certainty, in this section and in sections 52.01, 52.1, 74.01, 74.011 and 74.02, the making or sending of a representation includes permitting a representation to be made or sent.	**75.** (1) Subsection 52(1.2) of the Act is replaced by the following:
		(1.2) For greater certainty, in this section and in sections 52.01, 52.1, 74.01, 74.011 and 74.02, the making or sending of a representation includes permitting a representation to be made or sent.
	(2) Paragraph 52(2)(*d*) of the Act is replaced by the following:	(2) Paragraph 52(2)(*d*) of the Act is replaced by the following:
	(*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or	(*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or
	71. The Act is amended by adding the following after section 52:	
	52.01 (1) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product,	

	knowingly or recklessly send or cause to be sent a false or misleading representation in the sender information or subject matter information of an electronic message. (2) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly send or cause to be sent in an electronic message a representation that is false or misleading in a material respect. (3) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly make or cause to be made a false or misleading representation in a locator. (4) For greater certainty, in establishing that any of subsections (1) to (3) was contravened, it is not necessary to prove that any person was deceived or misled. (5) In a prosecution for a contravention of any of subsections (1) to (3), the general impression conveyed by a representation as well as its literal meaning are to be taken into account. (6) Any person who contravenes any of subsections (1) to (3) is guilty of an offence and (*a*) liable on conviction on indictment to a fine in the discretion of the court or to imprisonment for a term not exceeding 14 years, or to both; or (*b*) liable on summary conviction to a fine not exceeding $200,000 or to imprisonment for a term not exceeding one year, or to both. (7) Nothing in Part VII.1 is to be read as excluding the application of this section to the making of a representation that constitutes reviewable conduct within the meaning of that	**76.** The Act is amended by adding the following after section 52: **52.01** (1) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly send or cause to be sent a false or misleading representation in the sender information or subject matter information of an electronic message. (2) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly send or cause to be sent in an electronic message a representation that is false or misleading in a material respect. (3) No person shall, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, knowingly or recklessly make or cause to be made a false or misleading representation in a locator. (4) For greater certainty, in establishing that any of subsections (1) to (3) was contravened, it is not necessary to prove that any person was deceived or misled. (5) In a prosecution for a contravention of any of subsections (1) to (3), the general impression conveyed by a representation as well as its literal meaning are to be taken into account. (6) Any person who contravenes any of subsections (1) to (3) is guilty of an offence and (*a*) liable on conviction on indictment to a fine in the discretion of the court or to imprisonment for a term not exceeding 14 years, or to both; or (*b*) liable on summary conviction to a fine not exceeding $200,000 or to imprisonment for a

	Part.	term not exceeding one year, or to both.
	(8) No proceedings may be commenced under this section against a person on the basis of facts that are the same or substantially the same as the facts on the basis of which an order against that person is sought under Part VII.1.	(7) Nothing in Part VII.1 is to be read as excluding the application of this section to the making of a representation that constitutes reviewable conduct within the meaning of that Part.
	(9) For the purposes of this section,	(8) No proceedings may be commenced under this section against a person on the basis of facts that are the same or substantially the same as the facts on the basis of which an order against that person is sought under Part VII.1.
	(*a*) an electronic message is considered to have been sent once its transmission has been initiated; and	(9) For the purposes of this section,
	(*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination.	(*a*) an electronic message is considered to have been sent once its transmission has been initiated; and
	52.02 (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct prohibited under section 52, 52.01, 52.1, 53, 55 or 55.1,	(*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination.
	(*a*) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act or the *Criminal Code* to investigate an offence under any of those sections; and	**52.02** (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct prohibited under section 52, 52.01, 52.1, 53, 55 or 55.1,
	(*b*) disclose the information to the government of the foreign state or to the international organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of	(*a*) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act or the *Criminal Code* to investigate an offence under any of those sections; and

	which the assistance is being provided, if the government, organization or institution declares in writing that (i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent. (2) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1). **72.** (1) Subsection 52.1(1) of the Act is replaced by the following: **52.1** (1) In this section, "telemarketing" means the practice of communicating orally by any means of telecommunication for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product. (2) Paragraph 52.1(2)(*a*) of the Act is replaced by the following: (*a*) disclosure is made, in a fair and reasonable manner at the beginning of each communication, of the identity of the person on behalf of whom the communication is made, the nature of the business interest or product being promoted and the purposes of the	(*b*) disclose the information to the government of the foreign state or to the international organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of which the assistance is being provided, if the government, organization or institution declares in writing that (i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent. (2) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1). **77.** (1) Subsection 52.1(1) of the Act is replaced by the following: **52.1** (1) In this section, "telemarketing" means the practice of communicating orally by any means of telecommunication for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product. (2) Paragraph 52.1(2)(*a*) of the Act is replaced

	communication; (3) Subsection 52.1(5) of the Act is replaced by the following: (5) The disclosure of information referred to in paragraph (2)(*b*) or (*c*) or (3)(*b*) or (*c*) must be made during the course of a communication unless it is established by the accused that the information was disclosed within a reasonable time before the communication, by any means, and the information was not requested during the communication. **73.** The Act is amended by adding the following after section 74.01: **74.011** (1) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, sends or causes to be sent a false or misleading representation in the sender information or subject matter information of an electronic message. (2) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, sends or causes to be sent in an electronic message a representation that is false or misleading in a material respect. (3) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, makes or causes to be made a false or misleading representation in a locator. (4) In proceedings under this section, the general impression conveyed by a representation as well as its literal meaning shall be taken into account in determining whether or not the person who made the representation engaged in the reviewable	by the following: (*a*) disclosure is made, in a fair and reasonable manner at the beginning of each communication, of the identity of the person on behalf of whom the communication is made, the nature of the business interest or product being promoted and the purposes of the communication; (3) Subsection 52.1(5) of the Act is replaced by the following: (5) The disclosure of information referred to in paragraph (2)(*b*) or (*c*) or (3)(*b*) or (*c*) must be made during the course of a communication unless it is established by the accused that the information was disclosed within a reasonable time before the communication, by any means, and the information was not requested during the communication. **78.** The Act is amended by adding the following after section 74.01: **<u>74.011</u>** <u>(1) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, sends or causes to be sent a false or misleading representation in the sender information or subject matter information of an electronic message.</u> <u>(2) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, sends or causes to be sent in an electronic message a representation that is false or misleading in a material respect.</u> <u>(3) A person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, makes or causes to be</u>

	conduct. (5) For the purposes of this section, (*a*) an electronic message is considered to have been sent once its transmission has been initiated; and (*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination. **74.012** (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct that is reviewable under section 74.01, 74.011, 74.02, 74.04, 74.05 or 74.06, (*a*) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act to investigate conduct that is reviewable under any of those sections; and (*b*) disclose the information to the government of the foreign state or to the international organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of which the assistance is being provided, if the government, organization or institution declares in writing that	made a false or misleading representation in a locator. (4) In proceedings under this section, the general impression conveyed by a representation as well as its literal meaning shall be taken into account in determining whether or not the person who made the representation engaged in the reviewable conduct. (5) For the purposes of this section, (*a*) an electronic message is considered to have been sent once its transmission has been initiated; and (*b*) it is immaterial whether the electronic address to which an electronic message is sent exists or whether an electronic message reaches its intended destination. **74.012** (1) The Commissioner may, for the purpose of assisting an investigation or proceeding in respect of the laws of a foreign state, an international organization of states or an international organization established by the governments of states that address conduct that is substantially similar to conduct that is reviewable under section 74.01, 74.011, 74.02, 74.04, 74.05 or 74.06, (*a*) conduct any investigation that the Commissioner considers necessary to collect relevant information, using any powers that the Commissioner may use under this Act to investigate conduct that is reviewable under any of those sections; and (*b*) disclose the information to the government of the foreign state or to the international

	(i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent. (2) Subsection (1) does not apply if the contravention of the laws of the foreign state has consequences that would be considered penal under Canadian law. (3) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1). **74.** Paragraph 74.03(1)(*d*) of the Act is replaced by the following: (*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or **75.** The Act is amended by adding the following after section 74.1: **74.101** (1) If a court determines that a person is engaging in or has engaged in conduct that is reviewable under section 74.011 and orders the person to pay an administrative monetary penalty under paragraph 74.1(1)(*c*), then the court shall deduct from the amount of the penalty that it determines any amount that the person	organization, or to any institution of any such government or organization responsible for conducting investigations or initiating proceedings in respect of the laws in respect of which the assistance is being provided, if the government, organization or institution declares in writing that (i) the use of the information will be restricted to purposes relevant to the investigation or proceeding, and (ii) the information will be treated in a confidential manner and, except for the purposes mentioned in subparagraph (i), will not be further disclosed without the Commissioner's express consent. (2) Subsection (1) does not apply if the contravention of the laws of the foreign state has consequences that would be considered penal under Canadian law. (3) In deciding whether to provide assistance under subsection (1), the Commissioner shall consider whether the government, organization or institution agrees to provide assistance for investigations or proceedings in respect of any of the sections mentioned in subsection (1). **79.** Paragraph 74.03(1)(*d*) of the Act is replaced by the following: (*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or **80.** The Act is amended by adding the following

