PRB 05-35E

Library of Parliament Bibliothèque du Parlement

ACCESS TO INFORMATION AND PRIVACY RIGHTS: CHANGES INTRODUCED BY THE *ANTI-TERRORISM ACT* AND THE *PUBLIC SAFETY ACT, 2002*

Jennifer Wispinski
Law and Government Division

24 February 2006

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

TABLE OF CONTENTS

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

ACCESS TO INFORMATION AND PRIVACY RIGHTS: CHANGES INTRODUCED BY THE *ANTI-TERRORISM ACT* AND THE *PUBLIC SAFETY ACT, 2002*

INTRODUCTION

In the wake of the 11 September 2001 attacks in the United States, Parliament enacted the *Anti-terrorism Act*[1] and the *Public Safety Act, 2002*.[2] These statutes contain provisions that have altered the privacy rights of Canadians and those in Canada, as well as their ability to access government-held information. This paper briefly describes the key changes introduced by these Acts. It also summarizes concerns raised and recommendations made in relation to these changes by the Offices of the Information and Privacy Commissioners of Canada to the House of Commons Subcommittee on Public Safety and National Security[3] and the Special Senate Committee on the *Anti-terrorism Act*,[4] and by the Office of the Privacy Commissioner to the Standing Senate Committee on Transport and Communications.[5]

---

(1) S.C. 2001, c. 41.

(2) S.C. 2004, c. 15.

(3) A transcript of the Deputy Information Commissioner's 8 June 2005 testimony before the House of Commons Subcommittee on Public Safety and National Security is available on the Subcommittee's Web site at: http://www.parl.gc.ca/committee/CommitteePublication.aspx?SourceId=121672. A transcript of the Privacy Commissioner's 1 June 2005 testimony before this Subcommittee is similarly available at: http://www.parl.gc.ca/committee/CommitteePublication.aspx?SourceId=119943.

(4) A transcript of the Information and Deputy Information Commissioners' 30 May 2005 testimony before the Special Senate Committee on the *Anti-terrorism Act* is available on the Committee's Web site at: http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/12eva-e.htm?Language=E&Parl=38& Ses=1&comm_id=597. A transcript of the Privacy Commissioner's 9 May 2005 testimony before this Committee is similarly available at: http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/10evb-e.htm?Language=E&Parl=38&Ses=1&comm_id=597.

(5) A transcript of the Privacy Commissioner's 18 March 2004 testimony before the Standing Senate Committee on Transport and Communications is available on the Committee's Web site at: http://www.parl.gc.ca/37/3/parlbus/commbus/senate/Com-e/tran-e/03evb-e.htm?Language=E&Parl=37&Ses=3&comm_id=19.

KEY CHANGES INTRODUCED BY THE *ANTI-TERRORISM ACT*

Section 87 of the *Anti-terrorism Act* added section 69.1 to the *Access to Information Act*,[6] while sections 103 and 104 of the *Anti-terrorism Act* added section 4.1 to the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[7] and section 70.1 to the *Privacy Act*,[8] respectively. These new provisions are designed to work in conjunction with sections 38.13(1), (7), (9) and section 38.131 of the *Canada Evidence Act* (CEA), which, in turn, were added to the CEA by section 43 of the *Anti-terrorism Act*.

In order to understand the effect that the *Access to Information Act*, PIPEDA and *Privacy Act* amendments have had on the ability of Canadians and those in Canada to access government-held personal information and information about government generally, it is first necessary to understand the effect of the CEA amendments referred to above. Basically, sections 38.13(1), (7), (9) and 38.131 of the CEA provide that in circumstances where a decision or order has been made in connection with a "proceeding"[9] that may result in the disclosure of "sensitive information"[10] or "potentially injurious information,"[11] the Attorney General of Canada may issue a certificate prohibiting such disclosure. The certificate must be published in the *Canada Gazette* and is in force for 15 years, unless reissued. A party to the proceedings in relation to

---

(6) R.S.C. 1985, c. A-1.

(7) S.C. 2001, c. 5.

(8) R.S.C. 1985, c. P-21.

