Legislative Summary **LS-645E**

BILL C-27: ELECTRONIC COMMERCE PROTECTION ACT

Alysia Davies
Legal and Legislative Affairs Division

27 May 2009
Revised 13 November 2009
(unedited)

Library of Parliament

Bibliothèque du Parlement

Parliamentary Information and Research Service

LEGISLATIVE HISTORY OF BILL C-27

HOUSE OF COMMONS	
Bill Stage	**Date**
First Reading:	24 April 2009
Second Reading:	8 May 2009
Committee Report:	28 October 2009
Report Stage:	2 November 2009
Third Reading:	30 November 2009

SENATE	
Bill Stage	**Date**
First Reading:	1 December 2009
Second Reading:	15 December 2009
Committee Report:	
Report Stage:	
Third Reading:	

Royal Assent:

Statutes of Canada

This bill did not become law before the 2nd Session of the 40th Parliament ended on 30 December 2009.

N.B. Any substantive changes in this Legislative Summary that have been made since the preceding issue are indicated in **bold print.**

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CONTENTS

Page

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

BILL C-27: ELECTRONIC COMMERCE PROTECTION ACT*

BACKGROUND

On 24 April 2009, the Honourable Tony Clement, Minister of Industry, introduced Bill C-27, An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, in the House of Commons. This bill may be cited as the Electronic Commerce Protection Act (ECPA). It passed second reading on 8 May 2009, and was referred to the Standing Committee on Industry, Science and Technology ("the Committee") on the same date. **Several amendments were made during the clause-by-clause study of the bill by the Committee, most of them having been proposed by the government following the testimony of various stakeholders before the Committee.**

In addition to creating the new ECPA, this bill amends four existing Acts that deal with telecommunications regulation, competition and privacy. Among other changes, these amendments designate the Canadian Radio-television and Telecommunications Commission (CRTC) as the main regulator for the ECPA, although both the Commissioner of Competition and the Privacy Commissioner will also play enforcement roles related to their respective mandates.

The ECPA is a culmination of a process that began with the Anti-Spam Action Plan for Canada launched by the Government of Canada in 2004, which established a private-sector task force chaired by Industry Canada to examine the issue of unsolicited commercial email, or "spam." By the end of 2004, spam, which is in many ways the electronic equivalent of junk mail, had grown to encompass 80% of all global email traffic.(1)

---

* Notice: For clarity of exposition, the legislative proposals set out in the bill described in this Legislative Summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the House of Commons and Senate, and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent, and come into force.

(1) Task Force on Spam, *Stopping Spam: Creating a Stronger, Safer Internet*, Industry Canada, May 2005, pp. 1 and 7.

The Task Force on Spam, which led the action plan, held a round table of national stakeholders in December 2004, and solicited feedback from other stakeholders and Canadians through announcements in the *Canada Gazette* and in a dedicated online forum set up for this purpose.(2) The task force issued a report in May 2005 examining the spam situation in Canada, and recommended, among other measures, that legislation specifically aimed at combatting spam be created.

The ECPA is the resulting legislation. The federal government issued a news release to accompany the bill which thanked the Task Force, as well as Senators Donald Oliver and Yoine Goldstein "for their efforts to help address this issue."(3) Both senators have introduced bills concerning spam in the Senate during the past few years, and Senator Goldstein is the sponsor of a senator's public bill, Bill S-220, An Act respecting commercial electronic messages, which, at the time of writing of this legislative summary, is before the Standing Senate Committee on Transport and Communications. That bill, which contains an earlier proposal for anti-spam legislation, had also been introduced in the previous two sessions of Parliament, but died on the *Order Paper*.

The ECPA is a more extensive and complex bill than previous proposals, and will involve several agencies in the regulation of spam, including the Competition Bureau, the Office of the Privacy Commissioner, and the CRTC. In addition to setting up a regulatory scheme to deal with spam in Canada, it gives these agencies the power to share information and evidence with international counterparts in order to deal with spam coming from outside the country. The government indicates in its backgrounder on the proposed legislation that the ECPA is intended to "deter the most dangerous and damaging forms of spam from occurring in Canada and to help to drive spammers out of Canada."(4)

The ECPA can be seen as a complement to the e-commerce legislation that has gradually been developing in each of the Canadian provinces and territories over the past 10 years. E-commerce legislation has been enacted by every Canadian provincial and territorial jurisdiction except for the Northwest Territories, largely based on the model *Uniform Electronic Commerce Act* originally created by the Uniform Law Conference of Canada in 1998.(5) These provincial and territorial Acts have thus far served as the underpinning for a burgeoning

---

(2) Ibid., p. 9.

(3) Industry Canada, "Government of Canada Protects Canadians with the *Electronic Commerce Protection Act*," News release, Ottawa, 24 April 2009, http://www.ic.gc.ca/eic/site/ic1.nsf/eng/04595.html.

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

(5) Uniform Law Conference of Canada, *Uniform Electronic Commerce Act*, http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1.

e-commerce sector across the country.(6) The ECPA will expand the federal government's participation in this area considerably. Up to now, the main federal legislation related to e-commerce has been PIPEDA, which governs basic privacy requirements for private sector organizations and electronic documents within federal jurisdiction and in provinces or territories that have not yet established their own similar legislation.(7)

Canada is the last of the G8 countries to introduce specific anti-spam legislation. There are some existing *Criminal Code* provisions that were identified by the task force as being of possible assistance in prosecuting spam cases, and the task force worked with the Department of Justice and the Technological Crime Branch of the Royal Canadian Mounted Police during 2004–2005 to identify the evidentiary requirements to bring a charge under the existing provisions, although when the task force report was published, these provisions had not been used for this purpose. Other agencies, such as the Office of the Privacy Commissioner of Canada and the Competition Bureau, have received complaints from members of the public about spam as well, but there has been no overarching framework for addressing such complaints.(8)

The ECPA will provide a clear regulatory scheme, including administrative monetary penalties, with respect to both spam and related threats from unsolicited electronic contact, including identity theft,(9) phishing,(10) spyware,(11) viruses,(12) and botnets.(13) It will also grant an additional right of civil action to businesses and consumers targeted by the perpetrators of such activities.