		after section 74.1:
	(*a*) has been ordered to pay under paragraph 51(1)(*b*) of the *Electronic Commerce Protection Act* in respect of the same conduct; or	**74.101** (1) If a court determines that a person is engaging in or has engaged in conduct that is reviewable under section 74.011 and orders the person to pay an administrative monetary penalty under paragraph 74.1(1)(*c*), then the court shall deduct from the amount of the penalty that it determines any amount that the person
	(*b*) has agreed in a settlement agreement to pay on account of amounts referred to in paragraph 51(1)(*b*) of that Act in respect of the same conduct.	(*a*) has been ordered to pay under paragraph 52(1)(*b*) of the *Fighting Internet and Wireless Spam Act* in respect of the same conduct; or
	(2) If a court determines that a person is engaging in or has engaged in conduct that is reviewable under subsection 74.011(2), it may order the person to pay an amount under paragraph 74.1(1)(*d*), and may issue an interim injunction under section 74.111, as if the conduct were conduct that is reviewable under paragraph 74.01(1)(*a*).	(*b*) has agreed in a settlement agreement to pay on account of amounts referred to in paragraph 52(1)(*b*) of that Act in respect of the same conduct.
	76. Subsections 74.11(1) to (4) of the Act are replaced by the following:	(2) If a court determines that a person is engaging in or has engaged in conduct that is reviewable under subsection 74.011(2), it may order the person to pay an amount under paragraph 74.1(1)(*d*), and may issue an interim injunction under section 74.111, as if the conduct were conduct that is reviewable under paragraph 74.01(1)(*a*).
	74.11 (1) On application by the Commissioner, a court may order a person who it appears to the court is engaging in conduct that is reviewable under this Part not to engage in that conduct or substantially similar reviewable conduct if it appears to the court that	**81.** Subsections 74.11(1) to (4) of the Act are replaced by the following:
	(*a*) serious harm is likely to ensue unless the order is issued; and	**74.11** (1) On application by the Commissioner, a court may order a person who it appears to the court is engaging in conduct that is reviewable under this Part not to engage in that conduct or substantially similar reviewable conduct if it appears to the court that
	(*b*) the balance of convenience favours issuing the order.	(*a*) serious harm is likely to ensue unless the order is issued; and
	(1.1) On application by the Commissioner, a court may order any person named in the application to refrain from supplying to another person a product that it appears to the court is or is likely to be used to engage in conduct that is reviewable under this Part, or to do any act or thing that it appears to the court could prevent a	

	person from engaging in such conduct, if it appears to the court that (*a*) serious harm is likely to ensue unless the order is issued; and (*b*) the balance of convenience favours issuing the order. (2) Subject to subsection (5), an order made under subsection (1) or (1.1) has effect, or may be extended on application by the Commissioner, for any period that the court considers sufficient to meet the circumstances of the case. (3) Subject to subsection (4), at least 48 hours' notice of an application referred to in subsection (1), (1.1) or (2) shall be given by or on behalf of the Commissioner to the person in respect of whom the order or extension is sought. (4) The court may proceed *ex parte* with an application made under subsection (1) or (1.1) if it is satisfied that subsection (3) cannot reasonably be complied with or that the urgency of the situation is such that service of notice in accordance with subsection (3) would not be in the public interest. **77.** Section 74.16 of the Act is replaced by the following: **74.16** No application may be made under this Part against a person on the basis of facts that are the same or substantially the same as the facts on the basis of which proceedings have been commenced against that person under section 52 or 52.01. AMENDMENTS TO THE PERSONAL	(*b*) the balance of convenience favours issuing the order. (1.1) On application by the Commissioner, a court may order any person named in the application to refrain from supplying to another person a product that it appears to the court is or is likely to be used to engage in conduct that is reviewable under this Part, or to do any act or thing that it appears to the court could prevent a person from engaging in such conduct, if it appears to the court that (*a*) serious harm is likely to ensue unless the order is issued; and (*b*) the balance of convenience favours issuing the order. (2) Subject to subsection (5), an order made under subsection (1) or (1.1) has effect, or may be extended on application by the Commissioner, for any period that the court considers sufficient to meet the circumstances of the case. (3) Subject to subsection (4), at least 48 hours' notice of an application referred to in subsection (1), (1.1) or (2) shall be given by or on behalf of the Commissioner to the person in respect of whom the order or extension is sought. (4) The court may proceed *ex parte* with an application made under subsection (1) or (1.1) if it is satisfied that subsection (3) cannot reasonably be complied with or that the urgency of the situation is such that service of notice in accordance with subsection (3) would not be in the public interest. **82.** Section 74.16 of the Act is replaced by the following:

	INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT **78.** The *Personal Information Protection and Electronic Documents Act* is amended by adding the following after section 7: **7.1** (1) The following definitions apply in this section. "access" means to program, to execute programs on, to communicate with, to store data in, to retrieve data from, or to otherwise make use of any resources, including data or programs on a computer system or a computer network. "computer program" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "electronic address" means an address used in connection with (*a*) an electronic mail account; (*b*) an instant messaging account; or (*c*) any similar account. (2) Paragraphs 7(1)(*a*), (*c*) and (*d*) and (2)(*a*) to (*c.1*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of (*a*) the collection of an individual's electron- ic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or (*b*) the use of an individual's electronic address, if the address is collected by the use of a	**74.16** No application may be made under this Part against a person on the basis of facts that are the same or substantially the same as the facts on the basis of which proceedings have been commenced against that person under section 52 or 52.01. AMENDMENTS TO THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT **83.** The *Personal Information Protection and Electronic Documents Act* is amended by adding the following after section 7: **7.1** (1) The following definitions apply in this section. "access" means to program, to execute programs on, to communicate with, to store data in, to retrieve data from, or to otherwise make use of any resources, including data or programs on a computer system or a computer network. "computer program" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*. "electronic address" means an address used in connection with (*a*) an electronic mail account; (*b*) an instant messaging account; or

	computer program described in paragraph (*a*).	(*c*) any similar account.
	(3) Paragraphs 7(1)(*a*) to (*d*) and (2)(*a*) to (*c.1*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of	(2) Paragraphs 7(1)(*a*), (*c*) and (*d*) and (2)(*a*) to (*c.1*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of
	(*a*) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed without authorization; or	(*a*) the collection of an individual's electron- ic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses; or
	(*b*) the use of personal information that is collected in a manner described in paragraph (*a*).	(*b*) the use of an individual's electronic address, if the address is collected by the use of a computer program described in paragraph (*a*).
	79. Section 12 of the Act is replaced by the following:	(3) Paragraphs 7(1)(*a*) to (*d*) and (2)(*a*) to (*c.1*) and the exception set out in clause 4.3 of Schedule 1 do not apply in respect of
	12. (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that	
	(*a*) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;	(*a*) the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament; or
	(*b*) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or	(*b*) the use of personal information that is collected in a manner described in paragraph (*a*).
	(*c*) the complaint was not filed within a reasonable period from the date when the subject matter of the complaint arose.	**84.** Section 12 of the Act is replaced by the following:
	(2) Despite subsection (1), the Commissioner is not required to conduct an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if	**12.** (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that
		(*a*) the complainant ought first to exhaust

	proved, would constitute a contravention of any of sections 6 to 9 of the *Electronic Commerce Protection Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act. (3) The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons. (4) The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate. **12.1** (1) In the conduct of an investigation of a complaint, the Commissioner may (*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record; (*b*) administer oaths; (*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; (*d*) at any reasonable time, enter any prem- ises, other than a dwelling-house, occupied by an organization on satisfying any security	grievance or review procedures otherwise reasonably available; (*b*) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or (*c*) the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose. (2) Despite subsection (1), the Commissioner is not required to conduct an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 7 to 10 of the *Fighting Internet and Wireless Spam Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act. (3) The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons. (4) The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate. **12.1** (1) In the conduct of an investigation of a complaint, the Commissioner may (*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath

	requirements of the organization relating to the premises; (*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and (*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation. (2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation. (3) The Commissioner may delegate any of the powers set out in subsection (1) or (2). (4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced. (5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*). Discontinuance of Investigation **12.2** (1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that	and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record; (*b*) administer oaths; (*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law; (*d*) at any reasonable time, enter any prem- ises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises; (*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and (*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation. (2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation. (3) The Commissioner may delegate any of the powers set out in subsection (1) or (2). (4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this

	(*a*) there is insufficient evidence to pursue the investigation; (*b*) the complaint is trivial, frivolous or vexatious or is made in bad faith; (*c*) the organization has provided a fair and reasonable response to the complaint; (*d*) the matter is already the object of an ongoing investigation under this Part; (*e*) the matter has already been the subject of a report by the Commissioner; (*f*) any of the circumstances mentioned in paragraph 12(1)(*a*), (*b*) or (*c*) apply; or (*g*) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(*a*) or (*b*). (2) The Commissioner may discontinue an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of the *Electronic Commerce Protection Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act. (3) The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons.	section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced. (5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*). Discontinuance of Investigation **12.2** (1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that (*a*) there is insufficient evidence to pursue the investigation; (*b*) the complaint is trivial, frivolous or vexatious or is made in bad faith; (*c*) the organization has provided a fair and reasonable response to the complaint; (*d*) the matter is already the object of an ongoing investigation under this Part; (*e*) the matter has already been the subject of a report by the Commissioner; (*f*) any of the circumstances mentioned in paragraph 12(1)(*a*), (*b*) or (*c*) apply; or (*g*) the matter is being or has already been