(9) Under section 38 of the CEA, "proceeding" is defined as "a proceeding before a court, person or body with jurisdiction to compel the production of information." It is accordingly defined broadly enough to include a complaint made under the *Access to Information Act*, PIPEDA or the *Privacy Act*.

(10) Under section 38 of the CEA, "sensitive information" is defined as "information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside of Canada, and is of a type that the Government of Canada is taking measures to safeguard." Like the definition of "proceeding," the definition of "sensitive information" is broad. The Attorney General of Canada is empowered to issue a non-disclosure certificate if the information in question merely "relates" to international relations, national defence or national security. Non-disclosure certificates and the processes for issuing them and challenging them are discussed in greater detail below.

(11) Under section 38 of the CEA, "potentially injurious information" means "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security." It is unclear from this definition how harmful the information in question must be to be considered potentially injurious. It is therefore possible that information that might merely embarrass the Canadian government, a Canadian defence or security agency, a foreign government, or a foreign defence or security agency could provide sufficient grounds for the Attorney General to issue a non-disclosure certificate. In his 30 May 2005 testimony before the Special Senate Committee on the *Anti-terrorism Act*, the Deputy Information Commissioner identified this possibility.

which a certificate was issued may apply to a single judge of the Federal Court of Appeal for a review of the Attorney General's decision to issue it, and a judge of that court may confirm, vary or cancel the certificate. With respect to a decision to vary, section 38.131(8) states that a judge shall vary the certificate if he or she determines that some of the information subject to the certificate does not relate either to information obtained in confidence from or in relation to a foreign entity, or to national defence or national security. With respect to a decision to cancel, section 38.131(9) provides that a judge shall cancel if none of the information subject to the certificate relates to these matters. There is no appeal from the judge's decision.

In terms of the way these sections of the CEA interact with the new sections of the *Access to Information Act*, PIPEDA and the *Privacy Act*, the new sections of the latter three statutes state that if the Attorney General issues a section 38.13 CEA non-disclosure certificate in relation to documents or personal information before a complaint is filed under the *Access to Information Act*, PIPEDA or the *Privacy Act* respecting a request for information under these Acts, the Acts do not apply in relation to the documents or personal information sought. In addition, the new sections provide that where a non-disclosure certificate has been issued after a complaint has been filed under these Acts, all proceedings with respect to "the complaint" to the Information Commissioner under the *Access to Information Act* are discontinued, and all proceedings with respect to the "personal information" to which the complaint to the Privacy Commissioner under PIPEDA or the *Privacy Act* relates are discontinued.

Other provisions affecting the privacy rights of Canadians introduced by the *Anti-terrorism Act* include sections 273.65(1) to (4) of the *National Defence Act*.[12] These sections created a new mechanism whereby "private communication" as defined in the *Criminal Code*[13] could be intercepted by the Communications Security Establishment (CSE), Canada's signals intelligence agency, for the purpose of obtaining foreign intelligence or for the purpose of protecting Canadian government computer systems from mischief, unauthorized use or interference. Prior written authorization is required from the Minister of National Defence before such interceptions can be made, and there are conditions attached to the making of such

(12) R.S.C. 1985, c. N-5.

(13) As defined in section 183 of the *Criminal Code*, "private communication" means "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it… ." Accordingly, private communication can be thought of as communication where one of the parties or intended parties to the communication is in Canada.

authorizations designed to limit the circumstances under which they can be made and the effect of interceptions on the privacy of Canadians. For example, the Minister may authorize the CSE to intercept private communication only if he or she is satisfied that: the interception is directed at foreign entities outside of Canada, or, in the case of interception for the purpose of protecting Government of Canada computer systems or networks, is necessary to isolate or prevent harm to those systems or networks; the information could not reasonably be obtained by other means; the expected foreign intelligence value of the interception justifies the interception, or in the case of interceptions to protect Government of Canada computer systems or networks, the consent of those whose private communications may be intercepted cannot reasonably be obtained; and, in the event of an interception, satisfactory measures are in place to protect the privacy of Canadians.

