PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

COMMITTEE ON POLITICAL AND JURIDICAL AFFAIRS

OEA/Ser.G
CP/CAJP-3026/11 add. 5
1 February 2012
Original: TEXTUAL

QUESTIONNAIRE REGARDING PRIVACY AND DATA PROTECTION LEGISLATION AND PRACTICES

[AG/RES. 2661 (XLI-O/11)]

(Answers by Member States: Canada)

QUESTIONNAIRE

I. LEGISLATION

A. Does your country's domestic legal system include (comprehensive or sectoral) privacy/data protection laws or regulations at the national/federal level? If so, please describe the laws or regulations briefly, including whether they apply to the private and/or public sector contexts, and attach copies of the provisions and the documents containing them.

At the federal level, there are two statutes that create comprehensive privacy protection regimes: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The *Privacy Act*, which took effect in 1983, enunciates the obligations of federal government institutions regarding the collection, use, disclosure, retention and disposal of personal information. It gives individuals the right to access and request correction of personal information that Government holds about them, subject only to the exceptions in the Act. It also puts in place an independent ombudsperson, the Privacy Commissioner, to resolve problems and oversee compliance with the legislation. The *Privacy Act* also provides the right to apply to the Court for review in some limited circumstances. The *Privacy Act* must be read with the *Library and Archives of Canada Act* regarding the retention and disposal of personal information under the control of government institutions.

The *Personal Information Protection and Electronic documents Act* (PIPEDA), which took effect by stages between 2001 and 2004, sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. It applies to all organizations engaged in commercial activities or that operate in a federally-regulated area of jurisdiction, such as banking, telecommunications and interprovincial and international transportation. Private sector organizations subject to provincial privacy legislation that has been recognized by Order as being substantially similar to PIPEDA are exempt from the federal Act for all intra-provincial collections, uses or disclosures of personal information. The law gives individuals control over their personal information, by requiring organizations to seek their consent prior to collecting, using or disclosing their information. Individuals also have the right to access and to request correction of their personal information held by these organizations The Act gives to the Privacy Commissioner the power to receive or initiate complaints and requires the Commissioner to investigate and report on these complaints, which may be resolved through various dispute resolution mechanisms. Unresolved matters may be taken to Federal Court, which has the power to order an organization to change its practices and award damages to the applicant.

Relevant documents and links

- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act*
- *Library and Archives of Canada Act*

B. Does your country's domestic legal system include (comprehensive or sectoral) privacy/data protection laws or regulations at the state/municipal/local level? If so, please describe the laws or regulations briefly and attach copies of the provisions and the documents containing them.

In Canada, every province and territory has privacy legislation governing the collection, use disclosure, retention and disposal of personal information held by government agencies. The provisions of these acts are not identical but all statutes are based on the same fair information principles. They regulate the powers that a government institution has to collect, use and disclose personal information and usually provide individuals with a general right to access and correct their personal information. Oversight is through either an independent commissioner or ombudsperson authorized to receive and investigate complaints.

In some provinces, the same legislation applies to the provincial and the municipal levels while in other provinces this goal is achieved by two different statutes.

Some provinces have a legislation governing the collection, use, disclosure, retention and disposal of personal information by private sector organizations that were recognized as substantially similar to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Some provinces have also passed legislation to deal only with the collection, use, disclosure, retention and disposal of personal health information by health care providers and other health care organizations. Two of these healthcare privacy laws have been recognized as substantially similar to PIPEDA.

Relevant documents and links

Alberta

- *Freedom of Information and Protection of Privacy Act*
- *Health Information Act*
- *Personal Information Protection Act*

British Columbia

- *Freedom of Information and Protection of Privacy Act*
- *Personal Information Protection Act*
- *E-Health (Personal Health Information Access and Protection of Privacy) Act*

Manitoba

- *Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Act*

New Brunswick

- *Right to Information and Protection of Privacy Act*
- *Personal Health Information Privacy and Access Act*

Newfoundland and Labrador

- *Access to Information and Protection of Privacy Act*
- *Personal Health Information Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmNorthwest Territories

- *Access to Information and Protection of Privacy Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmNova Scotia

- *Freedom of Information and Protection of Privacy Act*
- *Part XX of the Municipal Government Act*
- *Personal Information International Disclosure Protection Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmNunavut

- *Access to Information and Protection of Privacy Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmOntario

- *Freedom of Information and Protection of Privacy Act*
- *Municipal Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act, 2004*

http://www.priv.gc.ca/resource/prov/index_e.cfmPrince Edward Island

- *Freedom of Information and Protection of Privacy Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmQuébec

- *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*
- *Act Respecting the Protection of Personal Information in the Private Sector*
- *An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Act respecting the Régie de l'assurance maladie du Québec*

http://www.priv.gc.ca/resource/prov/index_e.cfmSaskatchewan

- *Freedom of Information and Protection of Privacy Act*
- *Local Freedom of Information and Protection of Privacy Act*
- *Health Information Protection Act*

http://www.priv.gc.ca/resource/prov/index_e.cfmYukon

- *Access to Information and Protection of Privacy Act*

C. Does your country have constitutional provisions that address or implicate privacy/data protection, such as, for example, specific data protection provisions, freedom of expression provisions or habeas data? If so, please describe these provisions and attach copies of the relevant texts.

The *Canadian Charter of Rights and Freedoms* (*Charter*) forms part of Canada's Constitution and applies to all levels government: federal, provincial, territorial and municipal. Every government action and decision is subject to the *Charter*. Certain actions of non-governmental entities can also be subject to the *Charter* where these essentially amount to "government actions", which is assessed according to established jurisprudential criteria.

Section 8 of the *Charter*, which reads "Everyone has the right to be secure against unreasonable search or seizure", is the main constitutional provision framing the collection, use and disclosure of personal information by government institutions and agencies. Canadian courts have interpreted s. 8 broadly and contextually. Its protection encompasses a guarantee against any form of unwarranted state interference with a person's reasonable expectation of privacy. For such intrusions to be considered "reasonable", thus in compliance with s. 8, they must be authorised by law. The law itself must be reasonable and the search or

seizure must be carried out in a reasonable manner. Thus, absent reasonable lawful authorisation for an intrusion, a person whose reasonable expectation of privacy has been breached – be it from any of the protected perspectives (*i.e.* physical: one's body; territorial: one's home; or informational**:** one's information disclosing intimate details of lifestyle or personal choices) – can seek a constitutional remedy, which includes damages.

Section 7 of the *Charter* protects the right to life, liberty and security of the person in accordance with the principles of fundamental justice. It has, at times, been construed as also providing residual protection for privacy interests, including those pertaining to data.

While issues relating to informational privacy mainly implicate s. 8 of the *Charter*, section 2(b) can be construed as playing an ancillary role in the general protection of data. Section 2(b) constitutionally protects freedom of expression in Canada. The provision reads: "Everyone has the following fundamental freedoms: (…) (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;…" Canadian courts have interpreted this protection very generously, requiring any state-imposed restriction to satisfy the stringent justification test of section 1 of the *Charter*, which reads "The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society". The burden of the test rests with the state.
The principles underlying freedom of expression in Canada would extend to expression and data on the Internet, ensuring, for instance, a person's constitutional right to access data located on the Internet and to express themselves *via* the Internet, so long as the expression does not constitute violence or a threat thereof, or otherwise breach other applicable laws in Canada such as the *Criminal Code* prohibitions against child pornography, hate speech and incitement to terrorism. Section 2(b) includes the right to receive expression. However, absent exceptional circumstances, s. 2(b) does not formally guarantee a right of access to government information. Such a right is governed by other laws.

Relevant documents and links

- *Canadian Charter of Rights and Freedoms*

D. Does your country include self-regulatory codes of conduct or similar accountability systems for privacy/data protection? If so, please describe these systems briefly and attach copies of any relevant provisions and documents which describe their operation.

The Canadian Standard Association's *Model Code for the Protection of Personal Information* (Q830) was developed in 1996 and has been approved as a National Standard of Canada by the Standards Council of Canada. It sets out ten principles that balance the privacy rights of individuals and the information requirements of private organizations and has been incorporated into the *Personal Information Protection and Electronic Documents Act* (PIPEDA)**.** It continues to exist as self-regulatory tool independent of the PIPEDA and can be used as such by private sector organizations that are not subject to PIPEDA or to provincial legislation applicable to the private sector.