---

(6) For more information on the provincial and territorial e-commerce regimes, see Alysia Davies, *The Development of Laws on Electronic Documents and E-Commerce Transactions*, PRB 00-12E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, revised 20 December 2008.

(7) "*Personal Information Protection and Electronic Documents Act*: Process for the Determination of 'Substantially Similar' Provincial Legislation by the Governor in Council," *Canada Gazette*, Vol. 136, No. 31, 3 August 2002, http://www.gazette.gc.ca/archives/p1/2002/2002-08-03/html/notice-avis-eng.html#i10.

(8) Task Force on Spam (2005), pp. 11–13.

(9) Identity theft is the collection and use of stolen personal information to impersonate someone, generally for financial fraud purposes.

(10) Phishing is the impersonation of a trusted person or organization in order to steal a person's personal information, usually for the purposes of identity theft.

(11) Spyware is software that collects information about a user, or modifies the operation of the user's computer, without the user's knowledge or consent.

(12) A virus is hostile software (or "malware") that spreads by attaching itself to another resource on a computer such as e-mail.

(13) A botnet is a collection of "zombie" computers used to send spam or for another purpose. A "zombie" is a computer that runs malware so that the computer can be remotely controlled by the creator, distributor or controller of the malware.

DESCRIPTION AND ANALYSIS

A. Definitions (Clause 2)

The ECPA contains several important definitions which are updated or more detailed versions of definitions that appear in other Acts or contexts. It also contains some new definitions, particularly for technological concepts that have not appeared in federal legislation before.

The ECPA contains its own definition of "commercial activity," which is different from the one in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), although it does not modify the existing definition in that Act. The ECPA builds on the PIPEDA wording of "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character," adding a qualification: "whether or not the person who carries it out does so in the expectation of profit." This addition to the definition could be linked to some of the third party liability clauses in the ECPA, reflecting an intention to widen the scope of who could be considered responsible under the new law in cases where spamming or other activity occurs, possibly implicating Internet service providers (ISPs) or even those whose computers are being used for spamming without their awareness or consent.

The definition of "commercial activity" also contains a new exemption – it explicitly does not include any transaction, act or conduct carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada.

The ECPA contains a new definition of "electronic address," and it is a broad one, covering email, instant messaging (IM), text messages on phones, and messages on "any similar account," which could include messages sent over Facebook, Twitter, and many other more recent applications. It also contains a new and broad definition of "electronic message," which includes a message sent over any means of telecommunication, including text, sound, voice or image, and therefore implicates voice mail messages, webcam messages, and the exchange of pictures or graphic files by electronic means as well. This definition extends coverage of the ECPA to most means of electronic communication, with the exception of broadcasting, which is explicitly exempted from the ECPA in clause 5.

There are also provisions at the end of the ECPA, discussed in further detail later in this summary, which would **give the government the power to** repeal legislation for the relatively new Do Not Call List (DNCL) for telemarketers. Since it was introduced in 2008, the DNCL has been subject to much criticism owing to telemarketer misuse of the names on the list.(14) The breadth of the definition of "electronic message" in the ECPA means that the definition could apply to unsolicited voice mail messages left by telemarketers, and subject them to the "opt in" approach of the new legislation whereby they must obtain permission before contacting people, overriding the existing regime.

The ECPA goes on to provide a distinct definition for "commercial electronic message," based on the type of content contained in it. The definition specifies that the nature of the message can be inferred not only from the content, but also from any links contained in the message or the contact information of its sender. Categories of activity related to purchase, sale, barter or lease of products, services, land or an interest or right in land are included, as well as offers to provide a business, investment or gaming opportunity, and the promotion of any of these activities, or of a particular person engaged in such activities and their public image.

The definitions of "telecommunications service" and "telecommunications service provider" in the ECPA are broader than those in the *Telecommunications Act*, although it does not appear that they would replace the existing definitions except when referring to spam. The ECPA definition of "telecommunications service" extends to any service or feature of a service provided by means of telecom facilities, whether the provider "owns, leases or has any other interest in or right respecting the telecommunications facilities and any related equipment used to provide the service." The definition of a service provider covers those who provide such services either "independently or as part of a group or association."

The ECPA contains a definition of "transmission data," which is new and very detailed, seeking to cover any data relating to "the telecommunications functions of dialling, routing, addressing or signalling" – including by phone, Internet, and wireless – involved in all functions of transmitting data electronically outside of the actual substance of the message. The intent appears to be to capture all steps along the chain of transmission where a spammer or other malevolent communicator could insert some form of problematic technology such as malware or spyware, or fake an identity for the purposes of communication (such as pretending to be from a bank or other reputable institution that the recipient would trust).

(14) See, for example, Michael Geist, "Why the ECPA Lays the Groundwork To Kill The Do-Not-Call List," *Michael Geist's Blog*, 27 April 2009, http://www.michaelgeist.ca/content/view/3894/125/.