KEY CHANGES INTRODUCED BY THE *PUBLIC SAFETY ACT, 2002*

Other pieces of national security legislation, such as the *Public Safety Act, 2002*, also introduced provisions that could affect how personal information held in Canada is shared or used. For example, section 4.81 of the *Aeronautics Act*,[14] a section added to that Act by the *Public Safety Act, 2002*, empowers the Minister of Transport or other designated person to require air carriers and airline reservation systems operators to provide passenger information to him or her for the purpose of transportation security. The Minister of Transport may then disclose the information to other officials within the Department of Transport and to certain officials outside the department, such as the Minister of Citizenship and Immigration, the Minister of National Revenue, and the CEO of the Canadian Air Transport Security Authority (CATSA), for the purposes of transportation security. "Transportation security" is broadly defined in the Act.[15] Normally, information collected can be retained for a maximum of only seven days after it was provided or disclosed.

---

(14) R.S.C. 1985, c. A-2.

(15) Under section 4.81(0.1) of the *Aeronautics Act*, "transportation security" is defined as "the protection of any means of transportation or of any transportation infrastructure, including related equipment, from any actual or attempted action that could cause, or result in (a) loss of life or personal injury; (b) substantial damage to or destruction of a means of transportation or any transportation infrastructure; or (c) interference with any means of transportation or with any transportation infrastructure that is likely to result in loss of life or personal injury, or substantial damage to or destruction of any means of transportation or any transportation infrastructure."

Another provision introduced by the *Public Safety Act, 2002* that affects or has the potential to affect the privacy rights of Canadians is section 4.83 of the *Aeronautics Act*, which relieves aircraft operators from restrictions under PIPEDA that generally prohibit organizations from disclosing personal information in their possession without the consent of the individual to whom the information relates. Under section 4.83, aircraft operators can share advance information respecting passengers on board, or expected to be on board, aircraft scheduled to land in a foreign state with authorities of that state.

Section 4.82 of the *Aeronautics Act*, which is not yet in force, would allow the RCMP Commissioner, the Director of the Canadian Security Intelligence Service (CSIS), or officials designated by them to obtain this same airline passenger information, without warrant, for transportation security purposes, or for a variety of other purposes, some of which are not directly related to terrorism, transportation security or national security. For example, they would be able to obtain this information to enforce arrest warrants where a person has been charged with an offence punishable by imprisonment of five years or more, or arrest warrants under the *Immigration and Refugee Protection Act*(16) and the *Extradition Act*.(17)

In addition, the *Public Safety Act, 2002* amended section 7 of PIPEDA to allow private sector institutions to collect personal information about their clients without their consent, and to disclose this information to government, law enforcement and national security agencies in certain specified circumstances,(18) as long as the agencies have identified their lawful authority to obtain that information.

RECOMMENDATIONS FOR CHANGE MADE BY CANADA'S INFORMATION AND PRIVACY COMMISSIONERS TO COMMITTEES REVIEWING THE *ANTI-TERRORISM ACT*

Section 145 of the *Anti-terrorism Act* made it mandatory for a committee of the Senate, House of Commons or both, or a joint committee of both Houses of Parliament, to undertake a comprehensive review of the Act's provisions and operation within three years of its

(16) S.C. 2001, c. 27.

(17) R.S.C. 1985, c. E-21.

(18) For example, according to sections 7(1)(*e*)(i) and 7(3)(*c*.1)(i) of PIPEDA, such information may be collected by private institutions without consent and disclosed to government institutions if the institution in question suspects that information relates to national security, the defence of Canada or the conduct of international affairs.

receiving Royal Assent. The *Anti-terrorism Act* received Royal Assent on 18 December 2001, and accordingly, in December 2004, the Senate and the House of Commons each established a review committee: the Special Senate Committee on the *Anti-terrorism Act* and the House of Commons Subcommittee on Public Safety and National Security, respectively. These committees have been conducting parallel reviews of the Act and its operations.

