Privacy Handbook for Canadians

3rd Edition

2018

ACLRC

ACLRC
Alberta
Civil Liberties
Research
Centre

Privacy in Canada
3d Edition
2018

Alberta
Civil Liberties
Research Centre

Mailing Address:
c/o Faculty of Law
University of Calgary
2500 University Drive N.W.
Calgary, Alberta T2N 1N4
(403) 220-2505
Fax (403) 284-0945
E-mail: aclrc@ucalgary.ca

Acknowledgments

Alberta LAW FOUNDATION **The Alberta Law Foundation**
The Alberta Civil Liberties Research Centre is supported by a grant from the Alberta Law Foundation.

Brian A. F. Edy, Barrister and Solicitor, Calgary, Alberta, provided a grant for the first edition.

Board of Directors of the Alberta Civil Liberties Research Centre
Doreen Barrie; Michael Greene; Michael Wylie; Patricia Paradis; Ola Malik; and David Wright.

First Edition:
Editors and Principal Researchers and Writers
Brian A. F. Edy, B.A., LL.B., Barrister and Solicitor, Calgary, Alberta.
Linda McKay-Panos, B.Ed., LL.B., LL.M., Executive Director.
Contributing Writers:
Frank Work, Brian Edy, Gary Dickson and Valerie Steeves.
Researching and Writing Assistants (University of Calgary Law Students)
Edith Krawchuk, Hina Thaker, Mia Laister and Samantha Chrysanthou
The Research Centre appreciates the volunteer contributions of:
Gary Dickson, Tyler Lord, Kristen Read, Tracy Arnell, Jan Goodwin, B.J. Fontana, Judith Boer, Pamela Vanberg, Cartney Samson, Allison Eng, Jill Eslinger, Natalie Mohammed and Stephen Anderson. The Vocational Rehabilitation Research Institute kindly permitted us to use some of the graphics in this report.
Second Edition:
Principal Researchers, Writers and Updaters
Amina Osuoha-Muhammad, B.L., LL.B., LL.M. (Notingham), Student-at-Law
Carolyn Conford, B.A. LLB. (Candidate), Law Student Intern

Third Edition:
Principal updater: Jay Moch, B.A., Law Student

Project Management
Sharnjeet Kaur, B.Ed., Administrator.
Linda McKay-Panos, B.Ed., J.D., LL.M., Executive Director.

The Alberta Civil Liberties Research Centre's home page is located at: aclrc.com

ISBN # 1-896225-34-9

Table of Contents

1.0 INTRODUCTION

What is privacy?

Privacy is simply defined as "the right to be left alone".[1] The right to be left alone has expanded over the last 100 years to include the right to be protected from many of the potential invasions of privacy in our modern society. These include: protection of personal information; protection of our physical privacy; freedom from surveillance; privacy of our surroundings and privacy of our personality—the right not to have our personality stolen.[2] Privacy means that we control our information. We alone decide WHO will know WHAT about us.

Why is privacy important?

Privacy is essential in a democracy. The right to privacy:

- allows us to be free from interference from the government and from others;
- ensures that when we vote in an election, no one else will be able to know who we vote for;
- allows us to be candid with our doctors and our lawyers;
- is necessary in order to protect related rights—such as the right to life, liberty and security of the person;
- permits us to feel that we are safe in our homes, free from wiretapping and other surveillance; and
- respects our autonomy.

With the appearance of modern technological advances, such as computers and other electronic equipment, the protection of our privacy has become more challenging. However, some legislators and other advocates believe it is important to continue to safeguard our privacy, even though these new inventions make it more difficult.

What kinds of laws protect privacy in Canada?

Your rights to privacy are protected by:

---

[1] S.D. Warren & L.D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193.
[2] B. Phillips, *The Evolution of Canada's Privacy Laws*, January 28, 2000 Toronto, Ontario. Web site source: http://www.priv.gc.ca/speech/archive/02_05_a_000128_e.cfm

- International laws;
- Canadian constitutional law—the *Canadian Charter of Rights and Freedoms;*[3]
- Legislation, such as provincial and federal privacy legislation and other laws; and
- Common-law—judge-made law that applies to all Canadians.