	80. Subsection 13(2) of the Act is repealed.	addressed under a procedure referred to in paragraph 12(1)(*a*) or (*b*).
	81. Subsections 14(1) and (2) of the Act are replaced by the following:	(2) The Commissioner may discontinue an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 7 to 10 of the *Fighting Internet and Wireless Spam Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act.
	14. (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1, in subsection 5(3) or 8(6) or (7) or in section 10.	(3) The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons.
	(2) A complainant must make an application within 45 days after the report or notification is sent or within any further time that the Court may, either before or after the expiry of those 45 days, allow.	**85.** Subsection 13(2) of the Act is repealed.
		86. Subsections 14(1) and (2) of the Act are replaced by the following:
	82. (1) Subsection 20(1) of the Act is replaced by the following:	**14.** (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1, in subsection 5(3) or 8(6) or (7) or in section 10.
	20. (1) Subject to subsections (2) to (6), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part.	(2) A complainant must make an application within 45 days after the report or notification is sent or within any further time that the Court may, either before or after the expiry of those 45 days, allow.
	(2) Section 20 of the Act is amended by adding the following after subsection (5):	
	(6) The Commissioner may disclose	**87.** (1) Subsection 20(1) of the Act is replaced

	information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 50(*c*) of the *Electronic Commerce Protection Act* or in accord- ance with subsection 58(3) or 60(1) of that Act.	by the following: **20.** (1) Subject to subsections (2) to (6), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part.
	83. Section 23 of the Act is replaced by the following: **23.** (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation, has functions and duties similar to those of the Commissioner with respect to the protection of such information. (2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to (*a*) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested; (*b*) undertake and publish research or develop and publish guidelines or other instruments related to the protection of personal information; (*c*) develop model contracts or other instruments for the protection of personal information that is collected, used or disclosed interprovincially or internationally; and	(2) Section 20 of the Act is amended by adding the following after subsection (5): (6) The Commissioner may disclose information, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose information, in the course of proceedings in which the Commissioner has intervened under paragraph 51(*c*) of the *Fighting Internet and Wireless Spam Act* or in accord- ance with subsection 59(3) or 61(1) of that Act. **88.** Section 23 of the Act is replaced by the following: **23.** (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation, has functions and duties similar to those of the Commissioner with respect to the protection of such information. (2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to (*a*) coordinate the activities of their offices and

	(*d*) develop procedures for sharing information referred to in subsection (3).	the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;
	(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(*d*), share information with any person referred to in subsection (1), if the information	(*b*) undertake and publish research <u>or develop and publish guidelines or other instruments</u> related to the protection of personal information;
	(*a*) could be relevant to an ongoing or potential investigation of a complaint or audit under this Part or provincial legislation that has objectives that are similar to this Part; or	(*c*) develop model contracts <u>or other instruments</u> for the protection of personal information that is collected, used or disclosed interprovincially or internationally; and
	(*b*) could assist the Commissioner or that person in the exercise of their functions and duties with respect to the protection of personal information.	<u>(*d*) develop procedures for sharing information referred to in subsection (3).</u>
	(4) The procedures referred to in paragraph (2)(*d*) shall	<u>(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(*d*), share information with any person referred to in subsection (1), if the information</u>
	(*a*) restrict the use of the information to the purpose for which it was originally shared; and	<u>(*a*) could be relevant to an ongoing or potential investigation of a complaint or audit under this Part or provincial legislation that has objectives that are similar to this Part; or</u>
	(*b*) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.	<u>(*b*) could assist the Commissioner or that person in the exercise of their functions and duties with respect to the protection of personal information.</u>
	23.1 (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(*b*), disclose information referred to in subsection (2) that has come to the Commissioner's knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part to any person or body who, under the legislation of a foreign state, has	<u>(4) The procedures referred to in paragraph (2)(*d*) shall</u> <u>(*a*) restrict the use of the information to the purpose for which it was originally shared; and</u>

	(*a*) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or	(*b*) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.
	(*b*) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Part.	**23.1** (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(*b*), disclose information referred to in subsection (2) that has come to the Commissioner's knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part to any person or body who, under the legislation of a foreign state, has
	(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes	
	(*a*) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Part; or	(*a*) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or
	(*b*) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under this Part.	(*b*) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Part.
	(3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that	(2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes
	(*a*) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(*a*) or (*b*);	(*a*) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Part; or
	(*b*) restricts the use of the information to the purpose for which it was originally shared; and	(*b*) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under this Part.
	(*c*) stipulates that the information be treated in a	(3) The Commissioner may only disclose information to the person or body referred to in

	confidential manner and not be further disclosed without the express consent of the Commissioner. (4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to (*a*) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested; (*b*) establish procedures for sharing information referred to in subsection (2); (*c*) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information; (*d*) undertake and publish research related to the protection of personal information; (*e*) share knowledge and expertise by different means, including through staff exchanges; or (*f*) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.	subsection (1) if the Commissioner has entered into a written arrangement with that person or body that (*a*) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(*a*) or (*b*); (*b*) restricts the use of the information to the purpose for which it was originally shared; and (*c*) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner. (4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection (1) in order to (*a*) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested; (*b*) establish procedures for sharing information referred to in subsection (2); (*c*) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information; (*d*) undertake and publish research related to

		the protection of personal information; (*e*) share knowledge and expertise by different means, including through staff exchanges; or (*f*) identify issues of mutual interest and determine priorities pertaining to the protection of personal information. AMENDMENTS TO THE TELECOMMUNICATIONS ACT **89. (1) Subsection 39(2) of the *Telecommunications Act* is replaced by the following:** (2) Subject to subsections (4), (5), (5.1) and (6), where a person designates information as confidential and the designation is not withdrawn by that person, no person described in subsection (3) shall knowingly disclose the information, or knowingly allow it to be disclosed, to any other person in any manner that is calculated or likely to make it available for the use of any person who may benefit from the information or use the information to the detriment of any person to whose business or affairs the information relates.
	AMENDMENTS TO THE TELECOMMUNICATIONS ACT **84. Section 39 of the *Telecommunications Act* is amended by adding the following after subsection (5):** (5.1) The Commission may disclose designated information obtained by it in the perform- ance or exercise of its duties or powers related to any of sections 6 to 9 of the *Electronic Commerce Protection Act* in accordance with subsection 58(1) or 60(1) of that Act. **85.** (1) Section 41 of the Act is renumbered as subsection 41(1) and is amended by adding the	(2) Section 39 of the Act is amended by adding the following after subsection (5): (5.1) The Commission may disclose designated information obtained by it in the performance or exercise of its duties or powers related to section 41, in respect of conduct carried out by electronic means, in accordance with subsection 59(1) or 61(1) of the *Fighting*

	following:	*Internet and Wireless Spam Act.*
	(2) Despite subsection (1), the Commission may not prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications, if the telecommunication is	**90.** (1) Section 41 of the Act is renumbered as subsection 41(1) and is amended by adding the following:
	(*a*) a commercial electronic message to which section 6 of the *Electronic Commerce Protection Act* applies; or	(2) Despite subsection (1), the Commission may not prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications, if the telecommunication is
	(*b*) a commercial electronic message referred to in subsection 6(5) of that Act, except to the extent that it is one referred to in subsection 6(7) of that Act.	(*a*) a commercial electronic message to which section 7 of the *Fighting Internet and Wireless Spam Act* applies; or
	(2) Subsection 41(2) of the Act, as enacted by subsection (1), is replaced by the following:	(*b*) a commercial electronic message referred to in subsection 7(5) of that Act, except to the extent that it is one referred to in subsection 7(8) of that Act.
	(2) Despite subsection (1), the Commission may not prohibit — or, except to the extent provided by subsection (3), regulate — the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications, if the telecommunication is a commercial electronic message to which the *Electronic Commerce Protection Act* applies or a commercial electron- ic message referred to in subsection 6(5) of that Act.	(2) Subsection 41(2) of the Act, as enacted by subsection (1), is replaced by the following:
	(3) For the purposes of subsection (2), the Commission may regulate, with respect to the types of telecommunications described in subsection (4),	(2) Despite subsection (1), the Commission may not prohibit — or, except to the extent provided by subsection (3), regulate — the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications, if the telecommunication is a commercial electronic message to which the *Fighting Internet and Wireless Spam Act* applies or a commercial electron- ic message referred to in subsection 7(5) of that Act.
	(*a*) the hours during which the telecommunications facilities of a Canadian carrier may be used by any person;	(3) For the purposes of subsection (2), the Commission may regulate, with respect to the types of telecommunications described in subsection (4),

	(*b*) the contact information to be provided by a person referred to in subsection (2) and the circumstances in which and persons to whom it must be provided; (*c*) telecommunications made to medical or emergency services; and (*d*) telecommunications where a live operator is not immediately available when the recipient of the telecommunication connects to it. (4) For the purposes of subsection (3), the types of telecommunications are those that are (*a*) in whole or in part, interactive two-way voice communications between individuals; (*b*) sent by means of a facsimile to a telephone account; or (*c*) voice recordings sent to a telephone account. **86.** Sections 41.1 to 41.7 of the Act are repealed.	(*a*) the hours during which the telecommunications facilities of a Canadian carrier may be used by any person; (*b*) the contact information to be provided by a person referred to in subsection (2) and the circumstances in which and persons to whom it must be provided; (*c*) telecommunications made to medical or emergency services; and (*d*) telecommunications where a live operator is not immediately available when the recipient of the telecommunication connects to it. (4) For the purposes of subsection (3), the types of telecommunications are those that are (*a*) in whole or in part, interactive two-way voice communications between individuals; (*b*) sent by means of a facsimile to a telephone account; or (*c*) voice recordings sent to a telephone account. **91.** Sections 41.1 to 41.7 of the Act are repealed.

Appendix 2 – PIAC's Spam Survey

PIAC engaged Environics Research Inc. to undertake a telephone survey of Canadians' attitudes to spam in January 2010. The following is a description from Environics of the survey methodology employed. The crosstabs of PIAC's survey questions are appended.

METHOD OF INTERVIEWING

This report presents the findings of a telephone survey conducted among a national random sample of 1,000 adults comprising 500 males and 500 females 18 years of age and older, living in Canada. The margin of error for a sample of this size is +/- 3.10%, 19 times out of 20.

Interviewing for this Environics National Telephone Omnibus Survey was completed during the periods: January 7 – 13, 2010. Data collection was conducted from our central location dialing facilities in Toronto, Ontario.