B. Purpose (Clause 3) and Related Clauses (Clauses 4–5)

The ECPA identifies its purpose as promoting the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of e-commerce by (i) impairing the availability, reliability, efficiency and optimal use of e-commerce, (ii) imposing additional costs on businesses and consumers, (iii) compromising the privacy and security of confidential information and (iv) undermining the confidence of Canadians in using e-commerce for commercial activities at home and abroad (clause 3).

The ECPA establishes itself as binding on any corporation, whether it is provincially or federally incorporated (clause 4), but it does not, as previously indicated, apply to broadcasters (clause 5).

C. Key Provisions (Clauses 6–9 and 12)

The key violations which are at the heart of the ECPA are laid out in clauses 6 to 9 of the bill.

Clause 6 designates spamming, the sending of unsolicited commercial electronic messages, as a violation. It forbids sending a commercial electronic message unless there is express or implied consent from the recipient.[15] Any message sent must also be in a prescribed form – it must identify the person who sent the message and the person on whose behalf it is sent, provide accurate contact information for these parties, and set out an unsubscribe mechanism as outlined in clause 11. Exceptions include messages sent between those who have a personal or family relationship, and any message sent to someone engaged in a commercial activity that is solely an inquiry or application relating to that activity (clause 6(5)). Clause 6(6) exempts the service provider from liability in relation to spamming.

In addition, some new exemptions were added to the bill during its passage through the House of Commons, following testimony by various stakeholders before the Committee. The amendments create a new clause 6(5.1), which specifies that the prohibitions on sending a commercial electronic message do not apply to quotes or estimates for the supply of a product, goods, a service, land or an interest or right in land if

---

(15) For the purposes of the bill, the recipient of an electronic message is considered to be the holder of the account associated with an electronic address to which something is sent, as well as any person who it is reasonable to believe is or might be authorized by the account holder to use that address (clause 2(5)).

the message was requested by the recipient. They also do not apply to a message that facilitates, completes or confirms a commercial transaction that has already been agreed to by the recipient, or that provides warranty, product recall, safety or security information about a product, good or service that the recipient has used or purchased. Further exemptions have been added for certain types of ongoing messages such as those that provide notification of factual information; that provide information directly related to an employment relationship or benefit plan; or that deliver a product, good or service that the recipient is entitled to receive under the terms of a previous transaction. Further exemptions may be specified in the regulations.

These consent restrictions would also be used to deal with "phishing." A common phishing operation is one in which an e-mail is sent from what appears to be an organization the recipient knows, such as a bank, requiring the recipient to send back personal information or confirm the information via a link. The actual sender is not the bank but an impersonator who uses this means to steal the recipient's personal information, which the recipient would not otherwise give out.(16)

Clause 6(7) is noteworthy, since it exempts two-way voice communication between individuals (i.e., phone calls, faxes, and voice mail messages), which would normally mean that telemarketing activities covered by the DNCL are exempted from the ECPA. However, later in the ECPA, clause 64 provides for the repeal of this exemption provision, which indicates that while telemarketing activities covered by the DNCL may be exempt from the ECPA in the early stages of the Act's implementation, the government may eliminate that exemption at a later date. This would mean that all the requirements included in clause 6 of the ECPA would eventually become applicable to telemarketing activities as well, including a much more stringent consent standard than is currently applied under the DNCL. (See the section on "Consent," below.) The ECPA also contains language to directly repeal the DNCL in its current form (sections 41.1 to 41.7 of the *Telecommunications Act*), which could be activated at a time of the government's choosing (clause 86). **In their testimony before the Committee, Industry Canada officials indicated that technological convergence may make the DNCL obsolete at a point in the near future, since many voice calls will be made using Voice Over Internet Protocol (VOIP), which will essentially transform them into electronic messages. The**

(16) Task Force on Spam (2005), p. 58.

officials also testified that the DNCL is also currently dependent on a private provider for its administration, which may withdraw as the technologies increasingly converge. The officials indicated that the clauses in Bill C-27 concerning the DNCL are intended to give the government the flexibility to respond to this situation if and as it arises.[(17)]

Clause 7 addresses certain types of hacking operations, such as a "man in the middle attack," where an electronic communication between two parties is intercepted and redirected without either party's knowledge. Under this clause, no one is permitted to alter the transmission data for a message or cause it to be altered so that the message is sent or copied anywhere other than where the sender thinks it is going. All alterations to the transmission data require the express consent of the sender (which would include any recipient sending a reply to an electronic message). Clause 7(2) exempts service providers from this requirement, since they sometimes need to alter transmission data for technical reasons as part of the normal course of directing electronic messages through the service network.

Under clause 8, no one can, in the course of a commercial activity, install or cause to be installed a computer program on any other person's computer system, nor may anyone use any installed program to cause an electronic message to be sent from another person's computer, without the owner's express consent. This provision is aimed particularly at the surreptitious installation of spyware and malware, such as the kind that turns computers into "botnets" used to relay spam without their owners' permission.

Clause 9 designates the causing or procurement of any of the activities in clauses 6 to 8 to be a violation as well.

Activities under **clause 6** are violations only if a computer system located in Canada is used to send or access[(18)] the electronic message in question, **and in the case of clause 7, only if a computer system located in Canada is used to send, route or access the electronic message**. **This type of restriction** does not apply to clause 8 **(clause 12)**.

---

(17) Testimony of André Leduc and Philip Palmer, Industry Canada, to the House of Commons Standing Committee on Industry, Science and Technology, 26 October 2009, http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4171785&Language=E&Mode=1&Parl=40&Ses=2 at 16:45–17:10.

