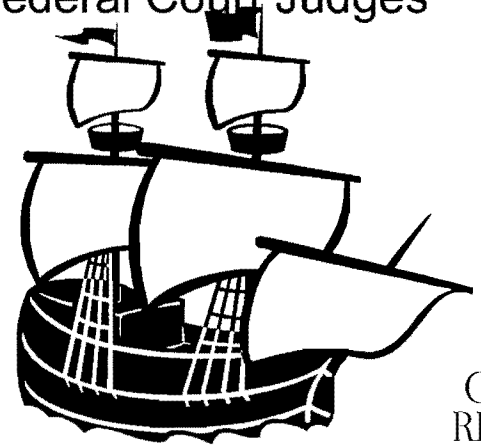
CMLA Admiralty Law Program

Federal Court Judges



OGILVY RENAULT

Johanne Gauthier

April 28, 2000

Number of Years to Reach 50 Million Users

INTERNET	**4 years**
TELEVISION	**13 years**
COMPUTERS	**16 years**
RADIO	**38 years**

Source : Cisco 1998

B2B and Shipping

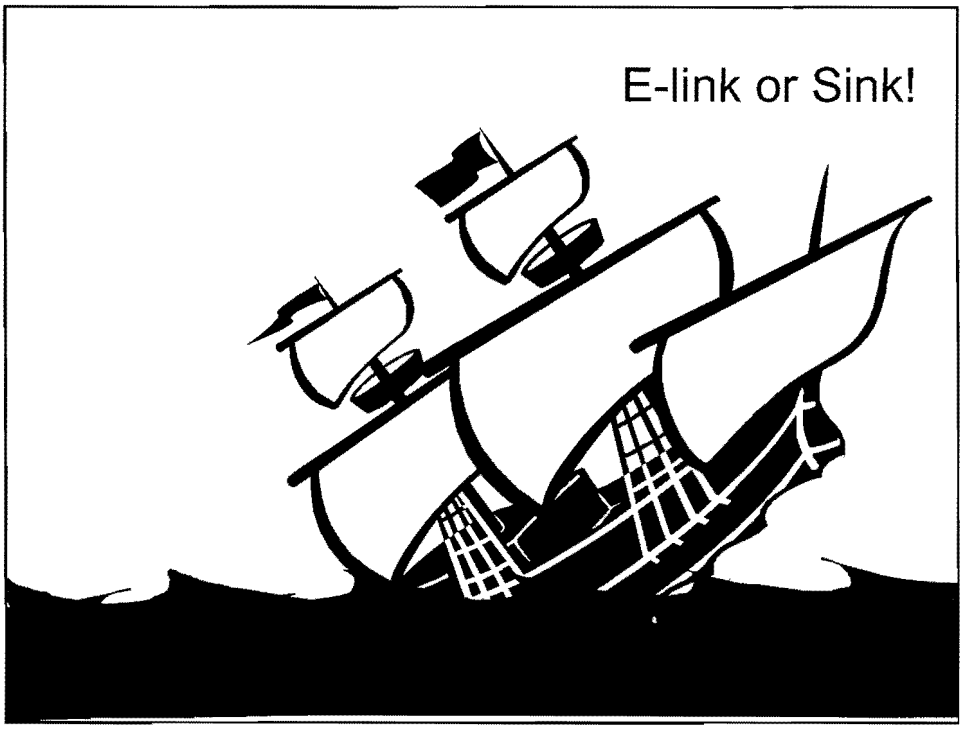
From A to Z

- bolero.net
- tradecard.com

Specialized services

- bunkerworld.com
- lr.org
- gocargo.com
- oocl.com

"Charles Darwin"



Uncitral

The model law on electronic commerce (1996)

the concept of "functional equivalent"

Uncitral

Art. 6 writing i.e. accessible so as to be usable for subsequent reference

Art. 7 signature i.e. identifies the source and confirms the approval of the information

Art. 8 original i.e. integrity - it is complete and has not been altered

Art. 9 admissibility in evidence - reliability of the system

Uncitral

Part two: carriage of goods
Art. 16 and 17

follows in the steps of the CMI Rules on Electronic b/l

Uncitral

Draft Uniform Rules on Electronic Signatures

- Status

European Union

Directive on Electronic Commerce

Directive on Digital Signatures

Creation of EESSI

National Initiatives

Argentina
Australia
Columbia
Germany
Italy
Japan
Russia
Singapore
South Korea
U.K.
U.S.