Both committees have heard from a variety of witnesses, including federal government officials, individual experts and academics, representatives of the Canadian legal community, policing and intelligence agencies and associations, civil liberties organizations, human rights advocates and advocacy groups, and community groups and individuals affected by the *Anti-terrorism Act*. These witnesses expressed a variety of views on the statutory provisions contained in the *Anti-terrorism Act* and Canada's national security legislation generally. With respect to access to information, privacy and government information sharing, some witnesses expressed particular concern about the effect that the provisions discussed above have had or could potentially have on the privacy rights of Canadians and those in Canada and their ability to access government-held information. Among the witnesses who expressed concern were the Information Commissioner, the Deputy Information Commissioner, and the Privacy Commissioner. Due to their particular expertise with respect to information and privacy issues, the concerns and recommendations of the Office of the Information Commissioner of Canada and the Office of the Privacy Commissioner of Canada in relation to the above provisions have been outlined below.

A. Recommendations of the Office of the Information Commissioner of Canada

When the Information Commissioner and the Deputy Information Commissioner appeared before the Special Senate Committee on the *Anti-terrorism Act* on 30 May 2005, and when the Deputy Information Commissioner appeared before the House of Commons Subcommittee on Public Safety and National Security on 8 June 2005, they expressed concern about section 38.13 CEA non-disclosure certificates and the way that these certificates, once issued by the Attorney General, could operate to interfere with the Information Commissioner's ability to independently investigate complaints under the *Access to Information Act* in accordance with his/her statutory mandate. In their view, section 69.1 had the potential to interfere with the Information Commissioner's mandate under the *Access to Information Act*

more than section 4.1 of PIPEDA or 70.1 of the *Privacy Act* had the potential to interfere with the Privacy Commissioner's mandate under those Acts. This was because section 69.1 states that where a certificate has been issued after an *Access to Information Act* complaint has been filed, all proceedings in relation to "the complaint" are discontinued. Thus, if a non-disclosure certificate is issued in relation to even one record that has been made the subject of a complaint, the Information Commissioner is prohibited from investigating the substance of the rest of the complaint. By contrast, section 4.1 of PIPEDA and section 70.1 of the *Privacy Act* state that where a section 38.13 non-disclosure certificate prohibits the disclosure of a particular piece of personal information, then only those proceedings relating to the information subject to the certificate are discontinued. The limitations on investigation imposed on the Privacy Commissioner by section 4.1 of PIPEDA and 70.1 of the *Privacy Act* are therefore narrower in scope than those imposed on the Information Commissioner under section 69.1 of the *Access to Information Act*.(19)

After identifying these concerns, the Office of the Information Commissioner of Canada made the following recommendations for change in relation to the provisions discussed above:

- repeal section 38.13 of the CEA, or, failing that;
- repeal section 69.1 of the *Access to Information Act* to permit independent investigation of complaints by the Information Commissioner, or, failing that;
- amend section 87 of the *Anti-terrorism Act* [section 69.1 of the *Access to Information Act*] to correspond to sections 103 and 104 of the *Anti-terrorism Act* [section 4.1 of PIPEDA and section 70.1 of the *Privacy Act*];
- amend section 31.131 of the CEA to permit substantive review of a section 38.13 non-disclosure certificate by the Federal Court; and
- reduce the effective period of a section 38.13 certificate from 15 years to 5 years.(20)

---

(19) See the Information Commissioner's 30 May 2005 Remarks to the Senate Special Committee on Anti-terrorism (Review of the *Anti-terrorism Act*), available on the Office of the Information Commissioner of Canada's Web site at: http://www.infocom.gc.ca/speeches/speechview-e.asp?intspeechId=112.

(20) See the 7 June 2005 letter of the Honourable John M. Reid, P.C., Information Commissioner, Office of the Information Commissioner of Canada, to Senator Joyce Fairbairn, Chair, Special Senate Committee on the *Anti-terrorism Act*, for the full text of these recommendations. In addition, Mr. Reid's 7 June 2005 letter contained one additional recommendation for change, which was to add the Information Commissioner to section 10(3) of the *Security of Information Act*, R.S.C. 1985, c. O-5, as a person who cannot be designated as a person permanently bound to secrecy.