QUALITY CONTROL

Environics Research Groups' commitment to excellence on custom studies applies equally to the Environics National Omnibus (EHO). All interviewers were fully briefed by experienced supervisory staff to ensure that there was a thorough understanding of study requirements and flow of the questionnaire. Field supervisors were present at all times to ensure accurate interviewing and recording of responses. Ten percent of each interviewer's work was unobtrusively monitored for quality control in accordance with the standards set out by the Marketing Research and Intelligence Association (MRIA). A minimum of five calls were made to a household before classifying it as a "no answer."

SAMPLE SELECTION

The most advanced probability sampling techniques are employed in the selection of households for telephone interviewing. The sampling model relies on stratification of the population by 10 regions (Atlantic Canada, Montreal CMA, the rest of Quebec, Toronto CMA, the rest of Ontario, Manitoba, Saskatchewan, Alberta, Vancouver CMA and the rest of British Columbia) and by four community sizes (1,000,000 inhabitants or more, 100,000 to 1,000,000 inhabitants, 5,000 to 100,000 inhabitants, and under 5,000 inhabitants). Samples are generated using a database of active phone ranges. These ranges are made up of a series of contiguous blocks of 100 contiguous phone numbers and are revised three to four times per year after a thorough analysis of the most recent edition of an electronic phonebook. Each number generated is put through an appropriate series of validation procedures before it is retained as part of a sample. Each number generated is looked up in a current electronic phonebook

database to retrieve geographic location, business indicator and “do not call” status. The postal code for listed numbers is verified for accuracy and compared against a list of valid codes for the sample stratum. Non-listed numbers are assigned a “most probable” postal code (FSA) based on the data available for all listed numbers in the phone exchange. This sample selection technique ensures both unlisted numbers and numbers listed after the directory publication are included in the sample.

SAMPLE DESIGN AND RESPONDENT SELECTION

Quotas are maintained within each of the regions to ensure that an equal number of interviews with male and female respondents are obtained. Respondents must indicate their age prior to proceeding with the questionnaire, however, there are no particular age quotas implemented. Qualification is based simply on being 18 years of age or older. From within each multi-person household contacted, respondents 18 years of age and older were screened for random selection using the “next birthday” method. The use of this technique produces results that are as valid and effective as enumerating all persons within a household and selecting one randomly. The sample is then weighted in tabulation to replicate actual population distribution by sex and age within region. Only one interview is conducted per household.

HOW TO READ TABLES

Data is percentaged vertically and, therefore should be read from top-to-bottom. The total number of interviews, both weighted and un-weighted, appears at the top of each column. Percentages are calculated on the weighted bases. Percentages may not add to 100% due to weighting factors or multiple responses. Where an asterisk (*) appears, it signifies any value of less than one-half percent.

SIGNIFICANCE TESTING

When results appear in the detailed tabulations, an indicator of statistically significant differences is added to the tables run on our standard demographic banners. Each column is assigned a letter. When the percentage of one column is significantly different from the percentage of another column the letter representing one of the two columns appears next to the percentage of the other column. Significance testing is done to the 95% confidence level. The columns compared are listed at the bottom of each table.

Note that any statistical test becomes less reliable when the sample sizes are small.

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

TABLE OF CONTENTS

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

QS. INTERNET ACCESS

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	1000	483	517	198	173	210	241	178	74	243	383	65	102	133	117	161	69	643	255	113
UNWEIGHTED TOTAL	1000	500	500	126	149	207	294	224	125	250	250	125	125	125	115	97	63	643	266	99
NET: Any	84%	86%	82%	97%	94%	91%	84%	51%	86%	80%	84%	84%	85%	88%	81%	89%	95%	85%	78%	86%
Home	81%	82%	79%	91%	90%	86%	82%	50%	84%	76%	81%	82%	81%	84%	79%	88%	92%	82%	74%	85%
Work	52%	54%	51%	70%	65%	67%	47%	10%	56%	44%	53%	53%	59%	61%	49%	61%	68%	56%	44%	51%
At School	25%	26%	25%	58%	23%	31%	13%	3%	20%	20%	25%	37%	30%	31%	20%	28%	41%	27%	18%	34%
None of the above	16%	14%	18%	3%	6%	9%	16%	49%	14%	20%	16%	16%	15%	12%	19%	11%	5%	15%	22%	14%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

QS. INTERNET ACCESS

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	1000	530	450	327	193	41	52	202	63	620	423	96	101	140	189	164	170	97
UNWEIGHTED TOTAL	1000	580	402	293	170	37	39	253	58	593	407	84	102	146	192	156	171	99
NET: Any	84%	74%	95%	95%	94%	71%	100%	57%	76%	93%	94%	92%	89%	66%	78%	91%	97%	98%
Home	81%	72%	90%	90%	90%	68%	96%	57%	72%	89%	90%	89%	85%	65%	72%	86%	95%	98%
Work	52%	39%	68%	68%	69%	31%	68%	6%	23%	71%	77%	56%	62%	20%	44%	53%	79%	95%
At School	25%	15%	37%	34%	47%	20%	96%	3%	15%	28%	28%	39%	17%	21%	18%	24%	33%	29%
None of the above	16%	26%	5%	5%	6%	29%	-	43%	24%	7%	6%	8%	11%	34%	22%	9%	3%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

QS. INTERNET ACCESS

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	1000	86	204	371	320	406	201	280	113
UNWEIGHTED TOTAL	1000	96	215	365	305	348	213	285	154
NET: Any	84%	58%	67%	89%	95%	88%	87%	82%	69%
Home	81%	57%	62%	86%	92%	86%	82%	77%	66%
Work	52%	11%	30%	55%	75%	59%	54%	48%	35%
At School	25%	6%	18%	28%	32%	29%	28%	22%	19%
None of the above	16%	42%	33%	11%	5%	12%	13%	18%	31%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q1S. APPROXIMATELY WHAT PERCENTAGE OF E-MAIL MESSAGES THAT YOU RECEIVE WOULD YOU CONSIDER SPAM?

SUBSAMPLE: THOSE WHO HAVE INTERNET ACCESS

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	838	415	422	191	162	191	202	91	64	194	322	55	87	116	95	143	65	550	198	97
UNWEIGHTED TOTAL	810	420	390	121	139	188	244	118	103	193	205	99	103	107	90	85	59	530	203	82
None	11%	12%	10%	4%	5%	11%	17%	23%	15%	15%	9%	6%	10%	13%	15%	7%	12%	11%	14%	9%
1-5	24%	25%	23%	25%	22%	22%	26%	23%	20%	19%	25%	34%	26%	23%	25%	26%	25%	27%	19%	18%
6-10	16%	15%	16%	13%	19%	14%	17%	16%	8%	16%	15%	17%	18%	17%	18%	21%	16%	15%	16%	13%
11-25	13%	12%	14%	15%	16%	13%	11%	7%	20%	12%	12%	9%	15%	15%	10%	15%	11%	12%	12%	20%
26-50	13%	12%	14%	13%	15%	18%	9%	9%	15%	16%	14%	15%	7%	7%	11%	13%	3%	12%	17%	10%
51-75	8%	7%	8%	14%	9%	6%	5%	4%	11%	12%	6%	3%	4%	8%	12%	3%	14%	7%	12%	6%
76-100	8%	10%	7%	12%	7%	7%	7%	7%	8%	5%	11%	3%	10%	7%	4%	6%	12%	9%	5%	9%
DK/NA	7%	7%	8%	4%	7%	9%	8%	11%	4%	4%	8%	12%	9%	9%	4%	7%	7%	7%	5%	16%
MEAN INCL. 0	24.96	25.40	24.54	31.62	26.88	24.65	19.95	18.54	27.21	25.56	26.78	17.76	22.17	22.96	22.23	20.59	28.02	24.42	26.54	26.91
SD	28.28	29.39	27.16	30.32	27.24	27.39	26.83	27.50	28.47	27.94	29.64	22.93	27.82	27.18	27.25	24.15	32.01	28.46	27.98	28.74
SE	1.12	1.63	1.55	2.87	2.49	2.24	1.92	3.02	3.07	2.13	2.20	2.78	2.99	2.83	3.03	2.75	4.45	1.41	2.12	3.77
MEAN EXCL. 0	28.38	29.16	27.63	33.14	28.50	27.89	24.52	25.20	32.12	30.31	29.54	19.16	24.75	26.91	26.48	22.36	32.10	27.53	31.10	30.20
SD	28.50	29.70	27.29	30.21	27.21	27.54	27.81	29.35	28.27	27.96	29.79	23.25	28.29	27.57	27.80	24.37	32.30	28.76	27.85	28.76
SE	1.22	1.79	1.67	2.94	2.56	2.41	2.20	3.81	3.38	2.36	2.34	2.95	3.24	3.11	3.44	2.91	4.82	1.53	2.31	4.03

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q1S. APPROXIMATELY WHAT PERCENTAGE OF E-MAIL MESSAGES THAT YOU RECEIVE WOULD YOU CONSIDER SPAM?