Personal Information Protection and Electronic Documents Act (C-6 alias C.54)

Part 1

Collection, use and disclosure of personal information in the private sector

Part 2

Electronic alternatives to paper

Part 3

Amendments to the Canada Evidence Act

Personal Information

All organizations federally regulated

All organizations in the course of commercial activities conducted in more than one province

The right of the Governor in Council to provide for exemption where there is legislation in a province substantially similar to the Act

Electronic Documents

Purpose

- To provide for the use of electronic alternatives where federal laws contemplate the use of paper to record or communicate information or transaction

Laws involving the government

Laws involving communications between private citizens

The Government

S. 33. "whenever the law does not specify the manner of doing so."

The governmental authorities may opt for electronic method of creating, collecting, storing, publishing or otherwise dealing with documents or information

The Government

For a number of other situations, the Act gives the responsible authority the power to make regulations providing for electronic alternatives

- e.g. s. 34 (payment)
- e.g. s. 35 (form to be filed)

The Government

S. 37 – Retention of Electronic Documents

Format preserves the integrity of the information

The information is readable or perceivable

Where applicable, the information identifying the origin and destination of the document and the date and time of its transmission, is retained

PART 2 introduces the concepts of "electronic signature" and "secure electronic signature"

definitions s. 31(1) and s. 48

Password with or without PIN

Smart card

Digitized signature

Biometric identification

Digital signature

"Secured Electronic Signature"

Section 48

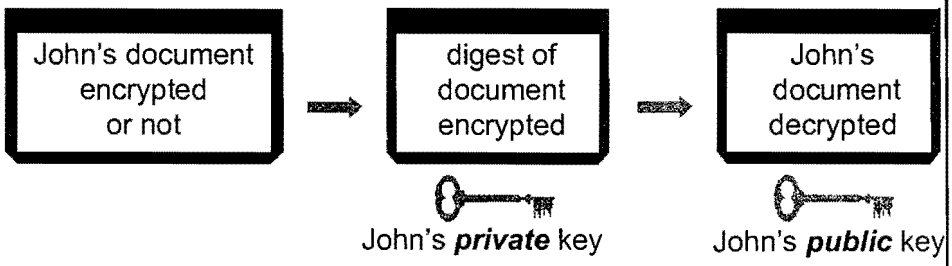
The signature which results from the use of the technology or process is unique to the person;

The use of the technology or process by which the signature is connected to the document is under the sole control of the person;

The technology or process can be used to identify the person using it; and

The signature can be linked to the document in such a way that it can be determined whether the document was altered thereafter.

John sends a message to Mary



If John's digest = Mary's digest, then integrity of message is confirmed

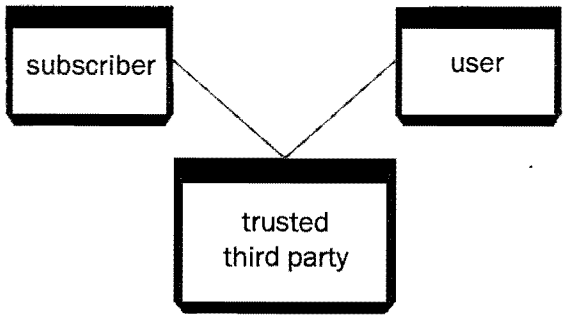
Fundamental Concepts

Private key known only to the owner

Public key easily available

Public key certified to belong to the user

PUBLIC KEY INFRASTRUCTURE (PKI)



Certification authority issues a certificate

Communications Between Private Parties

S. 40 Freedom to use electronic alternatives if

- the federal law is listed in Schedule 2 or 3 of the Act (not yet prepared)
- the parties consented
- the electronic document will be under the control of the person to whom it is provided, it is readable so as to be usable for subsequent reference.

BUT...

Communications Between Private Parties

BUT…

In all cases listed in s. 41 to s. 47, the parties must also comply with the regulations to be usable

AND...

Communications Between Private Parties

AND…

s. 42 original
s. 44 under oath
s. 45 declaration or certificate
s. 46 signature to be witnessed

also require the use of one or more secure electronic signatures

The Canada Evidence Act

The Queen's printer goes "electronic"

amendments to s. 19-20(c) – 21 (b) (c) – 22

New definitions are added in s. 31.8.

data that is recorded or stored on any medium in or by a computer system or other similar device that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

