LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

LEGISLATIVE SUMMARY

# *Bill C-28:*

# *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*

**Publication No. 40-3-C28-E**
**28 May 2010**
***Revised 4 February 2011***

**Alysia Davies**

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

**Terrence J. Thomas**

Industry, Infrastructure and Resources Division
Parliamentary Information and Research Service

# *Legislative Summary of Bill C-28*

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

*Ce document est également publié en français.*

Library of Parliament ***Legislative Summaries*** summarize government bills currently before Parliament and provide background about them in an objective and impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations. Legislative Summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

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.

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

Publication No. 40-3-C28-E
Ottawa, Canada, Library of Parliament (2011)

# CONTENTS

# LEGISLATIVE SUMMARY OF BILL C-28: 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

## 1 BACKGROUND

On 25 May 2010, the Honourable Tony Clement, Minister of Industry, introduced Bill C-28, 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.

**The House of Commons passed the bill as introduced, with one exception: it deleted clause 1, which had proposed the short title, the "Fighting Internet and Wireless Spam Act." The Senate passed the bill without amendment.**

**The short title and its acronym, FISA, were used in previous versions of this legislative summary. For convenience, this version will continue to use the acronym FISA as an unofficial designation when referring to the Act.**

The bill is an updated version of Bill C-27 from the 2nd Session of the 40th Parliament, which bore the short title of the "Electronic Commerce Protection Act" (ECPA). The ECPA died on the *Order Paper* when it reached the stage of second reading in the Senate, due to the prorogation of Parliament on 30 December 2009. Bill C-28 incorporates items that were added to the former ECPA as government amendments during its passage through the House of Commons, and it contains some additional changes.

As with the previous bill, in addition to creating FISA, this new 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 FISA, although both the Commissioner of Competition and the Privacy Commissioner will also play enforcement roles related to their respective mandates.

FISA 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]

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.

FISA is the latest attempt at creating legislation to act on the task force findings. When the federal government introduced the first attempt at this legislation during the 2nd Session of the 40th Parliament, it issued a news release to accompany it which thanked the task force, as well as Senators Donald Oliver and Yoine Goldstein "for their efforts to help address this issue."[3] During the past few years, both of these senators had introduced bills concerning spam in the Senate which contained their own proposals for anti-spam legislation; those bills died on the *Order Paper*.

The government's approach to anti-spam legislation, as encapsulated in FISA, is more extensive and complex, 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, the bill 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 news release on the currently proposed legislation that FISA is intended to "deter the most damaging and deceptive forms of spam … from occurring in Canada and to help to drive spammers out of Canada."[4]

FISA 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 e-commerce sector across the country.[6] FISA will expand the federal government's participation in this area considerably. Up to now, the main federal legislation related to e-commerce has been the *Personal Information Protection and Electronic Documents Act* (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] FISA specifies that in the event of any conflict between FISA and PIPEDA, it is now FISA that will prevail.[8] On 25 May 2010, along with FISA, the government introduced a companion bill, C-29, to update PIPEDA as well.[9]

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.[10]

FISA 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,[11] phishing,[12] spyware,[13] viruses,[14] and botnets.[15] It will also grant an additional right of civil action to businesses and consumers targeted by the perpetrators of such activities.

# 2 DESCRIPTION AND ANALYSIS

## 2.1 DEFINITIONS (CLAUSE 2)

FISA 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.

FISA contains its own definition of “commercial activity,” which is different from the one in PIPEDA, although it does not modify the existing definition in that Act. FISA 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 FISA, 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.

FISA 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 FISA to most means of electronic communication, with the exception of broadcasting, which is explicitly exempted from FISA in clause 6.

There are also provisions at the end of FISA, 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.[16] The breadth of the definition of "electronic message" in FISA 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.

FISA 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 FISA 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 FISA 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."

FISA 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).

### 2.2 Purpose (Clause 4) and Related Clauses (Clauses 3 and 4–6)

FISA 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 4).

FISA establishes itself as binding on any corporation, whether it is provincially or federally incorporated (clause 5), but it does not, as previously indicated, apply to broadcasters (clause 6). As indicated earlier, FISA contains a new provision that was not in its predecessor bill, specifying that in the event of a conflict between any provisions of FISA and PIPEDA, it is FISA that will prevail (clause 3).

## 2.3 KEY PROVISIONS (CLAUSES 7–10 AND 13)

The key violations which are at the heart of FISA are laid out in clauses 7 to 10 of the bill.