Relevant documents and links

- *Model Code for the Protection of Personal Information* (CSA)

II. REGULATION/ENFORCEMENT

C. What is/are the enforcement mechanism(s) for the above privacy/data protection laws, regulations or procedures and what are the available remedies? Please describe any existing mechanism(s), and attach copies of relevant texts or documentation.

Enforcement mechanisms, regulations and procedures vary between Canadian provinces. Usually, an individual can complain to a provincial privacy commissioner and has a right to apply to the court. Nevertheless, the powers of the provincial privacy commissioners varies in each jurisdiction as does the right to go to court for review.

At the federal level, the Privacy Commissioner of Canada has the mandate of overseeing compliance with both the *Privacy Act* and the *Personal Information Protection and Electronic documents Act* (PIPEDA). She receives and investigates complaints regarding the application of these Acts. She may also initiate a complaint where there are reasonable grounds to investigate a matter under these Acts as well as conduct audits of the fair information practices of government institutions and of the personal information management practices of an organization. In order to do so, she might use her power to summon witnesses, administer oaths and compel the production of evidence. After, she must issue a report with recommendations to federal government institutions or private sector organizations to remedy situations, as appropriate. Her recommendations are not binding.

The *Privacy Act* provides a person who has been refused access to her/his personal information with a right to apply to the Court for review after the Privacy Commissioner has reported on her investigation. The Commissioner is allowed to apply and appear on behalf of such an individual, with his or her consent. With respect to the collection, use, disclosure, retention and disposal of personal information, the Privacy Commissioner can report her findings and recommendations directly to a complainant and to Parliament when she believes that the Act has not been applied correctly by a government institution, but neither she nor the complainant is given the right, under the Act, to apply to Court to enforce her recommendations in this regard.

Under the PIPEDA, a complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made. The Commissioner may also apply to the Court for a hearing. The Court is provided with the power to award damages and order an organization to change its practices as well as to report publicly on actions taken or proposed to be taken to correct its practices.

It should be noted that the implementation of the *Privacy Act* is also the responsibility of the President of Treasury Board, who is the designated Minister for the Act. As such, he is responsible for the preparation and distribution of directives and guidelines on the operation of the Act and the *Privacy Regulations*. The directives and guidelines are presently issued as mandatory Treasury Board Secretariat policy instruments in the form of a policy (*Policy on Privacy Protection*) and four directives (*Directive on Social Insurance Number, Directive on Privacy Practices, Directive on Privacy Impact Assessment, Directive on Privacy Requests and Correction of Personal Information*). The policy instruments include monitoring and reporting requirements in regards to the administration of the Act and Regulations. Compliance is monitored through public reporting documents, Treasury Board submissions, Departmental Performance Reports, results of audits, evaluations, studies and the Management Accountability Framework (MAF) for those institutions subject to this framework. They also include consequences that may be imposed should evidence of compliance issues be brought to the attention of the Treasury Board Secretariat and the President of the Treasury Board. The applicable consequences range from additional reporting requirements and recommendations to removal of delegated authority granted to heads of government institutions by the designated minister under the *Privacy Act*. Aside from the role of the President of the Treasury Board, as designated minister for the administration of the *Privacy Act* and *Privacy Regulations*, the responsibility to monitor compliance in individual government institutions rests first and foremost with the designated heads of the government institutions.

An unjustified breach of sections 8, 7 or 2(b) of the *Canadian Charter of Rights and Freedoms* can lead to remedial action under section 24 of the *Charter*. Subs. 24(1) invests a "court of competent jurisdiction" (judicially defined by a set of criteria) with the power to grant any remedy considered appropriate and just in the circumstances. Subs. 24(2) allows a court that concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by the *Charter* to exclude this evidence if it is established, having regard to all the circumstances, that its admission in the proceedings would bring the

administration of justice into disrepute. In addition, pursuant to subs. 52(1) of the *Constitution Act, 1982*, any legislation or subordinate instrument that is judicially found to infringe s. 8, s. 7 or s. 2(b) of the *Charter* will be declared of no force or effect unless the state satisfies its burden to justify the restriction as a reasonable limit in a free and democratic society.