The Best Evidence Rule s. 31.2

Integrity of the system, or

Presumption from use of secure electronic signature

Printout

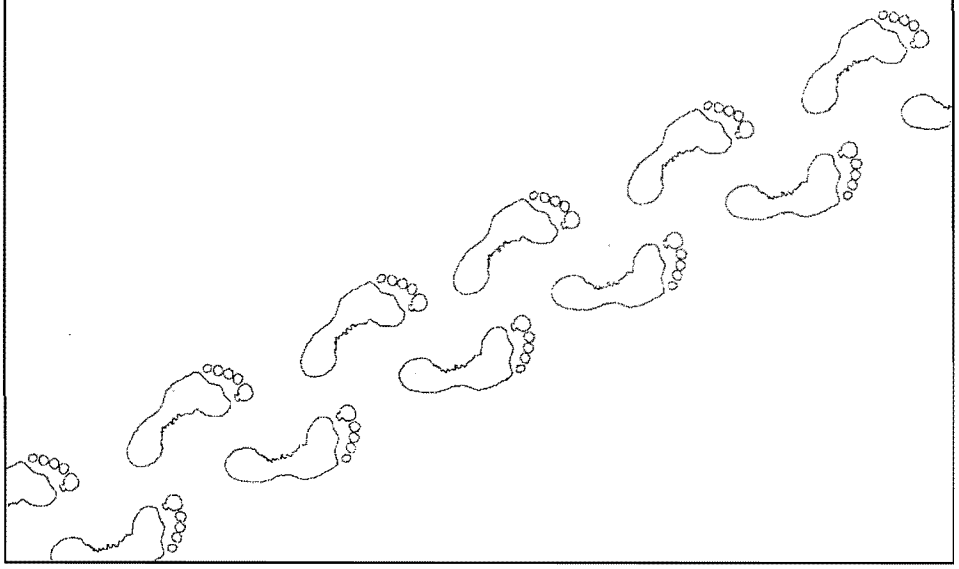
Integrity of the System

Burden of proof

Presumption s. 31.3

Proof by affidavit

The Next Step



We better start
e-thinking!

2nd Session, 36th Parliament,
48 Elizabeth II, 1999

The House of Commons of Canada

BILL C-6

An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

SHORT TITLE

Short title

1. This Act may be cited as the *Personal Information Protection and Electronic Documents Act* .

PART 1

PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR

Interpretation

Definitions

2. (1) The definitions in this subsection apply in this Part.

``alternative format'' « *support de substitution* »

``alternative format'', with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information.

``commercial activity'' « *activité commerciale* »

``commercial activity'' means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

``Commission er'' « *commissaire* »

``Commissioner'' means the Privacy Commissioner appointed under section 53 of the *Privacy Act* .

``Court'' « *Cour* »

``Court'' means the Federal Court-Trial Division.

``federal work, undertaking or business'' « *entreprises fédérales* »

``federal work, undertaking or business'' means any work, undertaking or business that is within the legislative authority of Parliament. It includes

(*a*) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;

(*b*) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;

(*c*) a line of ships that connects a province with another province, or that extends beyond the limits of a province;

(*d*) a ferry between a province and another province or between a province and a country other than Canada;

(*e*) aerodromes, aircraft or a line of air transportation;

(*f*) a radio broadcasting station;

(*g*) a bank;

(*h*) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces;

(*i*) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and

(*j*) a work, undertaking or business to which federal laws, within the meaning of section 2 of the *Oceans Act* , apply under section 20 of that Act and any regulations made under paragraph 26(1)(*k*) of that Act.

``organization'' « *organisation* »

``organization'' includes an association, a partnership, a person and a trade union.

``personal information'' « *renseignement personnel* »

``personal information'' means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

``record'' « *document* »

``record'' includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

Notes in Schedule 1

(2) In this Part, a reference to clause 4.3 or 4.9 of Schedule 1 does not include a reference to the note that accompanies that clause.

Purpose

Purpose

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Application

Application

4. (1) This Part applies to every organization in respect of personal information that

(*a*) the organization collects, uses or discloses in the course of commercial activities; or

(*b*) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Limit

(2) This Part does not apply to

(*a*) any government institution to which the *Privacy Act* applies;

(*b*) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or

(*c*) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

Other Acts

(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.

DIVISION 1

PROTECTION OF PERSONAL INFORMATION

Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

Meaning of ``should''

(2) The word ``should'', when used in Schedule 1, indicates a recommendation and does not impose an obligation.

Appropriate purposes

(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

Effect of designation of individual

6. The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organization of the obligation to comply with the obligations set out in that Schedule.

Collection without knowledge or consent

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(*a*) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(*b*) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(*c*) the collection is solely for journalistic, artistic or literary purposes; or

(*d*) the information is publicly available and is specified by the regulations.

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(*a*) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(*b*) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(*c*) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;

(*c* .1) it is publicly available and is specified by the regulations; or

(*d*) it was collected under paragraph (1)(*a*) or (*b*).

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(*a*) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(*b*) for the purpose of collecting a debt owed by the individual to the organization;

(*c*) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(*c* .1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

(*d*) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(*e*) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

(*f*) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(*g*) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(*h*) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(*h* .1) of information that is publicly available and is specified by the regulations;

(*h* .2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(*i*) required by law.

Use without consent

(4) Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection (2).