(18) The word "route" was removed with respect to violations under clause 6 by a Committee stage amendment.

D. Consent (Clauses 10–11 and 13)

Clause 10 defines express consent and implied consent for the purposes of the ECPA. Express consent is what is known as "opt in" consent – commercial communication may not take place unless the person or corporation in question first consents to be contacted. Implied consent is what is known as "opt out" consent – commercial communication may take place with persons or corporations under circumstances where it can be deemed that they might be interested, but the recipients of the communication must be able to "opt out" of such communication. In the case of the ECPA, implied consent can be assumed in cases where there is an "existing business relationship" or an "existing non-business relationship" between the sender and recipient – clauses 10(4) and 10(6) provide a detailed definition of what constitutes each type of relationship. In the absence of either of these relationships, express consent must be sought for sending any unsolicited commercial electronic messages.

Where express consent is sought, the party seeking it is required under clause 10 to set out "clearly and simply" the purpose(s) for which the consent is being sought, the prescribed information identifying the party seeking consent, and any other information that may be prescribed by the regulations.

Amendments added to the bill at the Committee stage in the House of Commons provide some extra instructions to those seeking consent on behalf of someone whose identity is not known. Under the new clause 10(1.1), the only information that is required to be provided is the prescribed information identifying the person seeking consent. Other conditions that govern this kind of consent relationship will be detailed in the regulations.

Another amendment replaces the provision originally laid out in clause 10(2) requiring that every installation of a computer program on a recipient's computer be accompanied by a description of the function, purpose and impact of that program. 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)).

The definition of "implied consent" in clause 10(3) of the bill, as expanded by Committee stage amendments, now includes a "conspicuous publication" exception, a concept borrowed from Australia and New Zealand. Under this exception, if a recipient has conspicuously published their e-mail contact information, for instance on a business web site, and has not posted with it a disclaimer that it is not to be used for unsolicited electronic commercial messages, then it may be used to contact them on matters relevant to their business or official capacity (clause 10(3)(*b*)). This exception also applies if the recipient has provided their e-mail contact information to the sender without indicating they do not wish to receive unsolicited commercial messages, and the message is related to their business or official capacity (clause 10(3)(*c*)). Further exceptions may be specified in the regulations (clause 10(3)(*d*)).

Those who can assume implied consent because of a business relationship must meet the one of the following criteria (clause 10(4)):

- They sold, leased or bartered a product, goods, services, land or an interest or right in land to the message's recipient within the **2 years** before the message was sent.
- They provided a business, investment or gaming opportunity that was accepted by the recipient within the preceding **2 years**.
- They entered into a written contract, which is still active or which expired within the preceding **2 years**, with the recipient for any reason.
- They received any kind of inquiry from the recipient within the previous 6 months.

Any purchaser of a business is considered to have inherited its existing business relationships for the purposes of the bill (clause 10(5.1)).

Businesses that may take advantage of this kind of relationship include cooperatives as defined in the *Canada Cooperatives Act*, cooperative corporations as defined in the *Cooperative Credit Associations Act*, and any similar organization that is federally or provincially incorporated (clause 10(5)).

Those who can assume implied consent because of a non-business relationship must meet one of the following criteria (clause 10(6)):

- The recipient made a donation or gift to them or their organization in the **2 years** before the message was sent, and they are a registered charity, or a political party, organization or candidate.

- The recipient performed volunteer work for them or their organization or attended a meeting organized by them within the preceding **2 years**, and they are a registered charity, or a political party, organization or candidate.

- The recipient has been a member of their organization during the **2 years** before the message was sent, and they are a club, association or voluntary organization, as defined in the regulations.

Where the existing business or non-business relationship is connected to a membership or an ongoing use or purchase under a subscription, account, loan or similar relationship, the 2-year period is considered to start on the day of its termination (clause 10(7)).

Even where consent of some kind for receiving an unsolicited commercial electronic message is given, the recipient must be able to "opt out" by unsubscribing from the communication. Clause 11 lays out the technical requirements for the mechanism to unsubscribe. It must allow the recipient to indicate, **at no cost to him or her**, using **either** the same electronic means by which he or she received the message **or any other electronic means that are practicable**, the wish not to receive any further messages, and it must specify an electronic address or provide a link **to a World Wide Web page** by which this indication can be given. The address or link must be valid and work for a period of 60 days following the sending of the original message in which it is contained (clause 11(2)). Any unsubscribe notification received by the sender must be put into effect within 10 **business** days (clause 11(3)).

For cases where there is express consent to alter transmission data under clause 7, an unsubscribe mechanism must be provided to the recipient of the electronic message throughout the period covered by the consent, and any activation of the unsubscribe option must be put into effect within 10 **business** days (clause 11(4)).

For cases where there is express consent to download a program onto a person's computer under clause 8 (botnets/spyware/malware), a mechanism whereby the recipient can send a request to remove or disable the computer program because its function, purpose or **other details required under clause 10(2.2) were** not as advertised in the original consent request, has to be provided for a year after the program's installation (clause 11(5)). The providers of the program have to grant a request to uninstall, without cost, if the request is made because of misrepresentation of the program in the original request for consent (clause 11(5)(*b*)).

Anyone who alleges to have either express or implied consent for activities under clauses 6 to 8 has the burden of proving it in court and/or before the regulator (clause 13).