These laws are discussed throughout this handbook.

Do all countries recognize the right to privacy?

Many countries recognize the right to privacy. Canada is a member of the United Nations. International laws drawn up by the United Nations and ratified (approved) by many of the world's countries recognize privacy as one of our essential human rights. These international documents deal with the relationship between the government and its citizens.

The *Universal Declaration of Human Rights* states in article 12 that:[4]

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

A number of other international documents, such as the *International Covenant on Civil and Political Rights*[5] and the *American Convention on Human Rights*, also speak about privacy rights.

Countries have taken different approaches to regulating privacy and legislating privacy protection. Fair information practices were first dealt with internationally in 1980 by the Organization for Economic Co-operation and Development (OECD) in the *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.*[6] Some countries have moved ahead to provide privacy protection in the private sector. In New Zealand, the *Privacy Act*[7] allows the Privacy Commissioner to review and approve privacy codes for different sectors. The initial code approved was for the New Zealand health sector. The

---

[3] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B of the *Canada Act 1982* (UK), 1982, c 11, (hereinafter "Charter" or "Charter of Rights and Freedoms").
[4] Signed December 10, 1948, G.A. Res. 217 A (III), U.N. Doc A/810, at 71, reprinted in [1948] UNYB 465.
[5] 19 December 1966, Canadian Treaty Service 1976 Number 47, Article 17.
[6] Organization for Economic Cooperation and Development. *Guidelines for the Protection of Privacy and TransBorder Flows of Personal Data* (Paris: OECD, 1981).
[7] *New Zealand Privacy Act*,1993, 028.

code, known as the *Health Information Privacy Code,*[8] once approved by the Commissioner, has the force of law. This approach allows different sectors to modify the notion of "fair information practices" to accommodate unique problems and issues in each sector.

Yet another model is found in the Netherlands.[9] The Netherlands model has standards or codes for privacy protection that are developed on a sector-by-sector basis. Once a code has been adopted, it is codified by regulation. The code is not binding and does not have the force of law.

In October, 1998, the *European Union Privacy Directive*[10] came into force. As a consequence of this Directive, EU members who transfer individual data in the course of commercial activities to other non-EU nations must ensure that those nations have legislation in place to protect the privacy of individuals. In 2001, the European Commission officially recognized that Canada's privacy laws give adequate protection for personal information transferred from the European Union.[11]

New Zealand has extended the scope of its privacy legislation to encompass the private sector. For example, the New Zealand code covers health insurance companies. This reflects the European trend exemplified by the *European Union Privacy Directive*.

When the European Union *Privacy Directive* was introduced in 1995, the province of Quebec was the only compliant jurisdiction in North America. Failure to enact legislative protection for privacy would jeopardize the substantial trade carried on by Canada with those western European nations that belong to the European Union. In response, the Canadian private sector put in place a voluntary code in the mid 1990s, the *Model Code for the Protection of Personal Information.* Next, the Canadian government and some of the provinces embarked on a course of passing privacy legislation that applied to the private

[8] In 1994, New Zealand adopted the *Health Information Code* pursuant to the authority in the *Privacy Act*, 1993.
[9] *Personal Data Protection Act* [Online]. Available: http://english.justitie.nl/themes/personal-data/
[10] Council of the European Parliament, 1995. Directive 95-46/EC on the Protection of Privacy and Transborder Flows of Personal Data and the Free Movement of such Data.
[11] December 20, 2001. Commission Decision pursuant to Directive 95/46/EC (2002/2/EC).

sector **(see Chapter 2: Privacy Protection and the Private Sector).**

Why is privacy a fundamental right in Canada?

Many scholars agree that privacy is essential to life in all societies.[12] Further, the Supreme Court of Canada has recognized that "privacy is at the heart of liberty in a modern state" and "is essential for the well-being of the individual."[13] The Court recognized that each person has three "zones of privacy": territorial (in our homes), personal (privacy of our bodies) and informational (information about ourselves).[14] Thus, it is clear that privacy is a fundamental value and a basic human right in Canadian society.[15]

Canadians' right to privacy in their dealings with the government has been recognized for several years through federal laws. More recently, Canadians' right to privacy in dealings with the private sector is also being recognized in legislation.