Disclosure without consent

(5) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in paragraphs (3)(*a*) to (*h* .2).

Written request

8. (1) A request under clause 4.9 of Schedule 1 must be made in writing.

Assistance

(2) An organization shall assist any individual who informs the organization that they need assistance in preparing a request to the organization.

Time limit

(3) An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request.

Extension of time limit

(4) An organization may extend the time limit

(*a*) for a maximum of thirty days if

(i) meeting the time limit would unreasonably interfere with the activities of the organization, or

(ii) the time required to undertake any consultations necessary to respond to the request would make the time limit impracticable to meet; or

(*b*) for the period that is necessary in order to be able to convert the personal information into an alternative format.

In either case, the organization shall, no later than thirty days after the date of the request, send a notice of extension to the individual, advising them of the new time limit, the reasons for extending the time limit and of their right to make a complaint to the Commissioner in respect of the extension.

Deemed refusal

(5) If the organization fails to respond within the time limit, the organization is deemed to have refused the request.

Costs for responding

(6) An organization may respond to an individual's request at a cost to the individual only if

(*a*) the organization has informed the individual of the approximate cost; and

(*b*) the individual has advised the organization that the request is not being withdrawn.

Reasons

(7) An organization that responds within the time limit and refuses a request shall inform the individual in writing of the refusal, setting out the reasons and any recourse that they may have under this Part.

Retention of information

(8) Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.

When access prohibited

9. (1) Despite clause 4.9 of Schedule 1, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.

Limit

(2) Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual's life, health or security is threatened.

Information related to paragraphs 7(3)(*c*), (*c* .1) or (*d*)

(2.1) An organization shall comply with subsection (2.2) if an individual requests that the organization

(*a*) inform the individual about

(i) any disclosure of information to a government institution or a part of a government institution under paragraph 7(3)(*c*), subparagraph 7(3)(*c* .1)(i) or (ii) or paragraph 7(3)(*d*), or

(ii) the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in paragraph 7(3)(*c*) or to a request made by a government institution or a part of a government institution under subparagraph 7(3)(*c* .1)(i) or (ii); or

(*b*) give the individual access to the information referred to in subparagraph (*a*)(ii).

Notification and response

(2.2) An organization to which subsection (2.1) applies

(*a*) shall, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

(b) shall not respond to the request before the earlier of

(i) the day on which it is notified under subsection (2.3), and

(ii) thirty days after the day on which the institution or part was notified.

Objection

(2.3) Within thirty days after the day on which it is notified under subsection (2.2), the institution or part shall notify the organization whether or not the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

(*a*) national security, the defence of Canada or the conduct of international affairs; or

(*b*) the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

Prohibition

(2.4) Despite clause 4.9 of Schedule 1, if an organization is notified under subsection (2.3) that the institution or part objects to the organization complying with the request, the organization

(*a*) shall refuse the request to the extent that it relates to paragraph (2.1)(*a*) or to information referred to in subparagraph (2.1)(*a*)(ii);

(*b*) shall notify the Commissioner, in writing and without delay, of the refusal; and

(*c*) shall not disclose to the individual

(i) any information that the organization has relating to a disclosure to a government institution or a part of a government institution under paragraph 7(3)(*c*), subparagraph 7(3)(*c* .1)(i) or (ii) or paragraph 7(3)(*d*) or to a request made by a government institution or a part of a government institution under either of those subparagraphs,

(ii) that the organization notified an institution or part under paragraph (2.2)(*a*) or the Commissioner under paragraph (*b*), or

(iii) that the institution or part objects.

When access may be refused

(3) Despite the note that accompanies clause 4.9 of Schedule 1, an organization is not required to give access to personal information only if

(*a*) the information is protected by solicitor-client privilege;

(*b*) to do so would reveal confidential commercial information;

(*c*) to do so could reasonably be expected to threaten the life or security of another individual;

(*c* .1) the information was collected under paragraph 7(1)(*b*); or

(*d*) the information was generated in the course of a formal dispute resolution process.

However, in the circumstances described in paragraph (*b*) or (*c*), if giving access to the information would reveal confidential commercial information or could reasonably be expected to threaten the life or security of another individual, as the case may be, and that information is severable from the record containing any other information for which access is requested, the organization shall give the individual access after severing.

Limit

(4) Subsection (3) does not apply if the individual needs the information because an individual's life, health or security is threatened.

Notice

(5) If an organization decides not to give access to personal information in the circumstances set out in paragraph (3)(*c* .1), the organization shall, in writing, so notify the Commissioner, and shall include in the notification any information that the Commissioner may specify.

Sensory disability

10. An organization shall give access to personal information in an alternative format to an individual with a sensory disability who has a right of access to personal information under this Part and who requests that it be transmitted in the alternative format if

(*a*) a version of the information already exists in that format; or

(*b*) its conversion into that format is reasonable and necessary in order for the individual to be able to exercise rights under this Part.

