

Bill C-27: *Electronic Commerce Protection Act*

CBA Submission to the House of Commons
Standing Committee on Industry, Science and
Technology

September 2009

Executive Summary

The Canadian Bankers Association (CBA), on behalf of its member banks, welcomes this opportunity to provide its comments to the House of Commons Standing Committee on Industry, Science and Technology during its consideration of Bill C-27, the proposed *Electronic Commerce Protection Act* (ECPA).

Originally, "spam" was a euphemism for unsolicited commercial e-mail. In recent years, however, criminals have used spam to deliver "spyware" that can steal personal information from its targets and to send counterfeit messages that lure individuals into divulging personal information ("phishing") that results in the theft of their identity. It is widely recognized, therefore, that these types of spam are a significant threat to individuals, businesses and the Canadian economy.

Canada is the only G8 country that does not currently have specific anti-spam laws and the banking industry agrees that legislation is required to protect consumers and businesses from these dangerous and damaging forms of spam. In the absence of Canadian legislation, the banking industry practice for sending commercial electronic messages developed in compliance with the requirements of legislation in other jurisdictions, notably the anti-spam legislation adopted in the United States, the *CAN-SPAM Act of 2003*.

For several years, the CBA has encouraged the government to introduce legislation to address the most notably malicious forms of spam and we support the overall objective of the Bill 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." We note, however, that Bill C-27 is clearly more extensive and restrictive than similar legislation in other jurisdictions, including the United States. As a result, if the Bill is enacted in its current form, foreign companies operating outside Canada may have a competitive advantage in doing business with Canadian consumers and businesses. In addition, the marked difference in the approach to commercial electronic messages between Canada and other countries will require Canadian businesses to follow separate Canadian and International laws as recipients of messages may be located outside Canada.

We are concerned with the broad range of the Bill and the strict nature of its language. The banking industry has always been very supportive of legislation to address malicious spam and protect Canadians from criminal activity. We believe, however, that Bill C-27 contains some provisions that are unnecessary to achieve these goals and other provisions which require drafting changes to ensure they are workable in the electronic commerce environment. The wording of these sections should be revised. In particular, we are concerned that some provisions in Bill C-27 may have a severe negative impact upon electronic commerce and we believe a number of changes should be made to the Bill before it is enacted to ensure that it does not harm legitimate communication between businesses and prospective customers.

Canada needs to stay competitive globally and, therefore, we believe Bill C-27 needs to be amended to ensure that it does not leave Canadian business at a competitive disadvantage. Our primary comments on the Bill are provided below, along with some proposed changes. In addition, in an Appendix we have briefly discussed some other specific sections of the Bill and requested clarification or suggested amendments.

Proposed “Opt-in” Requirement and Consent Exceptions

Opt-in vs. Opt-out

We believe that the “opt-in” framework proposed by the Bill would substantially restrict or render impossible, the ability of businesses to conduct direct marketing campaigns through an electronic channel to prospective consumers who are not current clients. The future for the Canadian economy, especially the best means for businesses to increase their customer base, is through such vehicles as the internet and other on-line methods. If the “opt-in” requirement in the ECPA is implemented it will have a severe negative impact on the ability of legitimate companies to market their goods and services electronically.

In our view, rather than its proposed opt-in model, Bill C-27 should be amended to adopt an “opt-out” method of consent similar to the current Telemarketing Regulations and National Do Not Call List (DNCL). We believe that an “opt-out” approach would still afford individuals control over the use of their personal information and address the issues of malicious and unwanted “spam” mail. In addition, it will permit businesses to continue their legitimate activities and advise members of the public in an efficient and simple way of products and services that will be beneficial to them.

Express Consent

Our concerns in this regard are increased due to the need (with some limited exceptions) to obtain express consent from a “person” to send them a “commercial electronic message.” First of all, the requirement to obtain express consent in order to send a business-to-business message is questionable given that the National DNCL registration process was not extended to business telecommunications numbers. In section 6, the Bill proposes to prohibit the sending of commercial electronic messages without the recipient's prior express consent. “Electronic message” refers to messages sent as text, sound, voice and images to a recipient's email, instant messaging, or telephone account for commercial purposes. Messages sent with consent must identify the person sending the message and enable the recipient to contact the sender and unsubscribe in accordance with defined rules. Most importantly, express consent cannot be obtained by sending an e-mail or other electronic communications to a person requesting consent. It can only be obtained in some other manner through some prior contact with the recipient. In other words, a business cannot send an unsolicited electronic message seeking consent to send more messages.