SUBSAMPLE: THOSE WHO HAVE INTERNET ACCESS

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	838	394	427	311	183	29	52	116	47	575	397	89	90	92	147	149	165	95
UNWEIGHTED TOTAL	810	417	379	278	158	25	39	149	41	541	378	75	88	85	145	139	166	97
None	11%	15%	8%	8%	11%	8%	8%	18%	17%	10%	10%	9%	13%	12%	11%	13%	7%	7%
1-5	24%	28%	21%	18%	24%	34%	33%	23%	15%	24%	26%	22%	16%	25%	18%	28%	25%	33%
6-10	16%	15%	15%	14%	14%	12%	19%	23%	15%	14%	13%	12%	18%	12%	13%	12%	22%	14%
11-25	13%	12%	14%	16%	12%	8%	21%	8%	14%	14%	14%	13%	14%	18%	12%	9%	15%	17%
26-50	13%	9%	17%	18%	16%	15%	6%	9%	5%	15%	14%	18%	17%	11%	17%	16%	9%	14%
51-75	8%	6%	9%	9%	8%	7%	5%	3%	13%	8%	9%	7%	9%	5%	11%	7%	9%	5%
76-100	8%	9%	8%	8%	9%	4%	5%	5%	14%	9%	8%	12%	7%	11%	11%	7%	8%	5%
DK/NA	7%	7%	8%	8%	6%	12%	2%	12%	7%	6%	6%	7%	6%	5%	7%	7%	4%	5%
MEAN INCL. 0	24.96	21.79	27.88	28.95	26.56	21.49	19.17	16.54	29.16	26.57	25.87	30.07	26.23	25.15	30.82	24.12	24.02	20.85
SD	28.28	27.93	28.48	28.46	29.35	26.47	25.19	23.57	31.69	28.61	28.37	30.78	27.57	28.56	30.58	28.38	27.66	23.86
SE	1.12	1.57	1.62	1.90	2.58	6.27	4.23	2.27	5.47	1.37	1.62	3.99	3.35	3.47	2.87	2.71	2.39	2.71
MEAN EXCL. 0	28.38	25.83	30.69	31.70	30.23	23.63	20.94	20.67	35.84	29.73	28.81	33.33	30.30	28.66	34.98	28.01	26.05	22.54
SD	28.50	28.64	28.40	28.27	29.49	26.85	25.63	24.69	31.53	28.67	28.49	30.68	27.47	28.80	30.26	28.75	27.87	24.03
SE	1.22	1.78	1.71	1.98	2.78	6.78	4.53	2.70	6.22	1.46	1.73	4.19	3.60	3.79	3.06	3.01	2.52	2.84

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q1S. APPROXIMATELY WHAT PERCENTAGE OF E-MAIL MESSAGES THAT YOU RECEIVE WOULD YOU CONSIDER SPAM?

SUBSAMPLE: THOSE WHO HAVE INTERNET ACCESS

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	838	50	137	332	304	356	174	229	78
UNWEIGHTED TOTAL	810	53	141	314	288	297	179	232	102
None	11%	26%	18%	10%	7%	10%	7%	14%	16%
1-5	24%	12%	22%	21%	30%	26%	23%	22%	19%
6-10	16%	12%	16%	14%	17%	19%	12%	16%	8%
11-25	13%	11%	10%	13%	15%	14%	12%	14%	12%
26-50	13%	11%	12%	15%	12%	10%	18%	12%	17%
51-75	8%	8%	8%	9%	5%	8%	9%	8%	6%
76-100	8%	6%	8%	10%	8%	6%	13%	8%	7%
DK/NA	7%	14%	6%	8%	6%	7%	6%	6%	15%
MEAN INCL. 0	24.96	23.30	23.62	28.16	21.71	21.73	31.65	24.93	24.74
SD	28.28	28.82	29.11	29.33	26.16	26.17	31.15	28.67	27.40
SE	1.12	4.58	2.74	1.88	1.74	1.66	2.71	2.10	3.22
MEAN EXCL. 0	28.38	33.49	29.15	31.61	23.54	24.47	34.26	29.21	30.46
SD	28.50	29.21	29.75	29.27	26.44	26.54	31.00	28.95	27.38
SE	1.22	5.53	3.16	2.00	1.85	1.81	2.81	2.32	3.58