Links to data protection authorities in Canada

- Privacy Commissioner of Canada
- Office of the Information and Privacy Commissioner of Alberta
- Office of the Information and Privacy Commissioner for British Columbia
- Ombudsman of Manitoba
- Access to Information and Privacy Commissioner of New Brunswick
- Information and Privacy Commissioner of Newfoundland and Labrador
- Information and Privacy Commissioner of the Northwest Territories
- Nova Scotia Freedom of Information and Protection of Privacy Review Office
- Information and Privacy Commissioner of Nunavut
- Office of the Information and Privacy Commissioner of Ontario
- Information and Privacy Commissioner of Prince-Edward Island
- Commission d'accès à l'information du Québec
- Information and Privacy Commissioner of Saskatchewan
- Information and Privacy Commissioner of Yukon

Other relevant documents and links

- Subsection 52(1) of the *Constitution Act, 1982*
- *Canadian Charter of Rights and Freedoms*
- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act*
- *Treasury Board Secretariat Policy on Privacy Protection*

B. Does your country's domestic legal system provide individuals with recourse in the national court system for harm caused by privacy/data protection violations? Does it provide government authorities with the authority to enforce relevant privacy/data protection laws and regulations? If so, please describe and attach copies of relevant texts or documentation.

Recourse for harm caused by privacy violation

In several Canadian provinces, the tort of invasion of privacy has been created by legislation. The right to privacy also exists in the Civil Law of Quebec. In these provinces, individuals are then provided with recourse for harm caused by privacy violations. In the other common law provinces, the recourse depends on the potential recognition of a privacy tort by the courts. Recently, the Ontario Court of Appeal has opened the door to such a recourse by recognizing a privacy tort of "intrusion upon seclusion" (see *Jones v. Tsige*, (2012) ONCA 32.)

At the federal level, the *Personal Information Protection and Electronic Documents Act* expressly permits the Court to order damages to the complainant, including damages for any humiliation that the complainant has suffered. (see : *Nammo v. TransUnion of Canada Inc*., (2010) FC 1284; *Girao v. Zarek Taylor Grossman Hanrahan LLP*, (2011) FC 1070 and *Landry v. Royal Bank of Canada*, (2011) FC 687)

Recourse for harm caused by privacy violation by a federal institution is not expressly established by the *Privacy Act*. Consequently, such recourse depends on the potential recognition of a privacy tort by the courts.

As set out in the previous sub-question, the *Charter* contains internal remedial provisions. An individual could have recourse under section 24 of the *Charter* in cases where the right guaranteed by sections 8, 7 or 2(b) has been infringed. Among the possible remedies ordered are damages and the exclusion of evidence obtained in violation of constitutional rights. Similarly, when legislation is inconsistent with the *Charter*, it can be declared of no force or effect pursuant to subs. 52(1) of the *Constitution Act, 1982*.

Authority to enforce data protection

As mentioned before, the provincial and federal legislations are enforced through Parliaments, privacy commissioners and the courts. See our answer at question IIA for the description of the enforcement models at the federal level.

Relevant documents and links

- Subsection 52(1) of the *Constitution Act, 1982*
- *Canadian Charter of Rights and Freedoms*
- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act*
- *Nammo* v. *TransUnion of Canada Inc*., (2010) FC 1284
- *Girao* v. *Zarek Taylor Grossman Hanrahan LLP*, (2011) FC 1070
- *Landry* v. *Royal Bank of Canada*, (2011) FC 687
- *Jones* v. *Tsige*, (2012) ON CA 32

C. Who are the government authorities in your country primarily responsible for enforcing privacy/data protection laws and regulations? Please describe its relation to (or independence from) the government, describe its size in terms of staff and budget and attach copies of relevant texts or documentation.

In each Canadian province and territory, an independent privacy commissioner is primarily responsible for enforcing data protection laws but its size in terms of staff and budget vary broadly.

At the federal level, the main authority responsible for enforcing data protection laws is the Privacy Commissioner of Canada. The Commissioner is an agent of Parliament independent from the executive and the government institutions that are the subject of her investigations and audits. The Privacy Commissioner is appointed for a seven-year term by the governor in council after approval by resolution of both Senate and House of Commons. The Commissioner holds office during good behavior and may only be removed on address of the Senate and House of Commons. The Commissioner is to "engage exclusively in the duties of the office of Privacy Commissioner" and reports annually on the activities of the office to Parliament but may also report more frequently in urgent situations. Her appointment may be renewed at the end of the seven year period.