B. Recommendations of the Office of the Privacy Commissioner of Canada

When the Privacy Commissioner appeared before the Special Senate Committee on the *Anti-terrorism Act* on 9 May 2005 and the House of Commons Subcommittee on Public Safety and National Security on 1 June 2005, she expressed concern about the effect that various amendments introduced by the *Anti-terrorism Act* had had on privacy rights generally, and then, on behalf of her Office, made several specific recommendations for change in relation to the provisions discussed above. With respect to her general comments, the Privacy Commissioner stated that the surveillance powers of security, intelligence and law enforcement agencies had been overly broadened, that constraints on the use of those surveillance powers had been unduly weakened, and that government accountability and transparency had been significantly reduced. With respect to specific recommendations for change directly related to the provisions discussed above, the Office of the Privacy Commissioner recommended:

- amending the provisions in the *National Defence Act* that allow the CSE to intercept private communication upon receipt of written authorization from the Minister of National Defence so that prior judicial authorization is required for such interceptions;
- amending section 273.65(2) of the *National Defence Act* so that when the Minister of National Defence authorizes the CSE to intercept private communication, he or she is not merely required to take "satisfactory measures" to protect the privacy of Canadians, but "all reasonable measures," or alternatively, amending section 273.65(2) to specify in further detail what constitutes "satisfactory measures";
- amending section 273.65(4)(*d*) of the *National Defence Act* (section 273.65(4) permits the CSE, with prior written authorization of the Minister of National Defence, to collect information essential to protecting the government's computer systems) to place limits on what information the CSE can obtain;
- repealing section 38.13 of the CEA on the basis that it is superfluous to empower the executive to trump an adjudicative order for disclosure;
- reducing the effective period of a section 38.13 CEA certificate from 15 years to 5 years, perhaps subject to renewal;
- amending section 38.131 of the CEA so that the Federal Court of Appeal judge reviewing a non-disclosure certificate under section 38.13 is able to judicially balance competing disclosure and security interests when deciding whether to uphold, cancel or vary the certificate; and
- allowing for appeals from the Federal Court of Appeal judge's decision under section 38.131 of the CEA, or alternatively, allowing the review to be conducted by a panel of three judges instead of one, so as to encourage greater checks and balances and the possibility of dissent.[21]

(21) The recommendations listed above are paraphrased, and only those recommendations specifically relevant to the statutory provisions discussed in this paper have been included. To view the full text of the Privacy Commissioner's remarks and recommendations, see the 9 May 2005 Opening Statement of the Privacy Commissioner of Canada to the Special Senate Committee on the *Anti-terrorism Act*, and the 1 June 2005 Opening Statement of the Privacy Commissioner of Canada to the House of Commons Subcommittee on Public Safety and National Security. This text is available on the Privacy Commissioner's Web site at: http://www.privcom.gc.ca/speech/2005/sp-d_050509_e.asp.

RECOMMENDATIONS FOR CHANGE MADE BY CANADA'S PRIVACY COMMISSIONER TO THE STANDING SENATE COMMITTEE ON TRANSPORT AND COMMUNICATIONS

In their appearances before and submissions to the House of Commons and Senate committees charged with reviewing the *Anti-terrorism Act*, neither the Information Commissioner or Deputy Information Commissioner nor the Privacy Commissioner made specific recommendations respecting the changes introduced by the *Public Safety Act, 2002*. Like most witnesses appearing before these committees, they confined their express recommendations for change to provisions introduced by the *Anti-terrorism Act.* The Privacy Commissioner did, however, express concerns and make recommendations for change in relation to Bill C-7, which became the *Public Safety Act, 2002*, when she appeared before the Standing Senate Committee on Transport and Communications in 2004 during its study of this bill.