Initial Contact Message

At a minimum, we recommend that Bill C-27 be amended to allow the sending of an **initial contact message** without consent, while strengthening the content requirements of the initial contact message consistent with principles of the DNCL legislation and the anti-spam legislation of other countries. This may be achieved by amending subsection 6 (2) of the ECPA by adding requirements that the initial contact message include:

- An identification of the subject matter as an advertisement or solicitation (including a clear and simple heading) in addition to the identification of the sender or an agent being used for this purpose;
- A valid physical postal address; and

- With respect to the opportunity to opt-out, present through a clear and conspicuous notice a functioning e-mail address or electronic registration process where the recipient can contact the sender to unsubscribe from receiving future e-mails

In addition, we would also suggest that subsection 6 (1) be amended by deleting paragraph (a), which requires that the recipient's consent be in place before a message can be sent and that subsection 2 (3) be deleted.

Should the recipient not wish to receive further communication, he/she could take advantage of an opt-out provision to prohibit the sending of any additional messages and, should a sender fail to respect the recipient's wishes, they could then avail themselves of the legislated remedies set out in the Bill.

In the event that Parliament decides to maintain the "opt-in" approach, we recommend that the current exceptions to obtaining express consent that are provided in sections 6 and 10 of the Bill be broadened, especially the exception that deals with implied consent if there is an "existing business relationship".

Existing Business Relationship

According to subsection 10 (3) of the Bill, consent is implied where the person sending the message, or the person causing the message to be sent, or the person who permits the message to be sent, has an "existing business relationship" with the recipient of the message. "Existing business relationship" is then defined in a variety of ways in subsection 10 (4). For example, paragraph 10 (4) (d) provides that an "existing business relationship" is one arising from

"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)"

Paragraph 10 (4) (a) purports to refer to a product or service purchased by a client from a financial institution:

"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 sent..." (our emphasis)

There is a significant difference between this definition and the 'equivalent' definition of "existing business relationship" in subsection 41.7(2) of the *Telecommunications Act*, which reads as follows:

"(c) any other written contract between the person to whom the telecommunication is made and the person or organization on whose behalf the telecommunication is made that is currently in existence or that expired within the eighteen-month period immediately preceding the date of the telecommunication."

The *Telecommunications Act* definition properly provides that if a contract is in existence, then there is an “existing business relationship”. Indeed, it then goes on to state that such a relationship is also in place if a contract expired within an eighteen-month period of the relevant communication. By way of contrast, the statement in subsection 10 (4) (d) in Bill C-27 “not referred to in any of paragraphs (a) to (c)” would appear to prevent a bank from utilizing an existing business relationship with its customer for the entire duration of the relationship, and would restrict the period during which the bank may use that relationship to the 18 months following the purchase/opening of an account with the bank by a customer.

We recommend that the term “existing business relationship” in paragraph 10 (4) (d) of the Bill be consistent with the *Telecommunications Act* exemption and, therefore, it should be clear that if there is a current written or electronic contract in place, that contract does not have to have been entered into within 18 months of the electronic communication. With a view to eliminating any uncertainty in this area and in order to provide that Bill C-27 recognizes that an “existing business relationship” is in place if a contract is in existence, we suggest that the words “not referred to in any of paragraphs (a) to (c)” in paragraph 10 (4) (d) be deleted. In addition, we recommend that the Bill be amended to extend the “existing business relationship” exception to affiliates of a company with which a person has a business relationship.

Honouring Unsubscribe Requests

Finally, with respect to the proposed 10-day timeframe for an “unsubscribe mechanism” set out in subsection 11 (3), we note that the CRTC *Unsolicited Telecommunications Rules* provide for a 31-day timeframe to respect a Do Not Call request has been received given the various channels through which such a request can potentially be received. We recommend, therefore, that subsection 11 (3) be amended to allow 31 days to respect an unsubscribe request.