Although it is not explicitly stated in the *Charter of Rights and Freedoms*, each Canadian's right to privacy is important to him or her. The late Hon. Sheila Finestone, Chair of the House of Commons Standing Committee that authored a report entitled *Privacy: Where Do We Draw The Line?*",[16] observed as follows:

> Privacy is one of the most comprehensive of all human rights - broad, ambitious and valued around the world. Traditionally understood as the 'right to be left alone', in this technological age, privacy has taken on new dimensions. To experts, privacy is the right to enjoy private space, to conduct private communications, to be free from surveillance and to respect the sanctity of one's body.

---

[12] A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 13, 21-22.

[13] *R v Dyment*, [1988] 2 Supreme Court Reports 417 at 427-28 (hereinafter *Dyment*). See also: *Hunter v Southam Inc.*, [1984] 2 Supreme Court Reports. 145, *R v Edwards*, [1996] 1 Supreme Court Reports 128, at para 50, and *R v Mills*, [1999] 3 Supreme Court Reports 668.

[14] *Dyment*, at 428.

[15] J.D.R. Craig, "Invasion of Privacy and Charter Values: The Common-law Tort Awakens" (1997) 42 McGill Law Journal 355 (hereinafter Craig).

[16] Hon. S. Finestone, *Forward in House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, Privacy: Where Do We Draw the Line?* (Ottawa Public Works and Government Services Canada, April 1997) at 3. Senator Sheila Finestone drafted a privacy bill, which was introduced in Canada's (Senate Bill S-21, March 16, 2001, 37th Parliament, 1st Session). The *Privacy Rights Charter* (Bill S-21) defined an overarching right to privacy in Canada and provided that any infringement of the right to privacy must be reasonable and justifiable. This bill did not get passed. See generally: *Albertans' Awareness of and Views on Privacy Issues Report 31* August 2000, Office of the Information and Privacy Commissioner, Province of Alberta: 78% of Albertans polled expressed strong agreement with the importance of protecting individual privacy.

> To the average Canadian, privacy is a question of power—the ability to control one's personal information and to remain anonymous by choice.

What rights or interests sometimes conflict with Canadians' right to privacy?

The protection of our right to privacy involves a difficult balancing with our right to freedom of expression and our right to freedom of information. This can lead to tension between our personal interest in being left alone and the public's interest in being informed.[17] Much of the law of privacy deals with balancing these rights and interests.

Is there other legislation in Canada, besides the Charter of Rights, *that protects my privacy?*

Yes. There are protections for privacy in the *Criminal Code*[18] and there are federal and provincial laws that provide privacy protection—applicable to the government and, in some cases, to private individuals and companies.

1.1 Privacy and Canada's Government Sector

What privacy legislation regulates the federal and provincial governments?

Federal and provincial governments are subject to the following laws, all of which contain privacy protections:

- The *Canadian Charter of Rights and Freedoms* provides some privacy protections to Canadians.
- Provincial and Federal privacy legislation; in line with Canada's 1984 endorsement of the Organization for Economic Co-operation and Development (OECD Guidelines), all Provincial and territorial jurisdictions in Canada have enacted laws that limit the collection, use and sharing of personal information by governments.[19]

---

[17] P. Osborne, *The Law of Torts* (Toronto: Irwin Law Books, 2000) (Quicklaw source) (hereinafter Osborne).
[18] R.S.C. 1985, c. C-46 (hereinafter Criminal Code).
[19] *Freedom of Information and Protection of Privacy Act*, Revised Statutes of British Columbia 1996, Chapter 165; *Freedom of Information and Protection of Privacy Act*, Statutes of Alberta 2000, Chapter F-25 [hereinafter FOIP Act]; *Freedom of Information and Protection of Privacy Act,* Statutes of Saskatchewan 1990-91, Chapter F-22.01; *Freedom of Information and Protection of Privacy Act*, Statutes of Manitoba 1997, Chapter F175; *An Act Respecting Access to documents held by public bodies and the Protection of Personal Information*, Revised Statutes of Quebec, Chapter A-2.1, *Freedom of Information and Protection of Privacy Act,* Revised Statutes of Ontario 1990, Chapter F-31; *Municipal Freedom of Information and Protection of Privacy Act,* Revised Statutes of Ontario 1990, Chapter M-56; *Protection of Personal Information Act,* Statutes of New Brunswick 1998, Chapter P-19.1; *Freedom of Information and Protection of Privacy Act*, Statutes of Nova Scotia 1993, Chapter