DIVISION 2

REMEDIES

Filing of Complaints

Contravention

11. (1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule 1.

Commissioner may initiate complaint

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

Time limit

(3) A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

Notice

(4) The Commissioner shall give notice of a complaint to the organization against which the complaint was made.

Investigations of Complaints

Powers of Commissioner

12. (1) The Commissioner shall conduct an investigation in respect of a complaint and, for that purpose, may

(*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

(*b*) administer oaths;

(*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(*d*) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;

(*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the investigation.

Dispute resolution mechanisms

(2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

Delegation

(3) The Commissioner may delegate any of the powers set out in subsection (1) or (2).

Return of records

(4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

Certificate of delegation

(5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*).

Commissioner's Report

Contents

13. (1) The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains

(*a*) the Commissioner's findings and recommendations;

(*b*) any settlement that was reached by the parties;

(*c*) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and

(*d*) the recourse, if any, that is available under section 14.

Where no report

(2) The Commissioner is not required to prepare a report if the Commissioner is satisfied that

(*a*) the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;

(*b*) the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province;

(*c*) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was filed is such that a report would not serve a useful purpose; or

(*d*) the complaint is trivial, frivolous or vexatious or is made in bad faith.

If a report is not to be prepared, the Commissioner shall inform the complainant and the organization and give reasons.

Report to parties

(3) The report shall be sent to the complainant and the organization without delay.

Hearing by Court

Application

14. (1) 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, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1, in subsection 5(3) or 8(6) or (7) or in section 10.

Time of application

(2) The application must be made within forty-five days after the report is sent or within any further time that the Court may, either before or after the expiry of those forty-five days, allow.

For greater certainty

(3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).

Commissioner may apply or appear

15. The Commissioner may, in respect of a complaint that the Commissioner did not initiate,

(*a*) apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;

(*b*) appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or

(*c*) with leave of the Court, appear as a party to any hearing applied for under section 14.

Remedies

16. The Court may, in addition to any other remedies it may give,

(*a*) order an organization to correct its practices in order to comply with sections 5 to 10;

(*b*) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (*a*); and

(*c*) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Summary hearings

17. (1) An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

Precautions

(2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

DIVISION 3

AUDITS

To ensure compliance

18. (1) The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1, and for that purpose may

(*a*) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record;

(*b*) administer oaths;

(*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(*d*) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organization on satisfying any security requirements of the organization relating to the premises;

(*e*) converse in private with any person in any premises entered under paragraph (*d*) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(*f*) examine or obtain copies of or extracts from records found in any premises entered under paragraph (*d*) that contain any matter relevant to the audit.

Delegation

(2) The Commissioner may delegate any of the powers set out in subsection (1).

Return of records

(3) The Commissioner or the delegate shall return to a person or an organization any record or thing they produced under this section within ten days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

Certificate of delegation

(4) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(*d*).

Report of findings and recommendations

19. (1) After an audit, the Commissioner shall provide the audited organization with a report that contains the findings of the audit and any recommendations that the Commissioner considers appropriate.

Reports may be included in annual reports

(2) The report may be included in a report made under section 25.

DIVISION 4

GENERAL

Confidentiality

20. (1) Subject to subsections (2) to (5), 13(3) and 19(1), the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part.

Public interest

(2) The Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

Disclosure of necessary information

(3) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

(*a*) conduct an investigation or audit under this Part; or

(*b*) establish the grounds for findings and recommendations contained in any report under this Part.

Disclosure in the course of proceedings

(4) The Commissioner may disclose, or may authorize any person acting on behalf or under the direction of the Commissioner to disclose, information in the course of

(*a*) a prosecution for an offence under section 28;

(*b*) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Part;

(*c*) a hearing before the Court under this Part; or

(*d*) an appeal from a decision of the Court.

Disclosure of offence authorized

(5) The Commissioner may disclose to the Attorney General of Canada or of a province, as the case may be, information relating to the commission of an offence against any law of Canada or a province on the part of an officer or employee of an organization if, in the Commissioner's opinion, there is evidence of an offence.

Not competent witness

21. The Commissioner or person acting on behalf or under the direction of the Commissioner is not a competent witness in respect of any matter that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part in any proceeding other than

(*a*) a prosecution for an offence under section 28;

(*b*) a prosecution for an offence under section 132 of the *Criminal Code* (perjury) in respect of a statement made under this Part;

(*c*) a hearing before the Court under this Part; or

(*d*) an appeal from a decision of the Court.

Protection of Commissioner

22. (1) No criminal or civil proceedings lie against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise of any duty or power of the Commissioner under this Part.