Clause 7 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.[17] 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 7(5)). Clause 7(7) exempts the service provider from liability in relation to spamming.

Clause 7(6), which was originally added to the predecessor bill through a government amendment when it was before the House of Commons Standing Committee on Industry, Science and Technology, 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* 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.[18]

Clause 7(8) 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 FISA. However, later in FISA, clause 69 provides for the repeal of this exemption provision, which indicates that while telemarketing activities covered by the DNCL may be exempt from FISA 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 7 of FISA 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.) FISA 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 91). In their testimony before the Committee on this bill's predecessor, 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 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 bill's clauses concerning the DNCL, which are mostly replicated in FISA with some technical changes, are intended to give the government the flexibility to respond to this situation if and as it arises.[19]

Clause 8 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), as well as the ability to withdraw that consent at will (under the specifications laid out in clause 12(4)). Clause 8(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 9, 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. (The owner must also have the option to withdraw that consent under the specifications laid out in clause 12(5).) 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 10 designates the aid, inducement, causing or procurement of any of the activities in clauses 7 to 9 to be a violation as well.

Activities under clause 7 are violations only if a computer system located in Canada is used to send or access[20] the electronic message in question, and in the case of clause 8, 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 9 (clause 13).

### 2.4 CONSENT (CLAUSES 11, 12 AND 14)

Clause 11 defines express consent and implied consent for the purposes of FISA. 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 FISA, 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 11(10) and 11(13) 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 11 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.

FISA incorporates some amendments that were added to its predecessor bill at the Committee stage to provide extra instructions to those seeking consent on behalf of someone whose identity is not known. Under clause 11(2) of FISA, 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 updated clause replaces the provision laid out in the original version of the predecessor bill 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. Clauses 11(3)–11(8) of FISA specify 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 11(4)(*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 11(5)). 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 11(6)–11(8)).

The definition of "implied consent" in clause 11(9) of the bill, which again incorporates amendments made to the predecessor bill, 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 11(9)(*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 11(9)(*c*)). Further exceptions may be specified in the regulations (clause 11(9)(*d*)).

Those who can assume implied consent because of a business relationship must meet the one of the following criteria (clause 11(10)):

- 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 11(12)).

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 11(11)).

Those who can assume implied consent because of a non-business relationship must meet one of the following criteria (clause 11(13)):

- 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 11(14)).

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 12 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 12(2)). Any unsubscribe notification received by the sender must be put into effect within 10 business days (clause 12(3)).

For cases where there is express consent to alter transmission data under clause 8, 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 12(4)).

For cases where there is express consent to download a program onto a person's computer under clause 9 (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 11(5) were not as advertised in the original consent request, has to be provided for a year after the program's installation (clause 12(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 12(5)(*b*)).

Anyone who alleges to have either express or implied consent for activities under clauses 7 to 9 has the burden of proving it in court and/or before the regulator (clause 14).

### 2.5 Violations and Penalties (Clauses 15–47)

FISA designates the CRTC as the main regulatory agency responsible for pursuing administrative penalties against those who violate the Act (clause 15). 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 FISA, and to prevent disclosure of that demand for the purposes of protecting an investigation (clause 16).[21] 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 17).

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 18). 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 19). The CRTC may also apply to a justice of the peace for a warrant to enter a place of business pursuant to FISA, 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 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 20(4)).

FISA imposes significant monetary penalties for violations of clauses 7 to 10 of the Act, along with a list of factors to be taken into account in determining the amount levied (clause 21(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 the regulations may define some types of violations as being separate for each day that they continue, so the maximum amounts for these could therefore be imposed for each day that the law is found to have been violated (clause 21(5)). If the regulations were to designate spamming to be this kind of violation, for example, a business that has been spamming for 10 days could conceivably be required to pay up to $100,000,000 in penalties.

FISA 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 FISA, and may require payment of a given amount (clause 22).

Otherwise, when a violation is committed, a notice of violation can be issued by the CRTC (clause 23). All violations that are pursued under FISA 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 24). 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 25). If representations are made, the CRTC has to make a finding of whether the violation was committed, on a balance of probabilities standard (clause 26). Once a violation has been deemed or found, the CRTC has the power to order the violating party to cease contravening the law (clause 27).

Any such finding (clause 26) or order (clause 27) 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 17 and 19, 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 25) cannot be appealed, but any orders arising from them (clause 27) 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 FISA. There is a five-year limitation period on the recovery of penalties, payments and expenses (clause 29(2)). 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 30).