With respect to the changes Bill C-7 would introduce into the *Aeronautics Act*, the Privacy Commissioner saw proposed sections 4.81 (requiring air carriers and airline reservation systems operators to provide passenger information to the Transport Minister for the purpose of transportation security), 4.82 (allowing the RCMP and CSIS to obtain the same passenger information, without warrant, for transportation security and other purposes)[(22)] and 4.83 (requiring airline operators to disclose passenger information to authorities of foreign states in certain circumstances) as raising serious privacy concerns. In her remarks to the Committee, she stated that these provisions, if enacted, would "dangerously blur the line between the private sector and the state by enlisting businesses, not only in the fight against terrorism, but in identifying individuals against whom there may be outstanding warrants for a wide variety of offences."[(23)] In her view, these provisions represented the beginning of a slippery slope: if Parliament was prepared to ask airline operators to turn over personal information to various government agencies, it might well decide to pass legislation, at some future date, requiring businesses such as car rental companies or Internet service providers to collect and turn over

(22) As stated previously in this paper, while sections 4.81 and 4.83 of the *Aeronautics Act* have been enacted, section 4.82 of the Act is not yet in force.

(23) See the 18 March 2004 Remarks of the Privacy Commissioner to the Standing Senate Committee on Transport and Communications in relation to Bill C-7, available on the Office of the Privacy Commissioner of Canada's Web site at: http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp.

personal information in their possession to government or law enforcement agencies.(24) The new proposed provisions of the *Aeronautics Act*, in her opinion, also contradicted or ran counter to the legislative trend, as evidenced by the enactment of PIPEDA, of granting increased recognition to the importance of privacy and to one of the general principles of privacy law: that information can and should be used only for the purpose for which it was originally collected.

In addition, the Privacy Commissioner saw clause 98 of Bill C-7, which proposed to amend section 7 of PIPEDA, as problematic because of its breadth: the proposed amendments would apply not just to air carriers but to all private organizations, allowing them to collect personal information about their clients without their consent and to disclose the information to government institutions with lawful authority to obtain the information in specified circumstances.

With respect to specific recommendations for change in relation to the provisions of the *Public Safety Act, 2002*, discussed above, the Office of the Privacy Commissioner of Canada recommended:

- dropping clause 98 of Bill C-7 (clause 98, introducing changes to section 7 of PIPEDA, was subsequently enacted);
- amending section 4.82 of the *Aeronautics Act* to allow the RCMP to match passenger information obtained from air carriers and airline reservation systems to databases related to national security only, rather than allowing the RCMP to match the information to databases containing warrant information generally; and
- requiring air carriers and airline reservations systems operators to inform individuals that they routinely provide government and law enforcement agencies with personal information in their possession.(25)

---

(24) The Privacy Commissioner's remarks in this regard would appear to have been prophetic. In the 1st Session of the 38th Parliament, the government of the day introduced Bill C-74, the *Modernization of Investigative Techniques Act*, which would have, among other things, made subscriber contact information from telecommunications service providers available on request to designated law enforcement and CSIS officials. Bill C-74 died on the *Order Paper* when Parliament was dissolved on 29 November 2005 in anticipation of a general election.

(25) The recommendations listed above are paraphrased. To view the original text, see the 18 March 2004 Remarks of the Privacy Commissioner to the Standing Senate Committee on Transport and Communications in relation to Bill C-7 at: http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp.

CONCLUSION

As the above overview demonstrates, the *Anti-terrorism Act* and the *Public Safety Act, 2002* have introduced several changes to Canada's access to information and privacy regimes. These changes have enhanced the federal government's ability to keep information in its possession out the hands of the public in certain circumstances, even when the information in question is personal information relating to the individual requesting it. They have also enhanced the ability of certain government departments to share personal information in their possession with other government departments and agencies and foreign authorities in specified circumstances.

Do these provisions go too far in their efforts to safeguard national security and protect confidential information? The matter is unclear. These changes may well be necessary, and may strike the right balance between privacy and access rights and national security. However, the recommendations made by the Offices of the Information and Privacy Commissioners suggest that, in their opinions at least, there should be some amendment or fine-tuning of the new statutory provisions, in order to allow the Commissioners to fully perform their respective statutory mandates, to provide Canadians with better access to government-held information, and to ensure that the privacy rights of Canadians are respected and upheld.