Definition and Installation of “Computer Program”

We would welcome clarification on the scope of the definition of a ‘computer program’ and confirmation that it does not include online data collection tools such as cookies and web beacons.

Subsection 8 (1) of the Bill states that:

“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.”

In other words, express consent is always required to install a “computer program” on every separate occasion, even where there is an existing business relationship. Where express consent is sought to install a computer program, information must be provided to describe clearly and simply the function, purpose and impact of every computer program that is to be installed.

Subsection 2 (1) of the Bill states that “computer program” has the same meaning as in subsection 342.1 (2) of the Criminal Code, which reads as follows:

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function."

The definition of "computer program" in the Criminal Code is extremely broad and it may not be appropriate to simply apply it in the proposed ECPA. For example, in its current form, “cookies” and “web beacons” may be considered computer programs under the ECPA and subject to the restrictions set out in section 8. Consequently, express consent would be required every time these tools could be used.

Many businesses use these tools for reasons that are beneficial to their customers. For example, cookies are needed to enable customers to authenticate themselves and, therefore, are a common security feature that protects the customer and is essential for a secure online site to operate. In addition, cookies are used to enhance customer experience by allowing the recognition of past visitors when they return to a site and display to those customers personalized web pages, taking into account his or her preferred language, professional association or other non-sensitive information. Finally, cookies gather anonymous data for statistical purposes and allow a business to monitor user behaviour on their web sites to determine what pages are being viewed and subsequent changes to satisfy user preferences.

We are concerned that “cookies” may be caught by the definition of “computer program” set out in the Bill as a cookie may be said to represent a “statement” (i.e. a number uniquely assigned to a specific browser program on a specific computer) which causes a function to be performed on another system. Given its importance, we would welcome clarification on this matter and confirmation that such tools as cookies and web beacons are not covered by section 8.

Administrative Monetary Penalties and Private Right of Action

An important component of the proposed ECPA is the enforcement regime whereby the Canadian Radio-television and Telecommunications Commission (CRTC), the Competition Bureau and the Office of the Privacy Commissioner (OPC) are given the authority to share information and evidence with their counterparts who enforce similar laws internationally, in order to pursue violators that reside outside Canada. In addition, the ECPA will be administered and enforced by CRTC using its authority to conduct investigations, impose administrative monetary penalties (AMPs) and prosecute offences. The Competition Bureau will use a similar AMP regime (already provided for in the *Competition Act*), and the OPC would use its existing tools and enforcement framework to enforce the provisions of this legislation.

While we accept that there is a need for an enforcement regime, including penalties for persons who breach the ECPA, we believe some aspects of the regime and, especially, the penalties proposed in the Bill are excessive and would discourage businesses from engaging in legitimate marketing activities, thereby stifling the development of legitimate electronic marketing and adversely affecting the ability of businesses to reach their consumers. In particular, we have the following comments:

- Warrants (Section 19 (3)) – The powers given in this section seem excessively broad given the stated purpose of the provision which is simply to determine whether or not a violation has occurred. Prohibiting or limiting access to a part of a business location (as is permitted in paragraph (a)) could have significant negative impact on a business.
- Penalties (Section 20) – In our view the proposed penalties are excessive and would discourage legitimate businesses from engaging in electronic marketing.
- Notice of Violation (Section 22 (c)) – We recommend that the section be amended to allow at least 30 days after the notice is issued for payment of the penalty in order to give the alleged violator the ability to make representation to the CRTC. Payment should not be required until all avenues of appeal have been exhausted.
- Determination of Responsibility (Section 24 (2)) – Deemed violation is not necessary. If the person has paid the penalty (whether or not they feel there has been a violation), what is the point of being deemed in violation of the legislation?
- Representations (Section 25) – There is no indication how long a period the CRTC has to make its determination.
- Debts due to Her Majesty (Section 28 (c)) – There should be a “grace period” to pay any penalty if it’s gone through the appeal process, before interest begins. Depending on the amount of the penalty (which could be substantial) being required to pay on the day the decision is issued could be very difficult from an accounting perspective.
- Information may be made public (Section 39 (b)) – This paragraph relates to Section 24 (2) (Deemed Violation). We do not think it is necessary to publish the name of someone who has voluntarily paid a penalty and, in addition, any publication should be delayed until all avenues of appeal have been exhausted.