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q2S. HOW MUCH OF A PROBLEM IS IT FOR YOU PERSONALLY TO RECEIVE SPAM?
IS IT A MAJOR PROBLEM, A MINOR PROBLEM OR NOT A PROBLEM AT ALL?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
A major problem	15%	14%	17%	8%	19%	17%	18%	17%	16%	13%	18%	10%	20%	11%	12%	16%	8%	16%	15%	12%
A minor problem	58%	59%	57%	56%	54%	63%	60%	54%	53%	55%	60%	52%	60%	61%	56%	59%	63%	59%	54%	62%
Not a problem at all	27%	27%	26%	36%	27%	20%	22%	29%	30%	32%	22%	38%	20%	28%	32%	25%	30%	25%	31%	26%
DK/NA	*%	-	*%	-	-	1%	-	-	2%	-	-	-	-	-	-	-	-	*%	-	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q2S. HOW MUCH OF A PROBLEM IS IT FOR YOU PERSONALLY TO RECEIVE SPAM?
IS IT A MAJOR PROBLEM, A MINOR PROBLEM OR NOT A PROBLEM AT ALL?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
A major problem	15%	14%	16%	19%	12%	20%	13%	15%	26%	14%	15%	15%	12%	15%	19%	12%	15%	16%
A minor problem	58%	59%	56%	55%	60%	61%	50%	56%	63%	58%	57%	48%	73%	45%	55%	58%	64%	59%
Not a problem at all	27%	26%	27%	25%	27%	20%	37%	29%	11%	27%	28%	37%	15%	40%	26%	29%	21%	24%
DK/NA	*%	*%	-	-	-	-	-	-	-	*%	*%	-	-	-	-	1%	-	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q2S. HOW MUCH OF A PROBLEM IS IT FOR YOU PERSONALLY TO RECEIVE SPAM?
IS IT A MAJOR PROBLEM, A MINOR PROBLEM OR NOT A PROBLEM AT ALL?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
A major problem	15%	26%	15%	16%	12%	13%	9%	22%	21%
A minor problem	58%	63%	51%	54%	64%	60%	64%	52%	51%
Not a problem at all	27%	11%	34%	29%	24%	27%	27%	25%	27%
DK/NA	*%	-	-	*%	-	-	-	*%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q3S. GENERALLY, WHAT DO YOU DO WHEN YOU RECEIVE SPAM? DO YOU…?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Use a filtering program to try and stop it	53%	52%	54%	41%	64%	55%	57%	47%	50%	46%	57%	50%	54%	57%	52%	60%	57%	57%	45%	43%
Ignore it	36%	38%	34%	47%	29%	36%	29%	33%	39%	49%	32%	42%	28%	25%	43%	30%	26%	29%	50%	51%
Respond to the sender	2%	1%	3%	2%	1%	2%	3%	2%	1%	2%	2%	-	2%	3%	3%	1%	4%	2%	2%	2%
Complain to your ISP	1%	1%	1%	1%	2%	1%	1%	1%	-	1%	2%	-	2%	2%	-	-	3%	2%	1%	-
Other	6%	7%	6%	6%	3%	5%	8%	14%	8%	2%	7%	6%	12%	7%	2%	8%	8%	8%	2%	4%
DK/NA	2%	1%	2%	3%	1%	1%	2%	3%	2%	-	1%	2%	3%	5%	-	-	3%	2%	*%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q3S. GENERALLY, WHAT DO YOU DO WHEN YOU RECEIVE SPAM? DO YOU…?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Use a filtering program to try and stop it	53%	50%	56%	55%	50%	50%	65%	48%	45%	53%	52%	53%	58%	41%	51%	43%	61%	65%
Ignore it	36%	36%	36%	38%	39%	32%	25%	36%	38%	37%	37%	42%	33%	38%	41%	48%	29%	27%
Respond to the sender	2%	3%	1%	1%	2%	4%	4%	1%	4%	2%	2%	-	4%	2%	2%	2%	2%	3%
Complain to your ISP	1%	3%	-	-	-	-	3%	2%	4%	1%	1%	-	-	5%	1%	-	1%	1%
Other	6%	8%	5%	4%	7%	14%	2%	11%	9%	5%	6%	5%	2%	13%	6%	5%	6%	3%
DK/NA	2%	1%	2%	1%	3%	-	-	2%	-	2%	2%	-	2%	-	-	3%	1%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q3S. GENERALLY, WHAT DO YOU DO WHEN YOU RECEIVE SPAM? DO YOU…?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Use a filtering program to try and stop it	53%	32%	41%	52%	61%	56%	48%	54%	47%
Ignore it	36%	50%	44%	35%	31%	33%	39%	36%	41%
Respond to the sender	2%	3%	3%	1%	2%	3%	1%	2%	2%
Complain to your ISP	1%	2%	1%	2%	1%	1%	4%	*%	1%
Other	6%	13%	8%	7%	4%	6%	6%	6%	9%
DK/NA	2%	-	2%	2%	1%	1%	2%	2%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q4S. WHICH ONE OF THE FOLLOWING PARTICULAR TYPES OF SPAM CONCERNS YOU THE MOST?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Viruses (e-mails that infect your computer with viruses)	40%	36%	43%	42%	40%	39%	40%	35%	55%	34%	43%	44%	43%	30%	32%	47%	27%	42%	34%	43%
Offensive or illegal product marketing (e.g., erectile dysfunction drugs)	18%	20%	16%	18%	19%	21%	10%	29%	8%	12%	20%	20%	19%	27%	10%	15%	29%	21%	15%	9%
SPYWARE (e-mails that link to spyware or install it when you click)	15%	15%	14%	19%	15%	16%	10%	11%	14%	18%	13%	18%	15%	14%	22%	15%	9%	14%	17%	15%
PHISHING (fake banking e-mails asking for you to enter account information)	14%	15%	14%	16%	14%	11%	17%	14%	10%	21%	14%	11%	13%	12%	18%	17%	13%	12%	18%	20%
All of them equally	10%	11%	10%	5%	9%	13%	17%	5%	9%	13%	10%	5%	8%	12%	15%	6%	13%	10%	12%	10%
None of them	1%	1%	1%	-	2%	1%	3%	-	2%	3%	-	-	1%	2%	3%	-	4%	1%	3%	-
DK/NA	1%	1%	1%	-	1%	1%	2%	7%	2%	*%	1%	3%	2%	3%	-	-	5%	1%	1%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q4S. WHICH ONE OF THE FOLLOWING PARTICULAR TYPES OF SPAM CONCERNS YOU THE MOST?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Viruses (e-mails that infect your computer with viruses)	40%	39%	41%	39%	41%	81%	44%	41%	35%	38%	38%	37%	36%	47%	42%	35%	44%	38%
Offensive or illegal product marketing (e.g., erectile dysfunction drugs)	18%	16%	20%	21%	20%	3%	18%	21%	26%	18%	15%	28%	21%	21%	17%	17%	18%	12%
SPYWARE (e-mails that link to spyware or install it when you click)	15%	15%	16%	16%	15%	10%	23%	11%	19%	15%	16%	13%	12%	12%	14%	15%	14%	22%
PHISHING (fake banking e-mails asking for you to enter account information)	14%	15%	14%	13%	14%	-	9%	15%	6%	16%	18%	9%	13%	8%	17%	19%	15%	17%
All of them equally	10%	12%	8%	9%	8%	6%	7%	6%	13%	11%	11%	8%	14%	8%	10%	11%	8%	8%
None of them	1%	2%	1%	1%	-	-	-	2%	-	1%	1%	1%	3%	3%	-	1%	2%	1%
DK/NA	1%	2%	1%	1%	1%	-	-	5%	-	1%	1%	4%	1%	-	1%	2%	-	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q4S. WHICH ONE OF THE FOLLOWING PARTICULAR TYPES OF SPAM CONCERNS YOU THE MOST?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Viruses (e-mails that infect your computer with viruses)	40%	37%	37%	39%	44%	38%	44%	41%	36%
Offensive or illegal product marketing (e.g., erectile dysfunction drugs)	18%	16%	24%	20%	14%	16%	17%	20%	22%
SPYWARE (e-mails that link to spyware or install it when you click)	15%	19%	14%	16%	14%	16%	14%	14%	14%
PHISHING (fake banking e-mails asking for you to enter account information)	14%	9%	13%	14%	14%	16%	14%	12%	18%
All of them equally	10%	10%	8%	10%	11%	10%	8%	13%	7%
None of them	1%	2%	2%	1%	1%	2%	*%	1%	3%
DK/NA	1%	6%	1%	1%	1%	1%	2%	1%	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q5S. THERE ARE A NUMBER OF THINGS A PERSON COULD DO TO CONTROL AND REDUCE SPAM AND ANY POTENTIAL SECURITY RISKS FROM IT. WHICH OF THE FOLLOWING STEPS HAVE YOU TAKEN IN THE PAST YEAR?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Installing anti-spam, antivirus software or a firewall	88%	87%	88%	81%	91%	93%	91%	79%	87%	86%	87%	88%	96%	87%	90%	88%	82%	89%	86%	86%
Never opening e-mails from unknown or untrusted sources	87%	83%	90%	87%	93%	86%	88%	72%	84%	90%	84%	94%	89%	84%	89%	79%	85%	86%	87%	91%
Setting up filtering options in e-mail or browser software	72%	70%	73%	70%	75%	77%	70%	61%	66%	71%	73%	70%	75%	71%	76%	68%	67%	73%	68%	70%
Updating your web browser	70%	71%	70%	77%	69%	72%	70%	52%	60%	71%	73%	72%	64%	72%	75%	68%	74%	69%	71%	77%
Changing key passwords frequently (e.g. banking)	44%	42%	46%	42%	46%	60%	39%	18%	37%	33%	51%	53%	48%	41%	30%	53%	35%	47%	34%	51%
Using more than one e-mail address (e.g. an e-mail address for online shopping)	43%	45%	41%	49%	53%	45%	33%	25%	40%	36%	47%	43%	44%	47%	39%	51%	45%	45%	34%	52%
Turning off your e-mail message preview pane	31%	34%	28%	29%	35%	38%	27%	19%	46%	26%	34%	29%	31%	23%	26%	30%	17%	33%	27%	27%
None of the above	1%	1%	1%	1%	-	1%	*%	4%	5%	-	-	1%	-	2%	-	-	2%	1%	1%	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q5S. THERE ARE A NUMBER OF THINGS A PERSON COULD DO TO CONTROL AND REDUCE SPAM AND ANY POTENTIAL SECURITY RISKS FROM IT. WHICH OF THE FOLLOWING STEPS HAVE YOU TAKEN IN THE PAST YEAR?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Installing anti-spam, antivirus software or a firewall	88%	85%	90%	91%	90%	90%	79%	87%	87%	89%	90%	79%	93%	82%	81%	90%	91%	97%
Never opening e-mails from unknown or untrusted sources	87%	84%	90%	91%	89%	83%	94%	72%	69%	90%	91%	86%	91%	77%	86%	90%	89%	92%
Setting up filtering options in e-mail or browser software	72%	69%	73%	73%	72%	71%	78%	59%	79%	72%	74%	62%	77%	60%	73%	68%	73%	82%
Updating your web browser	70%	69%	72%	70%	77%	75%	82%	54%	74%	72%	72%	66%	76%	65%	67%	71%	70%	69%
Changing key passwords frequently (e.g. banking)	44%	37%	50%	48%	49%	56%	35%	26%	44%	47%	50%	39%	45%	41%	50%	39%	44%	48%
Using more than one e-mail address (e.g. an e-mail address for online shopping)	43%	44%	43%	40%	47%	40%	54%	24%	40%	46%	46%	44%	45%	39%	44%	35%	46%	51%
Turning off your e-mail message preview pane	31%	30%	30%	32%	30%	36%	31%	23%	51%	31%	31%	33%	26%	34%	32%	35%	34%	15%
None of the above	1%	1%	1%	*%	1%	4%	2%	3%	-	*%	-	-	1%	2%	1%	*%	-	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q5S. THERE ARE A NUMBER OF THINGS A PERSON COULD DO TO CONTROL AND REDUCE SPAM AND ANY POTENTIAL SECURITY RISKS FROM IT. WHICH OF THE FOLLOWING STEPS HAVE YOU TAKEN IN THE PAST YEAR?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Installing anti-spam, antivirus software or a firewall	88%	72%	85%	88%	90%	88%	86%	89%	89%
Never opening e-mails from unknown or untrusted sources	87%	68%	88%	88%	88%	85%	90%	88%	83%
Setting up filtering options in e-mail or browser software	72%	65%	62%	70%	77%	70%	78%	70%	65%
Updating your web browser	70%	58%	67%	70%	73%	70%	73%	67%	75%
Changing key passwords frequently (e.g. banking)	44%	28%	44%	49%	42%	42%	45%	47%	44%
Using more than one e-mail address (e.g. an e-mail address for online shopping)	43%	20%	34%	39%	55%	46%	50%	36%	36%
Turning off your e-mail message preview pane	31%	37%	32%	36%	24%	26%	33%	38%	33%
None of the above	1%	-	3%	*%	*%	*%	1%	1%	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q6S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS OR SPAM, WHICH OF THE FOLLOWING WOULD BE THE BEST WAY TO PENALIZE SPAMMERS?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Fining spammers	33%	32%	34%	41%	24%	36%	33%	28%	29%	38%	31%	36%	32%	35%	41%	25%	27%	33%	37%	24%
Criminal charges against spammers	30%	33%	27%	22%	39%	31%	29%	31%	30%	22%	33%	30%	30%	32%	29%	31%	28%	32%	23%	34%
Injunctions against spammers to make them to stop	21%	19%	23%	22%	19%	18%	24%	25%	22%	22%	20%	26%	23%	19%	15%	28%	23%	20%	24%	25%
Giving people the right to sue spammers	9%	8%	9%	11%	11%	9%	5%	6%	9%	12%	9%	5%	7%	7%	7%	12%	12%	9%	9%	12%
All of them equally	2%	3%	1%	1%	1%	1%	5%	-	3%	1%	2%	2%	3%	1%	2%	1%	-	2%	1%	4%
None of them	2%	2%	2%	1%	4%	2%	4%	1%	3%	3%	1%	1%	5%	3%	2%	1%	5%	2%	3%	-
DK/NA	2%	2%	3%	3%	1%	3%	*%	9%	3%	2%	3%	-	-	3%	4%	3%	6%	3%	3%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q6S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS OR SPAM, WHICH OF THE FOLLOWING WOULD BE THE BEST WAY TO PENALIZE SPAMMERS?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Fining spammers	33%	29%	35%	32%	39%	26%	40%	27%	33%	34%	34%	25%	42%	26%	37%	35%	31%	29%
Criminal charges against spammers	30%	33%	28%	31%	23%	50%	13%	35%	37%	29%	30%	29%	25%	31%	31%	23%	34%	43%
Injunctions against spammers to make them to stop	21%	21%	22%	21%	22%	16%	18%	25%	14%	22%	21%	29%	18%	21%	19%	26%	23%	18%
Giving people the right to sue spammers	9%	10%	9%	10%	9%	8%	20%	7%	10%	9%	9%	8%	5%	12%	8%	9%	7%	3%
All of them equally	2%	2%	2%	2%	4%	-	4%	1%	2%	2%	2%	3%	1%	2%	3%	2%	1%	3%
None of them	2%	2%	3%	4%	3%	-	1%	-	-	3%	3%	2%	6%	3%	-	3%	4%	2%
DK/NA	2%	3%	1%	1%	1%	-	2%	5%	5%	2%	1%	4%	3%	6%	3%	2%	1%	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q6S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS OR SPAM, WHICH OF THE FOLLOWING WOULD BE THE BEST WAY TO PENALIZE SPAMMERS?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Fining spammers	33%	29%	34%	31%	34%	31%	37%	33%	37%
Criminal charges against spammers	30%	44%	33%	27%	30%	30%	27%	33%	26%
Injunctions against spammers to make them to stop	21%	17%	19%	24%	21%	23%	17%	20%	25%
Giving people the right to sue spammers	9%	10%	6%	11%	8%	9%	9%	9%	8%
All of them equally	2%	-	3%	2%	2%	1%	3%	2%	3%
None of them	2%	-	2%	2%	3%	3%	3%	2%	-
DK/NA	2%	-	3%	3%	2%	3%	4%	1%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q7S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS, WHICH OF THE FOLLOWING SHOULD BE EXEMPT FROM THE LAW, IF ANY?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Businesses with whom you already do business (that is, you are their customer presently)	43%	46%	41%	35%	54%	46%	43%	35%	32%	41%	44%	34%	43%	56%	38%	38%	54%	46%	41%	30%
Registered Charities	31%	35%	28%	34%	41%	26%	29%	23%	35%	36%	26%	29%	33%	36%	41%	25%	32%	32%	33%	26%
Political parties, candidates in elections and political riding associations	21%	21%	21%	19%	24%	17%	23%	21%	18%	24%	21%	18%	16%	20%	24%	22%	16%	19%	24%	22%
Newspapers of general circulation	18%	17%	19%	15%	19%	13%	24%	20%	18%	25%	15%	10%	19%	19%	20%	17%	20%	16%	22%	19%
Polling companies	17%	19%	15%	14%	17%	19%	18%	16%	9%	21%	16%	19%	19%	12%	23%	16%	10%	15%	22%	18%
All of them	9%	9%	8%	13%	5%	9%	8%	7%	4%	12%	8%	13%	6%	6%	17%	11%	6%	8%	12%	6%
None of them	13%	13%	13%	11%	13%	15%	13%	16%	18%	10%	15%	15%	12%	12%	9%	18%	16%	14%	10%	17%
DK/NA	3%	2%	4%	1%	2%	2%	5%	6%	3%	3%	2%	2%	4%	3%	3%	-	4%	2%	4%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q7S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS, WHICH OF THE FOLLOWING SHOULD BE EXEMPT FROM THE LAW, IF ANY?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Businesses with whom you already do business (that is, you are their customer presently)	43%	43%	44%	48%	32%	47%	35%	37%	35%	46%	44%	47%	53%	31%	49%	44%	43%	51%
Registered Charities	31%	34%	29%	30%	27%	14%	37%	24%	22%	34%	33%	35%	39%	29%	30%	43%	30%	31%
Political parties, candidates in elections and political riding associations	21%	24%	19%	19%	19%	21%	18%	24%	18%	21%	18%	31%	21%	24%	27%	24%	22%	17%
Newspapers of general circulation	18%	18%	18%	18%	20%	23%	17%	21%	12%	18%	17%	22%	18%	22%	21%	17%	17%	13%
Polling companies	17%	17%	17%	17%	17%	20%	11%	15%	34%	17%	18%	23%	8%	29%	13%	17%	19%	13%
All of them	9%	9%	8%	9%	8%	-	7%	8%	8%	10%	12%	5%	4%	5%	8%	5%	12%	16%
None of them	13%	13%	14%	13%	14%	11%	21%	16%	13%	12%	14%	6%	13%	10%	12%	11%	15%	12%
DK/NA	3%	4%	2%	2%	*%	-	-	9%	-	2%	2%	1%	3%	8%	2%	2%	1%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q7S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL UNSOLICITED E-MAILS, WHICH OF THE FOLLOWING SHOULD BE EXEMPT FROM THE LAW, IF ANY?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Businesses with whom you already do business (that is, you are their customer presently)	43%	23%	43%	43%	46%	40%	50%	40%	49%
Registered Charities	31%	14%	33%	31%	33%	32%	36%	28%	27%
Political parties, candidates in elections and political riding associations	21%	32%	23%	16%	24%	20%	19%	21%	29%
Newspapers of general circulation	18%	18%	22%	17%	17%	18%	21%	15%	22%
Polling companies	17%	26%	14%	16%	18%	16%	16%	16%	27%
All of them	9%	12%	5%	9%	10%	11%	5%	9%	5%
None of them	13%	20%	7%	12%	16%	15%	12%	13%	9%
DK/NA	3%	2%	6%	2%	2%	2%	3%	4%	4%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q8S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL SPAM WHEREBY YOUR CONSENT WAS REQUIRED BEFORE COMPANIES WERE ALLOWED TO SEND YOU UNSOLICITED COMMERCIAL E-MAILS, WHAT WOULD BE THE BEST WAY FOR THIS TO WORK? SHOULD IT BE THAT ...?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
You must OPT-OUT of receiving the company's e-mails, meaning companies can assume your consent until you ask the company to stop	13%	16%	10%	17%	10%	15%	8%	16%	6%	13%	13%	14%	12%	17%	9%	16%	17%	14%	11%	14%
You must OPT-IN to receiving the company's e-mails, meaning companies may not send you e-mails unless you provide your prior consent	86%	81%	90%	83%	89%	84%	89%	82%	93%	85%	85%	86%	86%	83%	88%	84%	81%	85%	87%	86%
DK/NA	1%	2%	*%	-	1%	2%	2%	1%	1%	2%	1%	-	2%	1%	4%	-	2%	1%	2%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q8S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL SPAM WHEREBY YOUR CONSENT WAS REQUIRED BEFORE COMPANIES WERE ALLOWED TO SEND YOU UNSOLICITED COMMERCIAL E-MAILS, WHAT WOULD BE THE BEST WAY FOR THIS TO WORK? SHOULD IT BE THAT ...?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
You must OPT-OUT of receiving the company's e-mails, meaning companies can assume your consent until you ask the company to stop	13%	12%	15%	16%	13%	4%	29%	14%	4%	12%	11%	18%	13%	12%	13%	10%	11%	21%
You must OPT-IN to receiving the company's e-mails, meaning companies may not send you e-mails unless you provide your prior consent	86%	87%	84%	84%	87%	96%	71%	85%	92%	86%	88%	81%	85%	86%	87%	88%	88%	79%
DK/NA	1%	2%	*%	1%	-	-	-	1%	4%	1%	1%	1%	2%	2%	-	1%	1%	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q8S. IF THE FEDERAL GOVERNMENT PASSED A LAW TO CONTROL SPAM WHEREBY YOUR CONSENT WAS REQUIRED BEFORE COMPANIES WERE ALLOWED TO SEND YOU UNSOLICITED COMMERCIAL E-MAILS, WHAT WOULD BE THE BEST WAY FOR THIS TO WORK? SHOULD IT BE THAT ...?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
You must OPT-OUT of receiving the company's e-mails, meaning companies can assume your consent until you ask the company to stop	13%	8%	13%	15%	11%	13%	15%	11%	15%
You must OPT-IN to receiving the company's e-mails, meaning companies may not send you e-mails unless you provide your prior consent	86%	92%	85%	84%	87%	85%	84%	88%	85%
DK/NA	1%	-	1%	1%	1%	2%	1%	1%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q9S. IF THERE WERE A WAY FOR YOU TO MAKE A COMPLAINT ABOUT GETTING SPAM, HOW LIKELY WOULD YOU BE TO COMPLAIN? WOULD YOU BE VERY, SOMEWHAT, NOT VERY OR NOT AT ALL LIKELY TO COMPLAIN?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
TOP 2 BOX	71%	70%	73%	56%	70%	79%	77%	81%	81%	60%	77%	65%	75%	68%	56%	79%	59%	73%	62%	78%
Very likely	32%	32%	33%	22%	27%	36%	43%	38%	24%	20%	44%	28%	30%	29%	18%	43%	21%	36%	23%	35%
Somewhat likely	39%	38%	39%	34%	43%	42%	33%	44%	56%	39%	33%	37%	45%	38%	39%	36%	38%	37%	39%	43%
Not very likely	18%	16%	20%	26%	17%	16%	16%	7%	12%	33%	12%	23%	10%	18%	37%	11%	24%	15%	31%	12%
Not at all likely	10%	15%	6%	18%	11%	5%	7%	10%	8%	7%	11%	12%	15%	13%	5%	10%	13%	11%	8%	9%
BOTTOM 2 BOX	28%	30%	27%	44%	28%	21%	23%	17%	19%	39%	23%	35%	25%	30%	42%	21%	37%	26%	38%	21%
DK/NA	*%	-	1%	-	2%	-	-	1%	-	1%	-	-	-	2%	2%	-	4%	*%	-	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q9S. IF THERE WERE A WAY FOR YOU TO MAKE A COMPLAINT ABOUT GETTING SPAM, HOW LIKELY WOULD YOU BE TO COMPLAIN? WOULD YOU BE VERY, SOMEWHAT, NOT VERY OR NOT AT ALL LIKELY TO COMPLAIN?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION			EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
TOP 2 BOX	71%	73%	70%	70%	68%	80%	58%	79%	73%	70%	71%	61%	73%	71%	71%	71%	69%	75%
Very likely	32%	36%	29%	29%	29%	47%	20%	34%	67%	30%	31%	21%	36%	36%	29%	23%	32%	41%
Somewhat likely	39%	36%	40%	41%	39%	33%	38%	45%	6%	40%	41%	39%	37%	35%	42%	48%	38%	34%
Not very likely	18%	16%	20%	22%	21%	14%	27%	13%	16%	19%	19%	23%	13%	11%	17%	20%	22%	15%
Not at all likely	10%	11%	10%	8%	11%	6%	14%	7%	11%	11%	9%	17%	12%	17%	12%	8%	8%	10%
BOTTOM 2 BOX	28%	27%	30%	29%	32%	20%	42%	20%	27%	30%	29%	39%	25%	28%	29%	29%	31%	25%
DK/NA	*%	*%	*%	*%	-	-	-	1%	-	1%	*%	-	2%	2%	-	-	-	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q9S. IF THERE WERE A WAY FOR YOU TO MAKE A COMPLAINT ABOUT GETTING SPAM, HOW LIKELY WOULD YOU BE TO COMPLAIN? WOULD YOU BE VERY, SOMEWHAT, NOT VERY OR NOT AT ALL LIKELY TO COMPLAIN?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
TOP 2 BOX	71%	78%	74%	72%	68%	68%	70%	77%	72%
Very likely	32%	50%	32%	34%	29%	30%	30%	39%	31%
Somewhat likely	39%	28%	43%	38%	39%	38%	39%	38%	41%
Not very likely	18%	13%	18%	17%	20%	20%	17%	15%	17%
Not at all likely	10%	8%	6%	10%	12%	10%	13%	8%	11%
BOTTOM 2 BOX	28%	22%	24%	28%	32%	31%	30%	23%	28%
DK/NA	*%	-	1%	-	1%	1%	-	-	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q10S. WHICH OF THE FOLLOWING WOULD BE THE MOST CONVENIENT WAY FOR YOU TO COMPLAIN ABOUT SPAM?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Forwarding the e-mail to a “spam complaint centre” e-mail address	50%	52%	48%	45%	56%	55%	54%	35%	49%	52%	48%	45%	48%	58%	54%	50%	56%	52%	52%	43%
Clicking on a link on the e-mail	26%	24%	28%	36%	26%	24%	18%	21%	25%	28%	25%	23%	29%	25%	28%	31%	26%	24%	27%	31%
Calling a toll-free number	14%	13%	15%	8%	13%	14%	15%	34%	17%	14%	15%	21%	12%	8%	13%	11%	5%	14%	13%	15%
Filling in a form on a website	8%	8%	7%	11%	4%	6%	10%	5%	6%	5%	9%	11%	10%	7%	6%	7%	9%	8%	7%	7%
All of them equally	1%	*%	1%	-	-	2%	1%	-	-	-	2%	-	-	-	-	1%	-	1%	-	2%
None of them	1%	1%	*%	-	1%	-	1%	-	2%	1%	*%	-	-	-	-	-	-	1%	1%	-
DK/NA	1%	1%	1%	-	-	1%	*%	6%	1%	-	1%	-	-	2%	-	-	3%	1%	-	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q10S. WHICH OF THE FOLLOWING WOULD BE THE MOST CONVENIENT WAY FOR YOU TO COMPLAIN ABOUT SPAM?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Forwarding the e-mail to a “spam complaint centre” e-mail address	50%	49%	51%	54%	44%	53%	45%	43%	53%	52%	54%	49%	41%	30%	51%	51%	60%	58%
Clicking on a link on the e-mail	26%	25%	27%	27%	30%	30%	35%	17%	5%	28%	24%	33%	41%	42%	24%	25%	22%	26%
Calling a toll-free number	14%	16%	12%	13%	12%	11%	7%	30%	31%	11%	12%	9%	7%	17%	18%	16%	11%	8%
Filling in a form on a website	8%	7%	8%	6%	11%	6%	12%	6%	11%	8%	8%	5%	8%	10%	5%	8%	7%	5%
All of them equally	1%	*%	1%	1%	2%	-	-	-	-	1%	-	2%	2%	-	-	1%	-	2%
None of them	1%	1%	-	-	-	-	-	2%	-	*%	*%	-	1%	-	-	-	-	-
DK/NA	1%	1%	*%	-	1%	-	-	3%	-	*%	*%	2%	-	-	2%	-	-	1%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q10S. WHICH OF THE FOLLOWING WOULD BE THE MOST CONVENIENT WAY FOR YOU TO COMPLAIN ABOUT SPAM?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Forwarding the e-mail to a “spam complaint centre” e-mail address	50%	39%	45%	53%	52%	51%	52%	50%	43%
Clicking on a link on the e-mail	26%	22%	30%	24%	28%	28%	24%	24%	29%
Calling a toll-free number	14%	30%	19%	12%	11%	11%	14%	18%	19%
Filling in a form on a website	8%	5%	4%	9%	8%	9%	7%	6%	9%
All of them equally	1%	-	-	1%	1%	1%	1%	1%	-
None of them	1%	-	1%	*%	1%	-	1%	1%	-
DK/NA	1%	4%	1%	1%	*%	1%	2%	*%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q11S. WHICH OF THE FOLLOWING WOULD BE THE WAY YOU WOULD PREFER TO HEAR ABOUT HOW YOUR COMPLAINT ABOUT SPAM WAS HANDLED?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		GENDER		AGE					REGION									LANGUAGE		
	TOTAL	M	F	18-29	30-39	40-49	50-64	65+	ATL	QC	ON	MB/SK	AB	BC	Mon. CMA	Tor. CMA	Van. CMA	Eng.	Fre.	Other
TOTAL WEIGHTED	683	337	347	175	143	154	152	60	52	156	268	45	71	90	76	122	53	454	161	73
UNWEIGHTED TOTAL	640	333	307	111	123	148	185	73	80	150	168	76	83	83	69	72	48	425	159	59
Receiving an e-mail notice when the complaint is resolved or other result	37%	36%	38%	41%	36%	34%	35%	43%	43%	32%	33%	43%	37%	51%	39%	30%	61%	38%	34%	38%
Obtaining a complaint tracking number and being able to track the complaint online	35%	36%	34%	36%	35%	38%	34%	26%	32%	35%	40%	32%	33%	26%	30%	47%	20%	33%	37%	38%
Receiving an e-mail acknowledgement of receipt of your complaint	22%	22%	23%	20%	23%	23%	25%	21%	24%	25%	22%	21%	24%	19%	21%	20%	13%	23%	21%	19%
All of the above	1%	1%	2%	2%	2%	2%	1%	-	-	4%	1%	1%	-	-	6%	1%	-	1%	3%	-
Other	*%	-	*%	-	*%	-	-	-	-	-	-	2%	-	-	-	-	-	*%	-	-
None of the above	3%	3%	2%	2%	2%	3%	2%	4%	2%	3%	2%	1%	4%	2%	4%	2%	3%	2%	3%	3%
DK/NA	1%	1%	1%	-	1%	-	2%	7%	-	1%	1%	1%	1%	3%	1%	-	3%	1%	1%	2%