Violations of FISA are not criminal offences (clause 31), 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 32). 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 33). There is a due diligence defence (clause 34(1)), but other common law defences can only be used to the extent that they do not conflict with other provisions of FISA (clause 34(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 35 and 36). The CRTC may designate one member or a panel to conduct hearings, and may set its own rules of procedure (clauses 37 and 38).

In addition to the various measures providing for hearings to establish if there has been a violation of FISA, the names of those who are deemed violators or who have given undertakings to cease activities prohibited by FISA can also be made public by the CRTC, along with the amounts of any monetary penalties imposed upon them (clause 40). 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 41).

The CRTC may also apply to the courts for an injunction to stop anticipated violations of FISA (clause 42(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 42(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 FISA, commits an offence (clause 43). So does anyone who obstructs, hinders or knowingly provides false or misleading information to the CRTC in connection with a FISA proceeding of any type (clause 44). The same broad vicarious liability of employers and piercing of the corporate veil that apply to FISA violations also apply to these offences (clauses 45 to 46). 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 47(2)). 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 (clauses 47(1)(*a*) and (*b*)).

It should be noted that in addition to this new regime, it appears from the proposed amendments to the *Competition Act* (see part 2.10 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 FISA (clauses 71–82).

### 2.6 Private Right of Action (Clauses 48–56)

In addition to all of these remedies, FISA also creates a private right of action for individuals who have been affected by contraventions of FISA. A person who alleges that he or she is affected by an act or omission that breaches the key provisions of the Act (clauses 7 to 10) 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 78), 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 83).

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 FISA. 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 49).

It appears from the wording of FISA 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." If the issue specifically engages the false and misleading messages provision(s) of the *Competition Act*, it is referred to as "reviewable conduct." In any case, these words all appear to refer to the same breaches of FISA, centred on clauses 7 to 10, 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 51). 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 FISA up to a maximum of $1,000,000 per day (clause 52(1)), depending on the particular type of contravention.[22] 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 52(3)). Another factor to be taken into account by the courts is the purpose of any such compensation, which cannot, under FISA, be punitive. Such awards are intended to "promote compliance" with FISA, PIPEDA and the *Competition Act* (clause 52(2)).

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, and may also be applied in relevant cases of violations of PIPEDA and the *Competition Act* (clauses 53–54). 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 FISA,

PIPEDA or the *Competition Act* (clause 55). In addition, where more than one party is found to have contravened the relevant sections of any of these three statutes, those parties are all jointly and severally liable for the damages and penalties imposed (clause 56).

### 2.7 Information Sharing (Clauses 57–62)

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

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). FISA 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 FISA (clauses 7–10), or of certain provisions of the *Competition Act*, the *Telecommunications Act*, and PIPEDA itself (clause 57).

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 58). 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 59), although each of them can only use this information in relation to the particular statute for which he or she is responsible (clause 60).

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 FISA. All such information-sharing arrangements must be in the form of written agreements, however (clause 61(1)), and they may concern only illegal activity under foreign laws that does not have penal consequences (clause 61(3)). 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 61(5)).

Clause 62 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 FISA (sections 7 to 10), including those in the *Competition Act* (sections 52.01 and 74.011) and PIPEDA (section 7.1).

### 2.8 MISCELLANEOUS (CLAUSES 63–67)

The CRTC is permitted to incur expenses and hire experts for the purpose of activities related to FISA (clauses 63 and 64). The CRTC may also make regulations (clause 65(2)) pertaining to:

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

The Governor in Council may make regulations on various matters (clause 65(1)), including:

- the circumstances in which consent is deemed to have been withdrawn for the purposes of clause 7;
- 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 11(5), (6) and (8);
- 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; and
- any general matters relating to carrying out the purposes and provisions of FISA.

FISA includes a clause that was added to its predecessor bill at the Committee stage requiring a parliamentary review of the legislation. However, the FISA version of the clause potentially changes the timing of such a review. The FISA review is to occur three years after the section mandating it comes into force, rather than three years after FISA as a whole comes into force (clause 66), as required in the earlier bill. Thus the timing of a parliamentary review of FISA could vary depending on when this section is declared in force.

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 7 of FISA 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 67 and 68).

### 2.9 AMENDMENTS TO THE *CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION ACT* (CLAUSE 70)

The only amendment to this Act is a provision incorporating the new powers of the CRTC under FISA by reference (clause 70).

### 2.10 AMENDMENTS TO THE *COMPETITION ACT* (CLAUSES 71–82)

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 text of the bill includes a series of "explanatory notes" to show what is being changed in this Act.