In subsection 20 (2) of the Bill, it states that the purpose of these substantial AMPs is to encourage co-operation and compliance with the legislation and not to punish. If that is the primary objective of the AMP provisions in Bill C-27, we recommend that the CRTC be given the ability to suspend an AMP for a period of time and, if the person subject to the AMP satisfies the CRTC that they have made changes to comply fully with the law, then the AMP is withdrawn.

The Bill also includes a private right of action that allows for statutory damages without proof of loss. We believe the appropriate enforcement regime is government based. We do not support a private right of action as we believe these actions are motivated more by private monetary considerations rather than general deterrence. This is particularly true where statutory damages may be claimed without any proof of loss. While the Bill provides for various factors to be considered in assessing damages under a private right of action, legitimate businesses are still put to the significant cost and task of defending themselves in this context. In particular, a private right of action will encourage class actions that will lead to substantive legal costs and reputation risk for businesses. We believe a private right of action will have a chilling effect on businesses who wish to engage in legitimate marketing activities.

Impact of Bill C-27 on National DNCL

Section 86 of the Bill, if proclaimed into force, would repeal sections 41.2 to 41.7 of the *Telecommunications Act* that authorize the establishment of the National DNCL. Bill C-27 also appears to state that unsolicited telephone calls are captured by the prohibitions within the Bill.

We understand from government officials that the provisions in the Bill that modify the National DNCL framework were included only to allow for future flexibility should the government decide to have the rules in the proposed ECPA replace the National DNCL. Provisions in the Bill that relate to telemarketing would not be brought into force at the same time as other anti-spam measures, and would potentially not be brought into force at all.

In our view, before any decision is made to eliminate the current National DNCL framework, extensive consumer research should be conducted to determine the success of the program. Furthermore, if, in the future, the government wants to substantially revise the DNCL regime there should be a full consultation process and any required amendment or new legislation should be passed by Parliament. Businesses have spent large amounts of time, resources and money in implementing the National DNCL and the new telemarketing rules. Similar National DNCL have operated in other countries very well. If there are issues with the administration or enforcement of the current regime those issues should be looked at directly and not dealt with in this Bill.

Amendments to PIPEDA

Several consequential amendments would be made to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by sections 78-83 of the Bill in order to complement the changes proposed in the ECPA, to implement measures that were considered during Parliament's review of PIPEDA in 2007, or to support the Office of the Privacy Commissioner's new approach to investigations. These amendments include the following:

- Adding provisions to section 12 of PIPEDA to permit the Privacy Commissioner to review the merits of each complaint and whether 'grievance procedures otherwise available' are exhausted.
- Giving the Privacy Commissioner broad discretion to discontinue an investigation (e.g. where there is insufficient evidence, the person has provided a fair and reasonable response to the complaint, or the matter has already been the subject of a Commissioner's report).
- Enabling the Privacy Commissioner to disclose information that is relevant to an investigation to any person under the legislation of a foreign state, provided a written agreement has been entered into.

We support the proposed changes to PIPEDA.