Libel or slander

(2) For the purposes of any law relating to libel or slander,

(*a*) anything said, any information supplied or any record or thing produced in good faith in the course of an investigation or audit carried out by or on behalf of the Commissioner under this Part is privileged; and

(*b*) any report made in good faith by the Commissioner under this Part and any fair and accurate account of the report made in good faith for the purpose of news reporting is privileged.

Consultations with provinces

23. (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation that is substantially similar to this Part, has powers and duties similar to those of the Commissioner.

Agreements

(2) The Commissioner may enter into agreements with any person with whom the Commissioner may consult under subsection (1)

(*a*) to coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(*b*) to undertake and publish research related to the protection of personal information; and

(*c*) to develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally.

Promoting the purposes of the Part

24. The Commissioner shall

(*a*) develop and conduct information programs to foster public understanding, and recognition of the purposes, of this Part;

(*b*) undertake and publish research that is related to the protection of personal information, including any such research that is requested by the Minister of Industry;

(*c*) encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10; and

(*d*) promote, by any means that the Commissioner considers appropriate, the purposes of this Part.

Annual report

25. (1) The Commissioner shall, as soon as practicable after the end of each calendar year, submit to Parliament a report concerning the application of this Part, the extent to which the provinces have enacted legislation that is substantially similar to this Part and the application of any such legislation.

Consultation

(2) Before preparing the report, the Commissioner shall consult with those persons in the provinces who, in the Commissioner's opinion, are in a position to assist the Commissioner in reporting respecting personal information that is collected, used or disclosed interprovincially or internationally.

Regulations

26. (1) The Governor in Council may make regulations

(*a*) specifying, by name or by class, what is a government institution or part of a government institution for the purposes of any provision of this Part;

(*a* .01) specifying, by name or by class, what is an investigative body for the purposes of paragraph 7(3)(*d*) or (*h* .2);

(*a* .1) specifying information or classes of information for the purpose of paragraph 7(1)(*d*), (2)(*c* .1) or (3)(*h* .1); and

(*b*) for carrying out the purposes and provisions of this Part.

Orders

(2) The Governor in Council may, by order,

(*a*) provide that this Part is binding on any agent of Her Majesty in right of Canada to which the *Privacy Act* does not apply; and

(*b*) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.

Whistleblowing

27. (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Division 1, may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality

(2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

Prohibition

27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that

(*a*) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1;

(*b*) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1;

(*c*) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 not be contravened; or

(*d*) the employer believes that the employee will do anything referred to in paragraph (*a*), (*b*) or (*c*).

Saving

(2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement.

Definitions

(3) In this section, ``employee'' includes an independent contractor and ``employer'' has a corresponding meaning.

Offence and punishment

28. Every person who knowingly contravenes subsection 8(8) or 27.1(1) or who obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of

(*a*) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or

(*b*) an indictable offence and liable to a fine not exceeding $100,000.

Review of Part by parliamentary committee

29. (1) The administration of this Part shall, every five years after this Part comes into force, be reviewed by the committee of the House of Commons, or of both Houses of Parliament, that may be designated or established by Parliament for that purpose.

Review and report

(2) The committee shall undertake a review of the provisions and operation of this Part and shall, within a year after the review is undertaken or within any further period that the House of Commons may authorize, submit a report to Parliament that includes a statement of any changes to this Part or its administration that the committee recommends.

DIVISION 5

TRANSITIONAL PROVISIONS

Application	30. (1) This Part does not apply to any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration.
Expiry date	(2) Subsection (1) ceases to have effect three years after the day on which this section comes into force.

PART 2

ELECTRONIC DOCUMENTS

Interpretation

Definitions

31. (1) The definitions in this subsection apply in this Part.

``data" « *données* »

``data" means representations of information or concepts, in any form.

``electronic document" « *document électronique* »

``electronic document" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

``electronic signature" « *signature électronique* »

``electronic signature" means a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.

``federal law" « *texte législatif* »

``federal law" means an Act of Parliament or an instrument, regardless of its name, issued, made or established under an Act of Parliament or a prerogative of the Crown, other than an instrument issued, made or established under the Yukon Act, the Northwest Territories Act or the Nunavut Act.

``responsible authority" « *autorité responsable* »

``responsible authority", in respect of a provision of a federal law, means

(*a*) if the federal law is an Act of Parliament, the minister responsible for that provision;

(*b*) if the federal law is an instrument issued, made or established under an Act of Parliament or a prerogative of the Crown, the person or body who issued, made or established the instrument; or

(*c*) despite paragraph (*a*) or (*b*), the person or body designated by the Governor in Council under subsection (2).

``secure electronic signature" « *signature électronique sécurisée* »

``secure electronic signature" means an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1).