In addition, Canada's 33-year-old federal *Privacy Act*[20] deals with personal information that is in the custody and control of the federal government.

1.1.1 Privacy and the Canadian Charter of Rights and Freedoms

What is the Canadian Charter of Rights and Freedoms*?*

The fundamental values of Canadians are reflected in the *Canadian Charter of Rights and Freedoms* ("the *Charter*"). The *Charter* was passed in 1982. It is part of the Constitution of Canada and can only be changed by an amendment to the Constitution. It is very difficult to make formal amendments to the Constitution. For this reason, it is a very powerful document.

Section 52 of the Constitution states that "the Constitution of Canada is the supreme law of Canada and any law that is inconsistent with the provisions of the Constitution is, to the extent of the inconsistency, of no force or effect". This statement makes it clear that the Charter is the supreme law of the land, and any law that contradicts the Charter is invalid. Of all the human rights legislation in Canada, the Charter is the most important.

What does the Charter do?

The Charter guarantees certain rights and freedoms.

5; *Freedom of Information Act*, Revised Statutes of Newfoundland 1990, Chapter F-25; *Access to Information and Protection of Privacy Act* Statutes of Northwest Territories 1994, Chapter 20 (also applies in Nunavut); *Access to Information and Protection of Privacy Act*, Revised Statutes of Yukon 2002, Chapter 1; Freedom of Information and Protection of Privacy Act, Statutes of Prince Edward Island, 2002, Chapter F-15.01. Prince Edward Island was the last jurisdiction to enact a privacy law. It enacted its *Freedom of Information and Protection of Privacy Act* on November 1, 2002.

[20] *Privacy Act*, Revised Statutes of Canada 1985, chapter P-21 (hereinafter "PA").

- A right is a legal claim to something that the state must grant and that can be enforced by a court.[21] For example, when you are arrested, you have the right to a lawyer.
- A freedom is an opportunity to do something without interference from the state. For example, we have the freedom to practice our choice of religion.

All of our rights and freedoms are limited by the need to protect our democracy society. For example, the right to freedom of expression under the *Charter* may be limited by hate laws, by obscenity laws, by anti-discrimination laws or by civil limits on our rights such as tort liability for defamation. Some of these limits are discussed below.

To whom does the Charter *apply?*

Before deciding whether a right has been violated it must first be determined if the *Charter* covers the situation. The *Charter* applies to actions of the government at all levels. So, the situation must be one where some official or law operating with government authority has violated a right. Section 32 states that the *Charter* applies to Parliament, to federal and provincial legislatures and to federal and provincial governments. "Provincial governments" has been interpreted to include municipalities, public schools and school boards.

The *Charter* does not cover private relations between individuals. Private relations are covered by provincial human rights codes.

What kinds of rights and freedoms does the Charter of Rights *protect?*

The following rights and freedoms are guaranteed by the *Charter:*

1. Fundamental Freedoms (Charter Section 2)

- freedom of conscience and religion;
- freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
- freedom of peaceful assembly; and
- freedom of association.

[21] C. Coombs, & J. Coombs, *Law, Fundamental Rights and Freedoms* (Toronto: IPI Publishing Ltd.) at 32.

Without the right to freedom of religion and freedom of expression, a person might be persecuted for belonging to an unpopular religious group or for speaking out against the government. For example, in 1933, Quebec passed a by-law prohibiting Jehovah's Witnesses from distributing their literature without permission of the police department. Today, this would not be permitted under the *Charter*.

Freedom of expression, thought, belief and opinion is a freedom that Canadians have enjoyed for many years. We have the right to speak out on issues without fear of repercussion. This right does not exist in all countries. In some countries, people who criticize the government are jailed or tortured.