FISA adds several new definitions to the 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 FISA (clauses 71 and 72).

The FISA 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 FISA (clause 71).

FISA 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 74).

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 75).

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 75).

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 77).

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 76).

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 76).

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 78 and 79). 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 FISA or has agreed to pursuant to a settlement agreement under FISA (clause 80).

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 81).

### 2.11 AMENDMENTS TO THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (PIPEDA) (CLAUSES 83–88)

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.

FISA adds some new definitions to this Act, including “computer program,” “computer system” and “electronic address” as they are defined under FISA. (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 83).

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. FISA introduces a caveat: in the case of the collection and/or use of an electronic address obtained through data mining or other automated crawling, most of the PIPEDA exceptions 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, in an illegal manner (i.e. one that "contravenes an Act of Parliament") (clause 83).[24] 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.

FISA 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 FISA (clauses 7 to 10) or the amended provisions of the *Competition Act*, although he or she would have the power to reconsider if there are "compelling reasons" (clause 84).

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 a FISA matter already under investigation by the CRTC is also included (clause 84). Complainants may apply to the court for a hearing with respect to a discontinuance decision if desired (clause 86).

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 88).

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 88).

### 2.12 AMENDMENTS TO THE *TELECOMMUNICATIONS ACT* (CLAUSES 89–91)

This Act currently prohibits the CRTC from disclosing any confidential information submitted to it during the course of proceedings. FISA would create an exception, allowing such information to be disclosed to others when the CRTC is applying its powers in respect of clauses 7 to 10 of FISA. This would include confidential financial, commercial or scientific information, trade secrets, and similar types of materials (clause 89).

FISA 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 FISA (clause 90(1)). However, this amendment appears to be temporary – a set of replacement subsections that partially restore this power in the case of interactive phone calls, faxes and voice mail messages (clauses 90(2), (3) and (4)) are listed next. This suggests that the government plans to replace the first amendment with the subsequent amendments at a later date.

The delayed set of amendments 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 amendments 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 90(3)). In addition, another delayed amendment (clause 91) would repeal the provisions in the current Act that created the DNCL.

### 2.13 COMING INTO FORCE (CLAUSE 92)

FISA 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 or the review of the legislation by Parliament.

---

## NOTES

1. Task Force on Spam, *Stopping Spam: Creating a Stronger, Safer Internet*, Industry Canada, May 2005, pp. 1 and 7.
2. Ibid., p. 9.
3. Industry Canada, "Government of Canada Protects Canadians with the Electronic Commerce Protection Act," News release, Ottawa, 24 April 2009.
4. Industry Canada, "Government of Canada Moves to Enhance Safety and Security in the Online Marketplace," News release, Ottawa, 25 May 2010.
5. Uniform Law Conference of Canada, *Uniform Electronic Commerce Act*.

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*, Publication no. 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.

8. FISA, clause 3.

9. For more information on Bill C-29, see Alysia Davies, *Bill C-29: An Act to amend the Personal Information Protection and Electronic Documents Act*, Publication no. 40-3-C29-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, forthcoming.

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

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

12. 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.

13. 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.

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

15. 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.

16. See, for example, with respect to the earlier version of FISA: Michael Geist, "Why the ECPA Lays the Groundwork To Kill The Do-Not-Call List," *Michael Geist's Blog*, 27 April 2009.

17. 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)).

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

19. House of Commons, Standing Committee on Industry, Science and Technology, *Evidence*, 2nd Session, 40th Parliament, 26 October 2009, 1645–1710 (André Leduc and Philip Palmer, Industry Canada).

20. The word "route" was originally also included in the predecessor bill's equivalent to clause 7, but was then removed by an amendment at the Committee stage, and has not reappeared in FISA.

21. 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 16(3)(*c*), 16(4)(*b*), 18(2)(*c*), 18(4)(*b*), 20(1)(*a*)(iii) and 61(3)(*a*) of FISA, as well as the new sections 52.02 and 74.012 of the *Competition Act* introduced by amendments to clauses 76 and 78 of the bill.)

22. Specifically, units of $200 can be awarded with respect to particular violations and/or contraventions of FISA 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 (clauses 52(1)(*b*)(i)–(vii)).

23. In the original version of this bill from the previous session, 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. These changes have been retained in the proposed FISA.

24. The wording of this provision in the bill from the previous session was “without authorization,” but this has been changed in FISA to refer to contravention of statutory law only.