Appendix

Comments on Specific Provisions in Bill C-27

- Subsection 2(4) seems to be missing a verb. As a result, the true purpose of the provision is unclear though it appears it is intended that the electronic message described in this section is NOT to be considered a commercial electronic message. In the French version of the provision this intention is made clear through its opening words “N’est pas considéré un message électronique commercial...” and we recommend that the English version be revised to also make the intention of the provision clear.
- Subsection 17(6) provides that documents produced by a person in response to a Notice to Produce under subsection 17 (1) do not have to be returned. In comparison, subsection 12 (4) of PIPEDA requires the Privacy Commissioner, within ten days of receiving a request, to return any items produced by a person pursuant to section 12 of PIPEDA. The Privacy Commissioner may request the same information from the person at a later date. We believe, therefore, that the Bill should be amended so that the person who produced the documents is able to request their return and/or destruction.
- We are also concerned that documents produced and then kept by a government agency may be accessed by way of an access to information request under the *Access to Information Act*. Under section 38 of the *Telecommunications Act*, the CRTC may make available for public inspection any information submitted to it in the course of proceedings, but that is subject to a claim of confidentiality made under section 39 of the *Telecommunications Act* by the person who originally provided the information. We recommend, therefore, that the Bill be amended to specifically protect the information from disclosure by the CRTC in response to an access to information request.
- Under subsection 18(1) a person has a right to apply to the CRTC for a review of a notice to produce a document on the grounds that the requirement is “unreasonable in the circumstances” or “would disclose privileged information”. Under subsection 18(2), the person does not have to prepare or produce the document if they apply for a review on the grounds that the requirement is “unreasonable in the circumstances” but, it appears, that the document must be produced if privilege is claimed. We recommend that the provision be amended so that a person does not have to produce the document when privilege is being claimed.
- Under section 42 of the Bill anyone who contravenes subsection 19(4) [which requires “reasonable assistance to a “designated person”] commits an offence and under subsection 19 (5) a warrant may be executed between 6 a.m. and 9 p.m. This means a warrant may be served outside core office hours of a company and, for example, an employee in a remote bank branch location may not have the assistance of their law or compliance group in the event they are served with a warrant outside core office hours. This raises the risk, though it may be small, an unknowledgeable employee unwittingly committing an offence under section 19 (4).
- Under subsection 20 (3) any previous “contravention” of section 5 of PIPEDA will be a factor in determining the amount of the AMP under the ECPA. This provision raises a number of questions. For example, what is the test for deciding that a person has contravened section 5 of PIPEDA? Does a “contravention” mean when a complaint is investigated by the OPC and the complaint is deemed “well-founded” and reported as such? We also wish to note that decisions by the OPC are published in an

anonymous format, yet the AMP under the ECPA may be made public (we have the same concerns with the similar language used in the proposed subsection 58 (3) of the ECPA).

- In addition, paragraph 20 (3) (c) of the Bill refers to “subsection 7.1 (2) or (3)” of PIPEDA and we wish to confirm that the intention is to refer to these new provisions of PIPEDA that will be created as part of the amendments to PIPEDA set out in clause 78 of the Bill and not to the current subsections 7 (1) and 7 (2) of PIPEDA.
- Under subsection 23(1) the CRTC has three years after the subject matter becomes known to the CRTC to commence a proceeding, but there does not appear to be a time limit on how long a person has following the actual event to file a complaint with the CRTC. As a result, there is no firm limitation on commencing a proceeding. We recommend that the Bill be amended to specify a time limit on the period a person has to make a complaint to the CRTC.
- Under subsection 51(2) “ability to pay” is a factor in determining the amount of an AMP. We believe that the amount of any AMP should be determined solely by the actual violation and that the size of an organization and its financial resources should be irrelevant. We recommend, therefore, that this reference to “ability to pay” be deleted.
- Paragraphs 56 (a) (ii) and (iv) refer to certain sections of the *Competition Act* and the *Telecommunications Act*. It appears from the wording of these paragraphs that an organization on its own initiative may disclose any contraventions of PIPEDA, the *Competition Act* or *Telecommunications Act* to any of the CRTC, Privacy Commissioner or Competition Commissioner and not just to the regulatory agency with responsibility for a specific act. We suggest that the paragraphs be amended to make this intention clear.
- Section 60 (1) refers to “the person responsible for disclosing the information”. It is unclear to us whether this is intended to refer to any of the listed Commissioners, or to a Minister of the Crown. We recommend that this provision be amended to make the intention clearer.
- We are also concerned that the wording of section 60 may allow a foreign government to require the Canadian government to make disclosure of personal information to such foreign authority, even though the section is written from the point of view of Canada. We believe that the section should be amended to make it clear that it can only be used by the Canadian government and/or the Commissioners listed in the section.