Freedom of assembly and freedom of association means that we can belong to any group, join trade unions and gather in peaceful groups without fear of being penalized by the government.

2. Democratic Rights (Charter Sections 3 to 5)

- the right to vote;
- the right to require the state to hold an election at least every five years; and
- the right to seek political office.

The right to vote is a right many Canadians have enjoyed for many years. However, in the past, the government has denied some groups this right. For example, Canadians of Japanese and Chinese origin were denied the right to vote until after World War II. Aboriginals were denied the right to vote until 1960 and women were not permitted to vote in federal elections until 1918.

There are still some restrictions on the right to vote. People under the age of eighteen are not permitted to vote. Only Canadian citizens can vote.

3. Mobility Rights (Charter Section 6)

- the right to enter, remain in and leave Canada;
- the right to move and take up residence in any province; and
- the right to pursue the gaining of a livelihood in any province.

This part of the *Charter* confirms the right of Canadians to move and seek work in other provinces. This right is not without limits. For example, if you are a member of a certain profession you may have to pass a test based on that province's standards before you can practice. Mobility rights are guaranteed only to Canadian citizens.

4. Legal Rights (Charter Sections 7 to 14)
These include:

- the right to life, liberty and security of the person; and
- the right to a fair trial when charged with a crime.

These are extremely important sections of the *Charter*. Without these sections the authorities could put you in jail without a reason, deny you legal counsel or deny you the right to a fair trial.

5. Equality Rights (*Charter* Section 15)

- the right to equality before the law, and the right to the equal protection and benefit of the law without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

This section guarantees equality to individuals regardless of race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.

Does the Charter *expressly protect privacy?*

No. Although several sections of the *Charter* have been found by the courts to require that individual privacy rights are protected, the *Charter* does not explicitly say that Canadians have a right to privacy.

Is privacy protected under the Charter *in other ways?*

Yes. The courts have interpreted various rights provided in the *Charter* as requiring protection of the right to privacy. These include:

- The right to life, liberty and security of the person (section 7);
- The right to be free from unreasonable search and seizure (section 8);
- The freedom of thought, opinion and belief (section 2);
- The right to consult legal counsel in private (section 10);

- The right not to incriminate oneself (sections 11 and 13); and
- The right to equality (section 15(1)).

The Supreme Court of Canada has recognized a constitutional right to privacy in these sections that is at the very core of liberty in Canadian society and is rooted in individual autonomy and dignity.[22]

What are some examples of situations where the Charter *right to privacy is important?*

- **Search and seizures by the police:** The Supreme Court of Canada said that a major purpose of the protection against search and seizure in section 8 is the protection of the privacy of the individual. The Court indicated that people have a reasonable expectation of privacy when interacting with the government. In *R v Dyment*, which was decided before amendments to the *Criminal Code* dealing with blood samples, the Supreme Court of Canada said that section 8 was violated when a blood sample drawn from an emergency patient without his consent or knowledge was provided to a police officer for investigation purposes. **(These matters are discussed in more detail in Chapter 4: Searches.)**
- **Surveillance by the police:** In some situations, individuals have a reasonable expectation of privacy and surveillance is considered unconstitutional (a violation of the *Charter*). An example might be the unauthorized videotape surveillance of a hotel room. **(These matters are discussed in more detail in Chapter 3: Surveillance.)**
- **Private choices:** The right of people to choose where to live is part of our right to enjoy individual dignity and independence or liberty. The Supreme Court of Canada said that an employer requiring a person to live in a certain place violated privacy rights under the *Charter* section 7.
- **Counselling records:** The right of accused persons to fully defend themselves must be balanced against the privacy rights of complainants who seek counseling. For example, courts need to weigh carefully whether they can order a helping professional to release the counseling records of a person who is a witness in a sexual assault case (This issue is discussed in more detail below).

[22] Craig, page 355 at note 79.