The Office of the Privacy Commissioner has a staff of approximately 176 employees and an annual budget of approximately $24 million (CAN).

Relevant documents and links

- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act*

- Report on Plans and priorities

D. What volume of complaints relating to privacy/data protection violations do your relevant government authorities receive? Do your authorities address each individual complaint or do they have discretion in which matters to investigate or pursue?

The Privacy Commissioner of Canada received an average of 750 complaints per year over the last 5 years related to the *Privacy Act* and about 330 per year over the last 5 years related to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Under the *Privacy Act*, the Privacy Commissioner shall receive and investigate each complaint. Under the PIPEDA, she is authorized to deal in a more summary fashion with some complaints. Indeed, she is permitted to refuse to investigate a complaint if, for example, the complaint ought first to be addressed under other grievance or review procedures reasonably available, or if it would be more appropriately handled through procedures established under another law. As well, the Privacy Commissioner may discontinue investigations in certain limited circumstances, including when she is of the opinion that there is insufficient evidence to proceed, the complaint is trivial, frivolous, vexatious, or made in bad faith, and that the matter is already the subject of an ongoing investigation, etc.

Relevant documents and links

- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act*
- Annual Report on the *Personal Information and Electronic Documents Act* (2010)
- Annual Report on the *Privacy Act* (2010-2011)

E. Are the investigations and privacy/data protection enforcement actions undertaken by your authorities exclusively complaint-driven or do these authorities have other bases or criteria for selecting and initiating an investigation or enforcement action (ie. proactive audits or filing requirements)? Please explain.

Under the *Privacy Act*, the Privacy Commissioner of Canada is empowered to receive complaint from an applicant on issues ranging from the use and disclosure of personal information to the right of access to personal information by individuals to whom it pertains. If the Privacy Commissioner is satisfied that there are reasonable grounds to investigate one of these issues, she may initiate a complaint. She may also, from time to time at her discretion, carry out investigation in respect of personal information under the control of government institutions to ensure compliance with provisions related to the collection, use

and disclosure of personal information. Following her investigation, she will issue a report containing her findings and any recommendation that she considers appropriate.

Under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Privacy Commissioner of Canada may, in addition to her power to investigate complaints as described under D above, initiate a complaint if she is satisfied that there are reasonable grounds to investigate a matter under the Act. The Privacy Commissioner has one year to file a report of a complaint that she has initiated. The report must to contain the Privacy Commissioner's findings and recommendations, a notice of settlement reached by parties and, if appropriate, a notice of any action taken or proposed to be taken to implement the Privacy Commissioner's recommendations. The Privacy Commissioner may also audit the personal information management practices of an organization if the she has reasonable grounds to believe that the organization is contravening the Act. After an audit, the Privacy Commissioner is required to provide the organization with a copy of the audit report containing the findings of the audit and any recommendations she considers appropriate. The audit report may also be included in the Privacy Commissioner's annual report to Parliament.

F. Are complaints relating to commercial data privacy issues subject to potential criminal prosecution? If so, explain the relationship, if any, between privacy regulators and public prosecutors in such cases and the general volume and nature of criminal proceedings.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not include criminal sanctions. However, under the Act, the Privacy Commissioner may disclose information in the course of a prosecution for an offence of perjury under the *Criminal Code of Canada* in respect of a statement made under PIPEDA. The Privacy Commissioner may also disclose to the Attorney General of Canada or to the provincial Attorney Generals information relating to the commission of an offence against any law of Canada or a province, if it is the Commissioner's opinion that there is sufficient evidence to do so. (see notably sections 56.1, 368(1) and 402.2 of *Criminal Code* regarding identity theft and related misconduct).

Relevant documents and links

- *Criminal Code*

III. CASE LAW

A. What is the role of case law in the protection of individuals' privacy in your country? Please attach any high court or appellate cases in your country.

At the provincial and federal levels, the protection of personal information is largely regulated by statutes. Consequently, the law regulating individual privacy protection is highly influenced by judges either in the context of judicial review applications challenging government decisions, or in the context of the interpretation of the statutes creating the privacy protection regimes.