Designation

(2) The Governor in Council may, by order, for the purposes of this Part, designate any person, including any member of the Queen's Privy Council for Canada, or body to be the responsible authority in respect of a provision of a federal law if the Governor in Council is of the opinion that it is appropriate to do so in the circumstances.

Purpose

Purpose

32. The purpose of this Part is to provide for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper to record or communicate information or transactions.

Electronic Alternatives

Collection, storage, etc.

33. A minister of the Crown and any department, branch, office, board, agency, commission, corporation or body for the administration of affairs of which a minister of the Crown is accountable to the Parliament of Canada may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with documents or information whenever a federal law does not specify the manner of doing so.

Electronic payment

34. A payment that is required to be made to the Government of Canada may be made in electronic form in any manner specified by the Receiver General.

Electronic version of statutory form

35. (1) If a provision of an Act of Parliament establishes a form, the responsible authority in respect of that provision may make regulations respecting an electronic form that is substantially the same as the form established in the provision, and the electronic form may be used for the same purposes as the form established in the provision.

Statutory manner of filing documents

(2) If a non-electronic manner of filing a document is set out in a provision of an Act of Parliament, the responsible authority in respect of that provision may make regulations respecting the filing of an electronic version of the document, and an electronic version of the document filed in accordance with those regulations is to be considered as a document filed in accordance with the provision.

Statutory manner of submitting information

(3) If a non-electronic manner of submitting information is set out in a provision of an Act of Parliament, the responsible authority in respect of that provision may make regulations respecting the manner of submitting the information using electronic means, and information submitted in accordance with those regulations is to be considered as information submitted in accordance with the provision.

Authority to prescribe form, etc.

(4) The authority under a federal law to issue, prescribe or in any other manner establish a form, or to establish the manner of filing a document or submitting information, includes the authority to issue, prescribe or establish an electronic form, or to establish an electronic manner of filing the document or submitting information, as the case may be.

Meaning of ``filing"

(5) In this section, ``filing" includes all manner of submitting, regardless of how it is designated.

Documents as evidence or proof

36. A provision of a federal law that provides that a certificate or other document signed by a minister or public officer is proof of any matter or thing, or is admissible in evidence, is, subject to the federal law, satisfied by an electronic version of the certificate or other document if the electronic version is signed by the minister or public officer with that person's secure electronic signature.

Retention of documents

37. A requirement under a provision of a federal law to retain a document for a specified period is satisfied, with respect to an electronic document, by the retention of the electronic document if

(*a*) the electronic document is retained for the specified period in the format in which it was made, sent or received, or in a format that does not change the information contained in the electronic document that was originally made, sent or received;

(*b*) the information in the electronic document will be readable or perceivable by any person who is entitled to have access to the electronic document or who is authorized to require the production of the electronic document; and

(*c*) if the electronic document was sent or received, any information that identifies the origin and destination of the electronic document and the date and time when it was sent or received is also retained.

Notarial act

38. A reference in a provision of a federal law to a document recognized as a notarial act in the province of Quebec is deemed to include an electronic version of the document if

(*a*) the electronic version of the document is recognized as a notarial act under the laws of the province of Quebec; and

(*b*) the federal law or the provision is listed in Schedule 2 or 3.

Seals

39. A requirement under a provision of a federal law for a person's seal is satisfied by a secure electronic signature that identifies the secure electronic signature as the person's seal if the federal law or the provision is listed in Schedule 2 or 3.

Requirements to provide documents or information

40. A provision of a federal law requiring a person to provide another person with a document or information, other than a provision referred to in any of sections 41 to 47, is satisfied by the provision of the document or information in electronic form if

(*a*) the federal law or the provision is listed in Schedule 2 or 3;

(*b*) both persons have agreed to the document or information being provided in electronic form; and

(*c*) the document or information in electronic form will be under the control of the person to whom it is provided and will be readable or perceivable so as to be usable for subsequent reference.

Writing requirements

41. A requirement under a provision of a federal law for a document to be in writing is satisfied by an electronic document if

(*a*) the federal law or the provision is listed in Schedule 2 or 3; and

(*b*) the regulations respecting the application of this section to the provision have been complied with.

Original documents

42. A requirement under a provision of a federal law for a document to be in its original form is satisfied by an electronic document if

(*a*) the federal law or the provision is listed in Schedule 2 or 3;

(*b*) the electronic document contains a secure electronic signature that was added when the electronic document was first generated in its final form and that can be used to verify that the electronic document has not been changed since that time; and

(*c*) the regulations respecting the application of this section to the provision have been complied with.