How does the court balance our right to privacy with other Charter *rights?*

As noted above, in a criminal matter, when requesting the complainant's counseling records, the accused person's right under the *Charter* to fully defend him/herself must be balanced against the privacy rights of the complainant(s). This issue has arisen recently in cases of sexual assault under the *Criminal Code*. Defence lawyers hoping to assist their clients applied for access to complainant's counseling, school, employment or other records in the possession of therapists or other third parties. Third parties and complainants objected on the basis that revealing the records violated the privacy rights of the complainant.

Originally, the *Criminal Code* did not deal with these types of requests and the Supreme Court of Canada was asked to weigh out the two competing values—the privacy of the complainant and the accused person's right to a full defence. In *R v O'Connor*,[23] the Court set down guidelines that sought to balance both rights. The court created a two-step process, including the third party, the complainant and the accused. The process involved the judge separately analyzing the documents to determine if they were relevant. Both the accused person's right to a full defence and the complainant's right to privacy were to be balanced by the judge.

Later, Parliament amended the *Criminal Code* to provide for a process that reflected the *O'Connor* decision. These amendments were challenged by the accused in *R v Mills*,[24] as improperly balancing the competing *Charter* rights of privacy, full answer and defence and equality. In response, the Supreme Court of Canada held that the *Criminal Code* process for production of private third party records did not violate *Charter* section 7 (security of the person) nor section 11(d) (right to a fair trial). The Supreme Court noted the fundamental importance of privacy in a democratic society and emphasized that privacy was necessary in the case of healing relationships. The societal interest in encouraging full and frank counseling in cases of assault was significant. The Court also noted that one *Charter* right does not trump another *Charter* right—*Charter* rights have to be looked at and weighed in context.

---

[23] *R v O'Connor*, [1995] 4 Supreme Court Reports 411.
[24] *R v Mills* (1999), 180 Dominion Law Reports (4th) 1 (SCC).

What can I do if my Charter *right to privacy is violated?*

If you as an individual feel that the government has violated your rights, you need to show in court that the law somehow violates or contradicts the *Charter*.

What happens after I show that my right to privacy has been violated?

Once it has been proven that a *Charter* right has been violated, the courts must then determine if the law is justified in a free and democratic society. Section 1 of the *Charter* is used by the courts to balance the right or freedom of the individual against the purpose and objective of the law. The government may rely on section 1 as a defence where its actions have been found to violate the *Charter*.

More specifically, the balancing test done in section 1 of the Charter is referred to as the "proportionality test". The *Charter* gives Parliament and the Provincial Legislatures the right to restrict our rights in certain cases. Section 1 declares that the *Charter* "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." In other words, with rights come responsibilities. For example, although we have freedom of expression, Parliament has specified certain limits on this such as censorship of certain movies.

Oakes test

The court has developed a test to decide what is a "reasonable limit" that can be "demonstrably justified in a free and democratic society." The test is called the "Oakes test" and was developed in a Supreme Court of Canada case called *The Queen v Oakes*.[25] **First**, before applying the test the Court must look at the government's goal in passing the law (i.e., the problem the government wants to solve). This goal must be so important that it is permissible to take priority over a right that is protected in the *Charter*. The more serious the violation, the more important the goal has to be to in order to give good reason for the violation.

Second, the court will examine whether the methods are reasonable and proven to be necessary. This is called the "proportionality test". The proportionality test involves three components. First, the court determines if the legislation is connected to the goal of the

[25] *R v Oakes* (1986), 24 Canadian Criminal Cases (3d) 321 (SCC).

government. Second, the way that the government has chosen to achieve its goal must violate the *Charter* rights as little as possible. Third, there must be balance between the consequences of the limiting measure and the goal of the government in passing the law.

Example

Suppose that an artist created a picture that the police consider to be obscene. In order for a *Charter* challenge to be started, the artist must first be charged under the appropriate *Criminal Code* section. The artist could then challenge the *Criminal Code* section by saying that his freedom of expression is being unreasonably limited by the charge. The government will say that no right or freedom has been violated or that there is a limitation but it is reasonable and justified.

The court looks at two things: first, whether the law that applies is an unreasonable limitation and second, whether the artist's piece of work is obscene. If the limitation is unreasonable, it is irrelevant whether or not the court believes that the work in question is obscene.