E. Violations and Penalties (Clauses 14–46)

The ECPA designates the CRTC as the main regulatory agency responsible for pursuing administrative penalties against those who violate the Act (clause 14). The CRTC is given numerous powers in relation to this mandate, including the right to cause a demand to be served on a telecommunications provider to verify compliance with the ECPA, and to prevent disclosure of that demand for the purposes of protecting an investigation (clause 15).[19] The telecommunications provider, which is required to preserve data for the purposes of complying with the demand, is entitled to apply for a review if either the preservation of data or non-disclosure would place an undue burden upon it (clause 16).

The CRTC also has the power to require that a person produce a document in his or her possession or control, or to require preparation of a document based on data, information or documents in the possession or control of that person (clause 17). Again, anyone subject to such a requirement has the right to apply for review on the grounds of unreasonableness or the possibility of disclosing privileged information, or to seek conditions on the disclosure (clause 18). The CRTC may also apply to a justice of the peace for a warrant to enter a place of business pursuant to the ECPA, and unless the warrant contains different conditions, may then examine anything found there, use any means of communication found there, and examine or use any

(19) As a result of committee-stage amendments, an investigation includes one that is undertaken by a foreign government, not just a Canadian one, as long as it concerns conduct substantially similar to that regulated under this bill. (See new clauses 15(3)(*c*), 15(4)(*b*), 17(2)(*c*), 17(4)(*b*), 19(1)(*a*)(iii) and 60(3)(*a*) of ECPA, as well as the new sections 52.02 and 74.012 of the *Competition Act* introduced by amendments to clauses 71 and 73 of the bill.)

computer systems, documents, and copying equipment found there. It may also remove, for copying or examination, anything found at the place it has entered, and it may prohibit or limit access to the place itself. The owner of the place is required to give all reasonably required assistance to the CRTC under such circumstances (clause 19).

The ECPA imposes significant monetary penalties for violations of clauses 6 to 9 of the Act, along with a list of factors to be taken into account in determining the amount levied (clause 20(3)). These factors include the purpose of the penalty, the nature and scope of the violation, any history of previous violations under the Act, any financial benefits obtained from the violation, ability to pay, whether voluntary compensation has already been paid, and any other relevant factors or factors established by the regulations.

The maximum penalty for an individual is $1,000,000 and the maximum penalty for a corporation or other organization is $10,000,000. These fines are imposed per violation, and a violation is defined as being separate for each day that it continues, so these maximum amounts can therefore be imposed for each day that the law is found to have been violated (clause 20). If a business, for example, has been spamming for 10 days, it could conceivably be required to pay up to $100,000,000 in penalties.

The ECPA also permits violations to be dealt with by way of undertakings – if the perpetrator enters into an undertaking in accordance with the Act, proceedings against the perpetrator are automatically halted. The undertakings must identify every violation committed under the ECPA, and may require payment of a given amount (clause 21).

Otherwise, when a violation is committed, a notice of violation can be issued by the CRTC (clause 22). All violations that are pursued under the ECPA **have** a limitation period **of three years from the date on which the subject matter of the proceeding became known to the relevant authority** (clause 23). The person or entity issued a notice can make representations in response, but if this does not occur, the person or entity is deemed to have committed the violation (clause 24). If representations are made, the CRTC has to make a finding of whether the violation was committed, on a balance of probabilities standard (clause 25). Once a violation has been deemed or found, the CRTC has the power to order the violating party to cease contravening the law (clause 26).

Any such finding (clause 25) or order (clause 26) by the CRTC may be the subject of an appeal to the Federal Court of Appeal, as may a decision of the CRTC with respect to preservation or production orders under clauses 16 and 18, if they concern questions of law.

However, appeals with respect to questions of fact can only be brought with leave of that court. Deemed violations (clause 24) cannot be appealed, but any orders arising from them (clause 26) can be.

All penalties or payments are payable to the Receiver General, including any "reasonable expenses" incurred in trying to pursue a payment or penalty owed under the ECPA. There is a five-year limitation period on the recovery of penalties, payments and expenses (clause 28). The CRTC may issue a certificate certifying any unpaid amount, and this can be registered in the Federal Court to give it the same effect and enforceability as a judgment of the Court for the amount owing (clause 29).

Violations of the ECPA are not criminal offences (clause 30), but they do create both direct and vicarious liability, and allow for the possibility of holding the directors and/or officers of a corporation directly responsible for the actions of that corporation, "piercing the corporate veil," as it is commonly known. Any officer, director agent or mandatary of a corporation that commits a violation is liable for it if they directed, authorized, assented to, acquiesced in or participated in the commission of the violation, regardless of whether proceedings are commenced against the corporation itself (clause 31). An employer is also liable for violations committed by an employee (or their agent or mandatary) acting within the scope of their employment, whether or not the employee is proceeded against or even identified (clause 32). There is a due diligence defence (clause 33(1)), but other common law defences can only be used to the extent that they do not conflict with other provisions of the ECPA (clause 33(2)).

In pursuing violations, the CRTC has the powers of a superior court with respect to witnesses and the production of evidence, and may make findings of fact without regard to the findings or judgement of a court (clauses 34 and 35). The CRTC may designate one member or a panel to conduct hearings, and may set its own rules of procedure (clauses 36 and 37).

In addition to the various measures providing for hearings to establish if there has been a violation of the ECPA, the names of those who are deemed violators or who have given undertakings to cease activities prohibited by the ECPA can also be made public by the CRTC, along with the amounts of any monetary penalties imposed upon them (clause 39). Demands, notices, undertakings or orders of the CRTC may be converted into court orders by filing them with any court in the appropriate jurisdiction (clause 40).