Judicial rulings regarding the scope and the application of the section 8 of the *Charter* play certainly a capital role in the protection of individual's privacy in Canada.

Relevant documents and links

Privacy Act decisions

- Dagg v. *Canada (Minister of Finance),* [1997] 2 S.C.R. 403
- *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General*), [2006] 1 S.C.R. 441
- *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66.

Section 8 of the *Charter* decisions

- *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145
- *R. v. Dyment*, [1988] 2 S.C.R. 417
- *R. v. Plant,*[1993] 3. S.C.R. 281
- *R. v. Colarusso*, [1994] 1 S.C.R. 20
- *Smith v. Canada (Attorney General)*, [2001] 3 S.C.R. 902
- *R. v. Law*, [2002] 1 S.C.R. 227
- *R. v. Tessling*, [2004] 3 S.C.R. 432
- *R. v. Rodgers*, [2006] 1 S.C.R. 554
- *R. v. Kang-Brown*, [2008] 1 S.C.R. 456
- *R. v. A.M.*, [2008] 1 S.C.R. 569
- *R. v. Patrick*, [2009] 1 S.C.R. 579

- *R. v. Gomboc*, [2010] 3 S.C.R. 211.

IV. CROSS-BORDER COOPERATION

A. Does your country's domestic legal system limit or condition the transfer of any personal data to other countries? If so, please explain.

The disclosure of personal information held by provincial or territorial government institutions to other countries is regulated by provincial or territorial statutes. The limits or conditions on such transfers vary from province or territory to another.

At the federal level, the rules are different depending on whether the *Privacy Act* or the *Personal Information Protection and Electronic documents Act* (PIPEDA) is applicable.

The *Privacy Act* does not establish special rules or conditions for the disclosure of personal information to other countries. The same specific and limited rules governing the disclosure of personal information to third parties applicable in the domestic context are also applicable to disclosures made to other countries. The Federal Government, however, has issued a guidance document to institutions subject to the *Privacy Act* which includes a privacy checklist and advice on considering privacy prior to initiating contracts, in particular, those that involve transborder data flows. (see *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*)

The PIPEDA contains an accountability principle that makes an organization accountable for the personal information in their control or custody, including personal information that they have transferred to a third party for processing. Organization subject to PIPEDA are required to use contractual or other means to ensure that the information that they have transferred to a third party for processing will receive, from the third party processor, a level of protection comparable to that established under PIPEDA. This requirement applies whether the processor is in Canada or abroad.

Relevant documents and links

Guidance Document: Taking Privacy into Account Before Making Contracting Decisions

B. Has your country received a privacy/data protection certification by the European Union?

Yes. In December 2001, the European Commission ruled that Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) received an "Adequacy Finding", meaning that it meets the standards for the protection of personal data as outlined in the European Union's Data Protection Directive. This decision was confirmed in 2006 following the assessment of the Canadian compliance with the 2001 adequacy decision.

In 2005, the protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency was also considered adequate.

Relevant documents and links

Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian *Personal Information Protection and Electronic Documents Act*

The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian *Personal Information Protection and Electronic Documentation Act*

Commission decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency

C. Is your country a party to any international instruments or arrangements regarding general privacy principles and the cross-border flow of information (e.g., the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; the APEC Privacy Guidelines and Cross Border Privacy Rules; the Council of Europe's Convention No. 108)? If so, please list these instruments or arrangements to which your country is a party, the date on which they became enforceable in you jurisdiction and what actions have your country has taken, if any, pursuant thereto.

Canada signed OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1984. Both statutes regulating protection of personal information at the federal level, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), were adopted to follow the OECD guidelines.

Canada is an APEC member since 1989. It endorsed the APEC Privacy Guidelines in 2004 and the APEC Cross Border Privacy Rules System in 2011.

D. Do the laws in your country permit the relevant enforcement authorities to share investigation and enforcement information and evidence with their counterpart authority in foreign jurisdictions? If so, please explain.

Under the *Privacy Act*, the Privacy Commissioner and every person acting on behalf or under her direction shall keep confidential information that comes to their knowledge in the performance of their duties and functions. The Commissioner is nevertheless authorized to disclose that information if this is, in her opinion, necessary to carry out an investigation following the Act.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) prohibits the Privacy Commissioner of Canada or any person acting on her behalf from disclosing any information that comes to their knowledge as a result of the performance of her duties or powers under the Act. The Privacy Commissioner may however make public information about the management practices of an organization if the Commissioner believes that it is in the public interest to do so.