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q11S. WHICH OF THE FOLLOWING WOULD BE THE WAY YOU WOULD PREFER TO HEAR ABOUT HOW YOUR COMPLAINT ABOUT SPAM WAS HANDLED?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		HOUSEHOLD COMPOSITION				EMPLOYMENT STATUS								FAMILY INCOME				
	TOTAL	Adlts only	Any kids	Kids 0-17	Kids 18+	Home-maker	Stu-dent	Re-tired	Unemp loyed	TOTAL Emp-loyed	Emp. Full-time	Emp. Part-time	Self Emp-loyed	Under $25K	$25K Under $50K	$50K Under $80K	$80K Under $120K	Over $120K
TOTAL WEIGHTED	683	310	358	260	150	23	47	81	36	481	334	74	73	76	121	119	146	84
UNWEIGHTED TOTAL	640	314	314	231	129	17	34	100	29	448	314	63	71	68	115	104	142	86
Receiving an e-mail notice when the complaint is resolved or other result	37%	39%	36%	37%	33%	15%	46%	40%	49%	36%	36%	37%	37%	43%	38%	31%	41%	42%
Obtaining a complaint tracking number and being able to track the complaint online	35%	35%	34%	36%	34%	60%	36%	27%	32%	36%	37%	36%	29%	31%	32%	43%	38%	25%
Receiving an e-mail acknowledgement of receipt of your complaint	22%	21%	24%	24%	25%	25%	7%	23%	19%	24%	23%	24%	29%	24%	26%	23%	17%	26%
All of the above	1%	1%	2%	1%	2%	-	6%	1%	-	1%	1%	-	-	-	-	2%	1%	1%
Other	*%	-	*%	*%	-	-	-	-	-	*%	-	1%	-	-	-	-	*%	-
None of the above	3%	2%	3%	2%	4%	-	4%	3%	-	2%	3%	-	4%	1%	2%	-	2%	6%
DK/NA	1%	1%	1%	*%	1%	-	-	5%	-	1%	1%	2%	1%	-	1%	1%	1%	-