The CRTC may also apply to the courts for an injunction to stop anticipated violations of the ECPA (clause 41(1)). It must give 48 hours notice of such an application, unless the situation is so urgent that it would not be in the public interest to do so (clause 41(2)).

Anyone who fails to comply with a demand or notice issued by the CRTC, or any warrant issued by a justice of the peace under the ECPA, commits an offence (clause 42). So does anyone who obstructs, hinders or knowingly provides false or misleading information to the CRTC in connection with an ECPA proceeding of any type (clause 43). The same broad vicarious liability of employers and piercing of the corporate veil that apply to ECPA violations also apply to these offences (clauses 44 to 45). Again, a due diligence defence is available, and there does not appear to be any restriction on other common law defences in this case (clause 46). Fines of up to $10,000 (first offence) or $25,000 (subsequent offences) for individuals, or $100,000 (first offence) and $250,000 (subsequent offences) for corporations or other organizations may be applied.

It should be noted that in addition to this new regime, it appears from the proposed amendments to the *Competition Act* (see part J below) that recourse either to the courts or to the Commissioner of Competition are also available in cases of false and misleading telemarketing or electronic messages, which may violate both the *Competition Act* and the ECPA (clauses 66–77).

F. Private Right of Action (Clauses 47–55)

In addition to all of these remedies, the ECPA also creates a private right of action for individuals who have been affected by contraventions of the ECPA. A person who alleges that he or she is affected by an act or omission that breaches the key provisions of the Act (clauses 6 to 9) may apply to a court for an order of compensation. This right is also available where a person alleges that he or she has been the target of false or misleading electronic messages under the proposed amendments to the *Competition Act* (clause 73), where an electronic address has been obtained without consent through data mining or other automated crawling, or where personal information has been obtained through accessing a computer system, or causing it to be accessed, without authorization (see the proposed amendments to PIPEDA at clause 78).

The three-year limitation period applies to this right, and the court is not able to consider the order if an undertaking has already been agreed to or a notice of violation already issued under the ECPA. However, if an application for an order is filed in court first, then no undertaking may be made or notice of violation issued. In other words, one remedial scheme or the other must be chosen – the alleged violator cannot be pursued in the courts and before the CRTC at the same time (clause 48).

It appears from the wording of the ECPA that if the issue is pursued under the CRTC scheme, then it is generally called a "violation," whereas if it is pursued through some of the other avenues currently provided in the statute, it is referred to as a "contravention." In any case, both words refer to the same breaches of the ECPA, centred on clauses 6 to 9, irrespective of the choice of remedy.

If the avenue of the courts is chosen, then the CRTC, the Commissioner of Competition, and the Privacy Commissioner all have the right to be intervenors in the court proceedings, depending on the contraventions alleged (clause 50). With respect to remedies, the court may order compensation equal to the loss or damage suffered and expenses incurred, in addition to another $200 for each contravention of the ECPA up to a maximum of $1,000,000 per day (clause 51(1))**.**[(20)] If it imposes this additional **compensation payment**, on top of damages, the court must use prescribed factors to determine the amount, **including, among others, the nature and scope of the contravention, the violator's history, any previous undertakings, the financial benefit obtained from the contravention, and the ability to pay** (clause 51(2)). **Another factor to be taken into account by the courts is the purpose of any such compensation, which a new government amendment to the bill prescribes cannot be punitive. Such awards are intended to "promote compliance with the Act" (clause 51(1.1))**.

The same vicarious liability and ability to pierce the corporate veil that is applicable to violations before the CRTC can be found by the courts as well (clauses 52–53). Due diligence is again the only explicit defence, and other common law defences do not apply to the extent that they are inconsistent with the ECPA (clause 54). In addition, where more than one party is found to have contravened the ECPA, those parties are all jointly and severally liable for the damages and penalties imposed (clause 55).

G. Information Sharing (Clauses 56–**60.1**)

In addition to amending other Acts, the ECPA sets out several provisions which affect the operation of those Acts without amending them.

---

(20) As amended at Committee stage the provisions break down the applicable penalties more specifically. Units of $200 can be awarded with respect to particular violations and/or contraventions of the ECPA and the other amended statutes, although the judge is not restricted to these units for all of them. However, all types of violations/contraventions are subject to the $1,000,000 per day maximum (clause 51(1)(*b*)(i)–(vii)).

For example, PIPEDA contains a section which prohibits private sector organizations from disclosing the personal information of others without their knowledge or consent, except in exceptional circumstances, as per subsection 7(3). The ECPA would introduce a provision that operates despite subsection 7(3) of PIPEDA, allowing disclosure to the CRTC, the Commissioner of Competition or the Privacy Commissioner of this type of personal information in the event of a contravention of the key provisions of the ECPA (clauses 6–9), or of certain provisions of the *Competition Act*, the *Telecommunications Act*, and PIPEDA itself (clause 56).

The CRTC, the Commissioner of Competition, and the Privacy Commissioner are required to consult with each other to the extent that they consider appropriate to ensure that activities such as spamming are controlled under the complementary provisions in the Acts for which each of them has responsibility (clause 57). They can also share information and make certain disclosures to each other that would not normally be allowed under certain conditions relating to violations of those Acts (clause 58), although each of them can only use this information in relation to the particular statute for which he or she is responsible (clause 59).