Signatures

43. Subject to sections 44 to 46, a requirement under a provision of a federal law for a signature is satisfied by an electronic signature if

(*a*) the federal law or the provision is listed in Schedule 2 or 3; and

(*b*) the regulations respecting the application of this section to the provision have been complied with.

Statements made under oath

44. A statement required to be made under oath or solemn affirmation under a provision of a federal law may be made in electronic form if

(*a*) the person who makes the statement signs it with that person's secure electronic signature;

(*b*) the person before whom the statement was made, and who is authorized to take statements under oath or solemn affirmation, signs it with that person's secure electronic signature;

(*c*) the federal law or the provision is listed in Schedule 2 or 3; and

(*d*) the regulations respecting the application of this section to the provision have been complied with.

Statements declaring truth, etc.

45. A statement required to be made under a provision of a federal law declaring or certifying that any information given by a person making the statement is true, accurate or complete may be made in electronic form if

(*a*) the person signs it with that person's secure electronic signature;

(*b*) the federal law or the provision is listed in Schedule 2 or 3; and

(*c*) the regulations respecting the application of this section to the provision have been complied with.

Witnessed signatures

46. A requirement under a provision of a federal law for a signature to be witnessed is satisfied with respect to an electronic document if

(*a*) each signatory and each witness signs the electronic document with their secure electronic signature;

(*b*) the federal law or the provision is listed in Schedule 2 or 3; and

(*c*) the regulations respecting the application of this section to the provision have been complied with.

Copies

47. A requirement under a provision of a federal law for one or more copies of a document to be submitted is satisfied by the submission of an electronic document if

(*a*) the federal law or the provision is listed in Schedule 2 or 3; and

(*b*) the regulations respecting the application of this section to the provision have been complied with.

Regulations and Orders

Regulations

48. (1) Subject to subsection (2), the Governor in Council may, on the recommendation of the Treasury Board, make regulations prescribing technologies or processes for the purpose of the definition "secure electronic signature" in subsection 31(1).

Characteristics

(2) The Governor in Council may prescribe a technology or process only if the Governor in Council is satisfied that it can be proved that

(*a*) the electronic signature resulting from the use by a person of the technology or process is unique to the person;

(*b*) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;

(*c*) the technology or process can be used to identify the person using the technology or process; and

(*d*) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.

Effect of amendment or repeal

(3) An amendment to or repeal of any provision of a regulation made under subsection (1) that has the effect of removing a prescribed technology or process from the regulation does not, by itself, affect the validity of any electronic signature resulting from the use of that technology or process while it was prescribed.

Amendment of schedules

49. For the purposes of sections 38 to 47, the responsible authority in respect of a provision of a federal law may, by order, amend Schedule 2 or 3 by adding or striking out a reference to that federal law or provision.

Regulations

50. (1) For the purposes of sections 41 to 47, the responsible authority in respect of a provision of a federal law may make regulations respecting the application of those sections to the provision.

Contents

(2) Without restricting the generality of subsection (1), the regulations that may be made may include rules respecting any of the following:

(*a*) the technology or process that must be used to make or send an electronic document;

(*b*) the format of an electronic document;

(*c*) the place where an electronic document is to be made or sent;

(*d*) the time and circumstances when an electronic document is to be considered to be sent or received and the place where it is considered to have been sent or received;

(*e*) the technology or process to be used to make or verify an electronic signature and the manner in which it is to be used; and

(*f*) any matter necessary for the purposes of the application of sections 41 to 47.

Minimum rules

(3) Without restricting the generality of subsection (1), if a provision referred to in any of sections 41 to 47 requires a person to provide another person with a document or information, the rules set out in the regulations respecting the application of that section to the provision may be that

(*a*) both persons have agreed to the document or information being provided in electronic form; and

(*b*) the document or information in electronic form will be under the control of the person to whom it is provided and will be readable or perceivable so as to be usable for subsequent reference.

Incorporation by reference

(4) Regulations may incorporate by reference the standards or specifications of any government, person or organization, either as they read at a fixed time or as they are amended from time to time.

Effect of striking out listed provision

51. The striking out of a reference to a federal law or provision in Schedule 2 or 3 does not affect the validity of anything done in compliance with any regulation made under section 50 that relates to that federal law or provision while it was listed in that Schedule.

SCHEDULE 1
(Section 5)

PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, CAN/CSA-Q830-96

4.1 Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organization's policies and practices; and

(*d*) developing information to explain the organization's policies and procedures.

4.2 Principle 2 - Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to>

Transfer interrupted!

Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(*c*) consent may be given orally when information is collected over the telephone; or

(*d*) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 Principle 4 - Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 - Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 - Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 - Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organizational measures, for example, security clearances and limiting access on a ``need-to-know'' basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 - Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organization;

(*c*) a description of the type of personal information held by the organization, including a general account of its use;

(*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(*e*) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 - Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.