PUBLIC INTEREST ADVOCACY CENTRE: ECPA SPAM SURVEY - JAN 2010 (PN6583)

Q11S. WHICH OF THE FOLLOWING WOULD BE THE WAY YOU WOULD PREFER TO HEAR ABOUT HOW YOUR COMPLAINT ABOUT SPAM WAS HANDLED?

SUBSAMPLE: THOSE WHO PERSONALLY RECEIVED SPAM EMAIL

		EDUCATION				COMMUNITY SIZE			
	TOTAL	LESS THAN HS	HS	COLL/ SOME UNIV.	UNIV. GRAD	OVER 1 MIL.	100K- 1 MIL.	5K- 100K	UNDER 5K
TOTAL WEIGHTED	683	30	104	273	263	295	151	184	54
UNWEIGHTED TOTAL	640	32	104	249	243	240	153	178	69
Receiving an e-mail notice when the complaint is resolved or other result	37%	41%	45%	37%	35%	38%	35%	34%	52%
Obtaining a complaint tracking number and being able to track the complaint online	35%	14%	30%	36%	37%	35%	38%	39%	15%
Receiving an e-mail acknowledgement of receipt of your complaint	22%	37%	15%	24%	22%	20%	22%	24%	31%
All of the above	1%	-	3%	1%	2%	2%	2%	-	-
Other	*%	-	-	*%	-	-	-	*%	-
None of the above	3%	4%	5%	1%	3%	4%	2%	2%	-
DK/NA	1%	4%	1%	1%	1%	1%	2%	1%	1%