In addition, the CRTC, the Commissioner of Competition, and the Privacy Commissioner can share information with foreign states and international organizations for the purposes of pursuing violations under their respective Acts and the ECPA. All such information-sharing arrangements must be in the form of written agreements, however (clause 60**(1)), and they may concern only illegal activity under foreign laws that does not have penal consequences (clause 60(2.1)). A written agreement can be presumed from the acceptance of a written request for assistance from a foreign state or international organization if it is accompanied by a declaration that assistance between Canada and the requesting party will be reciprocal (clause 60(4)).**

Clause 60.1 requires the CRTC, the Commissioner of Competition and the Privacy Commissioner to provide the Minister of Industry with any reports requested for the purpose of coordinating the implementation of the main violation provisions related to ECPA (sections 6 to 9), including those in the *Competition Act* (sections 52.01 and 74.011) and PIPEDA (section 7.1).

H. Miscellaneous (Clauses 61–**63.2**)

The CRTC is permitted to incur expenses and hire experts for the purpose of activities related to the ECPA (clauses 61 and 62). The CRTC may also make regulations (clause 63(2)) pertaining to:

- the form of a request for express consent;
- undertakings;
- the manner of service for documents required under the ECPA; and
- prescribing anything to be prescribed under the ECPA.

The Governor in Council may make regulations on various matters (clause 63(1)), including:[(21)]

- the circumstances in which consent is deemed to have been withdrawn **for the purposes of clause 6**;
- the definitions relating to the exceptions to the anti-spamming provisions in clause 6, such as what constitutes a "personal relationship";
- additional circumstances that constitute implied consent;
- definitions relating to the "existing non-business relationship" exemption;
- **the use that may be made of a consent and the attendant conditions**;
- **the type of computer program installations which do not require details about them to be disclosed under clauses 10(2.2), (2.3) and (2.5)**;
- determining which contraventions generate separate penalties for each day they continue;
- establishing additional criteria to be taken into account in setting the amount of a penalty;
- any general matters relating to carrying out the purposes and provisions of the ECPA.

---

(21) Committee stage amendments lengthened the list of matters that may be dealt with by the Governor in Council in the regulations (clause 63(1)).

At the Committee stage, a provision was added requiring a one-time Parliamentary review of ECPA three years after it comes into force (clause 63.1).

Transitional provisions, added at Committee stage, specify that implied consent to receipt of electronic commercial messages for the purpose of business and non-business relationships that already existed prior to the legislation will continue for three years after the date on which section 6 of ECPA comes into force. Express consent will need to have been sought during the 3-year transition period to continue them after that point. This is also true for the installation of computer program upgrades or updates (clauses 63.1 and 63.2).

I. Amendments to the *Canadian Radio-television and Telecommunications Commission Act* (Clause 65)

The only amendment to this Act is a provision incorporating the new powers of the CRTC under the ECPA by reference (clause 65).

J. Amendments to the *Competition Act* (Clauses 66–77)

There are several amendments to the *Competition Act*, which give the Competition Bureau and the Commissioner of Competition a role in investigating and enforcing the new anti-spam provisions by extending the Act's existing regime on misleading and deceptive practices to include on-line activity.

The ECPA adds several new definitions to this Act, and it amends the existing definition of "record" to give it a much broader meaning: "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." It also specifies that the definition of "information" in the Act now includes "data," and replaces the definitions for "computer system" and "data" with those in the ECPA (clauses 66 and 67).

The ECPA definition of "electronic message" is also added to this Act. Definitions for three other terms – "locator," "sender information," and "subject matter information" – are added to this Act only and are not in the ECPA (clause 66).

The ECPA modifies the provisions in the Act concerning applications to a court for injunctions. In the case of injunctions for most infractions of the Act, the grounds on which one can apply for an injunction are simplified. If someone has committed an offence under the

Act or is about to, and this would result in either injury to competition that cannot be remedied under the Act, or serious harm, an injunction can be granted, provided the balance of convenience favours it (clause 69).

For provisions relating to false and misleading electronic messages or telemarketing, the conditions to be met are the same, except potential injury to competition is no longer a factor. An injunction may also be granted in order to prevent someone from supplying a product that would facilitate the commission of an offence relating to false or misleading electronic messages or telemarketing, or in some cases to require them to actually prevent such an offence from taking place (clause 70).

The amendments specify that offences under the Act relating to false or misleading electronic messages or telemarketing are committed not only by those who make or send them, but by those who permit them to be sent (clause 70).

In addition to this, the definition of "telemarketing" is expanded to cover promotional calls by "any means of telecommunication," instead of restricting telemarketing solely to telephone communications (clause 72).

Some provisions are generally updated to include references to the broader definition of telemarketing and to the use of electronic messages in ways which violate the Act.

In particular, a new section is added to define false or misleading representations by electronic message as an offence. This offence extends not only to the content of the message, but also to its sender and its subject matter information, as well as to its locator. It is not necessary to prove that someone was misled or deceived by the message, or even that the person was the intended recipient; it suffices to prove that the message was misleading or deceptive. The penalties for this new offence are a prison term of up to 14 years or a fine at the discretion of the court for an indictment, or both, or a prison term of up to 1 year or a fine of up to $200,000 for a summary conviction, or both (clause 71).

However, proceedings cannot be brought by the Commissioner of Competition both under this new section and under the regime of review for deceptive marketing practices that exists in Part VII.1 of the Act at the same time – one or the other route must be chosen to seek a remedy (clause 71).

The provisions under Part VII.1 concerning deceptive marketing practices are also updated to permit a review under that part to be pursued where it involves an electronic message, and to apply to the wider definition of telemarketing (clauses 73 and 74). Where the

Competition Bureau finds that a breach of the Act has taken place, the penalties applied can deduct any amounts someone has already been ordered to pay under the ECPA or has agreed to pursuant to a settlement agreement under the ECPA (clause 75).