The Privacy Commissioner is permitted to disclose certain information to her foreign counterparts provided that these counterparts have, under the laws of a foreign state, 1) functions and duties similar to those of the Privacy Commissioner in respect of the protection of personal information and 2) responsibilities with respect to addressing conduct that would be considered to contravene PIPEDA.

This information must be 1) relevant to an ongoing or potential investigation of a contravention of the foreign law, provided that the conduct being investigated is substantially similar to that which would be in contravention of PIPEDA or; 2) necessary to disclose in order for the Privacy Commissioner to obtain from her foreign counterpart information that would be useful to an investigation or audit under PIPEDA.

The Privacy Commissioner can only disclose information to her foreign counterparts if she has entered into a written arrangement.

E. Does your government or its enforcement authorities cooperate with other governments or counterpart authorities on investigations and enforcement matters relating to privacy/data protection, for example to address the fraudulent use, transfer or mishandling of personal data?

The Privacy Commissioner of Canada collaborates with counterpart authorities in certain investigations the transfer of personal information across international borders. The Privacy Commissioner is a founding member of Global Privacy Enforcement Network (GPEN), a network designed to facilitate the sharing of information about issues related to enforcement and collaborative outreach activities. The Privacy Commissioner is also a participant in the APEC Cross Border Privacy Enforcement Arrangement (the APEC CPEA), which provides mechanisms to facilitate cross-border cooperation in the enforcement of privacy laws, including facilitating the contact between CPEA participants for the purpose of seeking assistance or making referrals regarding privacy investigations and enforcement matters.

In addition, police authorities cooperate with other governments as needed in matters respecting the enforcement of *Criminal Code* provisions regarding the theft of identity and other specific infractions relating to data protection issues.

F. If cross-border collaboration exists, is this collaboration informal, does it take place via privacy/data protection regulators, or does it take place via cross-border cooperation networks (i.e. Global Privacy Enforcement Network (GPEN), APEC's Cross Border Privacy Enforcement Arrangement, or Iberoamerican Network of Data Protection)? If so, please describe this collaboration and/or your countries participation in said networks.

Cross-border collaboration exists between specific Canadian federal institutions and counterparts in foreign countries.

As noted under E, the Office of the Privacy Commissioner of Canada joined with privacy enforcement agencies around the world in September 2010 to establish the Global Privacy Enforcement Network (GPEN). The Office of the Privacy Commissioner of Canada is also a participant in the APEC CPEA.

G. If does not exist, could some form of cross-border collaboration among OAS member states assist with the enforcement or implementation of your country's privacy/data protection laws? If so, provide suggestions for what would be most useful.

n/a

V. HABEAS DATA

A. Does your country's domestic legal system include laws providing for access to information about oneself, including habeas data? If so, please characterize what rights individuals may exercise under habeas data, describe the source of the right briefly, describe whether said right apply to the private and/or public sector contexts and attach copies of the provisions and the documents containing them.

As Habeas Data is a constitutional right granted in several Latin America' countries, it does not exist as such in Canada's legal system. However, all Canadian provincial, territorial and federal laws applicable to the private or the public sector provide individuals with a right of access to their personal information, subject only to specific exceptions.

The *Privacy Act* and its regulation do include provisions for the access to and correction of personal information under the control of a government institution. Individuals are required to present a formal written request to the appropriate officer of the government institution which has control of their personal information. Informal requests can also be accepted however, individuals may not submit a complaint to the Privacy Commissioner for such requests since they are not done under the *Privacy Act.*

VI. TECHNOLOGY AND BUSINESS CHALLENGES

A. Are there any technologies or business practices that pose particular challenges for the enforcement or implementation of privacy/data protection laws and/or other consumer protection laws in your country? If so, describe.

The development of new technologies, in particular the computer with its virtually limitless power to collect, use, disseminate and retain data, was the key policy driver in the adoption of both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Both Acts were drafted in a technology-neutral fashion and, as such, it has been possible to find ways of applying the privacy protection principles to new technologies and services that have developed since the laws were adopted.