The existing powers in the Act that permit the Commissioner of Competition to apply to the court for an order similar to an injunction are updated so that they can also be used against those who supply products facilitating the commission of an offence under the Act, or who fail to prevent an offence. The requirement that the court meet the standard of a "strong *prima facie* case" before issuing this order would be replaced by a less stringent standard of "if it appears to the court" (clause 76).

K. Amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (Clauses 78–83)

There are several amendments to PIPEDA which expand the Privacy Commissioner's discretion and permit the Office of the Privacy Commissioner to take measures against the unauthorized collection of personal information through hacking or illicit trading of lists of electronic addresses.

The ECPA adds some new definitions to this Act, including "computer program," "computer system" and "electronic address" as they are defined under the ECPA. (The first two are standardized with the definitions in the *Criminal Code*.) The new definition for "access" appears in this Act alone: it is defined as meaning "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" (clause 78).

Under PIPEDA as it currently exists, there is a list of exceptional circumstances under which personal information can be collected, used and/or disclosed by a private sector organization without consent, such as in life-threatening emergencies or for debt collection. The ECPA introduces a caveat: in the case of the collection and/or use of an electronic address obtained through data mining or other automated crawling,[(22)] **most** of the PIPEDA exceptions

---

(22) In the original bill, programs related to functions such as e-mail harvesting were described as computer programs "designed or marketed for use in generating or searching for, and collecting, electronic addresses." In the subsequent amendments to the bill, this language was changed to "designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses" [emphasis added] (clause 78).

do not apply.[23] The same caveat is also applied to the collection and/or use of personal information through any means of telecommunication if it is obtained through accessing a computer system, or causing it to be accessed, without authorization (clause 78). Consent must be obtained under all circumstances where personal information is obtained using these methods, **unless the collection is related to law enforcement or investigative purposes**.

The ECPA also grants the Privacy Commissioner new discretionary powers to refuse to investigate a complaint under certain circumstances – if he or she believes that there are other grievance or review procedures available that ought to be exhausted first, if there are other laws such as provincial ones under which the complaint could be dealt with more appropriately, or if the complaint was not filed within a reasonable period following the initial issue. The Privacy Commissioner also does not have to conduct an investigation into any matter which concerns a violation of the main provisions of the ECPA (clauses 6 to 9) or the amended provisions of the *Competition Act*, although he or she would have the power to reconsider if there are "compelling reasons" (clause 79).

The Privacy Commissioner's existing powers to discontinue the investigation of a complaint on various grounds would also be expanded. In addition to stopping an investigation because of insufficient evidence, trivial, frivolous or vexatious complaints, or complaints made in bad faith, the Commissioner could also discontinue if he or she had already investigated the particular matter or if the organization had already provided a reasonable response to the complaint. Specific language allowing him or her to discontinue if it is an ECPA matter already under investigation by the CRTC is also included (clause 79). Complainants may apply to the court for a hearing with respect to a discontinuance decision if desired (clause 81).

The other investigative powers of the Privacy Commissioner remain the same, although the order in which they appear in PIPEDA would be renumbered.

Additional powers are granted to the Privacy Commissioner to coordinate with provincial and territorial privacy commissioners to develop guidelines or model instruments governing the handling of personal information by private sector organizations. The Commissioner would also be granted the power to share information about investigations with his or her counterparts, provided it is done confidentially and for the same purpose for which it was collected (clause 83).

---

(23) In the original bill, none of the PIPEDA exceptions applied, but amendments introduced at the Committee stage altered this following concerns raised by stakeholders that those related to law enforcement should continue to apply.

In addition, the Commissioner would be empowered to share information with his or her investigative counterparts in foreign states, if it would be relevant to an investigation of a contravention of similar laws or would establish an information exchange from a foreign state to assist with a domestic investigation. Powers similar to the existing ones to develop research, guidelines and knowledge-sharing with provincial and territorial counterparts would also be expanded to extend to foreign counterparts (clause 83).

L. Amendments to the *Telecommunications Act* (Clauses 84–86)

The Act currently prohibits the CRTC from disclosing any confidential information submitted to it during the course of proceedings. The ECPA would create an exception, allowing such information to be disclosed to others when the CRTC is applying its powers in respect of clauses 6 to 9 of the ECPA. This would include confidential financial, commercial or scientific information, trade secrets, and similar types of materials (clause 84).

The ECPA also amends the absolute power of the CRTC to prohibit or regulate the use of the telecommunications facilities of any Canadian carrier in cases where the telecommunication is a commercial electronic message under the ECPA (clause 85(1)). However, this amendment appears to be temporary – a replacement subsection is listed next which partially restores this power in the case of interactive phone calls, faxes and voice mail messages (clause 85(2)). This suggests that the government plans to replace the first amendment with the second one at a later date.

The delayed amendment **provides a framework for** replacing the DNCL with a new scheme at a future date, **as described earlier in this summary**. The powers to be restored with the delayed amendment include the power to regulate the hours during which such communications can be made, the contact information that must be provided by the communicator and the way in which it must be provided, and the use of automated telephone calls. A provision allowing the CRTC to regulate communications with medical and emergency services is also included (clause 85(2)). In addition, **another** delayed amendment (clause 86) would repeal the provisions in the current Act that created the DNCL.

M. Coming Into Force (Clause 87)

The ECPA and its associated amendments of other Acts would come into force on a day or days to be fixed by the Governor in Council. This would permit the phasing in of certain provisions, including any delayed amendments such as those affecting the DNCL.