If the court finds that this section unreasonably limits the right to freedom of expression then it will be of no "force or effect". This means that the law no longer applies to Canadians.

What can a court do if it finds that the law violates the **Charter** *and is not a reasonable limitation on my freedom?*

The *Charter* allows courts to declare the law of "no force and effect".

- Courts can strike down the law if it is found to be inconsistent with the *Charter*. This means that the law is no longer valid.
- Courts can sever the law. Severance is appropriate when only part of the law is unconstitutional. A court may say that only the bad part of the law should be struck down or severed from the good part.
- Courts can read in new words to a law, which means that even though the words are not written, the law should be read as if they were. For example, in the

Vriend[26] decision the court said that the words "sexual orientation" should be read in to the Alberta *Individual's Rights Protection Act* (now the *Human Rights Act*).

- Courts can read down the law. Reading down should not be confused with reading in. "Reading down" the law means that the Court gives an interpretation to certain words in the law that makes it comply with the Charter. This specific reading of the words by the court applies even though the words may be capable of other meanings.
- Courts can also provide other remedies that are fair in the circumstances. Some possibilities include: excluding evidence, dismissing charges, quashing a search warrant or awarding damages to someone whose *Charter* rights have been violated. These remedies are provided in *Charter* section 24.

What is the "notwithstanding clause"?

Section 33 is one of the most controversial sections in the *Charter*. It is commonly referred to as the "notwithstanding clause." It allows provinces to override the *Charter*. This can be done when the law specifically states it is to be exempted from one or more of the *Charter* sections. For example, in 1989, Premier Bourassa of Quebec used the clause to override a decision of the Supreme Court of Canada which set aside a law requiring signs displayed on the outside of public buildings be in French only.[27]

1.1.2 FEDERAL AND PROVINCIAL PRIVACY LEGISLATION

FEDERAL PRIVACY ACT

How does Canada's privacy legislation work?

The protection of our privacy when we deal with the government of Canada is governed by the *Privacy Act* ("PA"),[28] and the regulations passed under this Act. The federal Privacy Commissioner oversees the implementation of the PA. Federal legislation has been in place for several years, resulting in numerous court decisions that interpret various sections. This

[26] *Vriend v Alberta* (1998), 156 Dominion Law Reports (4th) 385 (SCC), overturning, [1996] 8 Western Weekly Reports 405 (Alta CA), which had overturned (1994), 18 Alberta Law Reports (3d) 286 (QB).
[27] *Ford v Attorney General Quebec* (1988), 2 Supreme Court Reports 712.
[28] Revised Statutes of Canada, 1985, chapter P-21 (hereinafter "PA").

legislation deals with the collection, disclosure and correction of personal information held by the federal government.

The purposes of the PA are:

- to protect the privacy of individuals regarding their personal information held by government institutions; and
- to provide these individuals with a right of access to that information.[29]

What is "personal information"?

The PA defines "personal information" as information recorded in any form about an identifiable individual, including:

- his or her race, national or ethnic origin, colour, religion, age, marital status;
- his or her education history, medical history, criminal history, employment or financial history;
- an identifying number assigned to an individual;
- his or her address, fingerprints or blood type;
- the personal opinions of the individual (with some exceptions);
- private and confidential correspondence;
- other people's opinions about the person; and
- the person's name.[30]

When the government is dealing with the use or disclosure of personal information, or access to another person's information under certain sections of the PA, "personal information" ***does not*** include: information about government employees, including their title, business address and telephone number, salary range or personal opinions given in the course of employment; information about individuals who perform contractual services for the government; information about certain financial benefits received by an individual; and information about an individual who has been dead for at least 20 years.[31]

---

[29] PA, section 2.
[30] PA, section 3.
[31] PA, section 3.

What types of information are not covered by the Privacy Act*?*

The PA specifically excludes some records. These records may be available from government institutions, but you cannot use the PA to obtain them. They include: published material; public library or museum materials; and materials placed by the public in the National Archives, the National Library, the National Gallery, the Canadian Museum of Civilization, or the National Museum of Science and Technology.[32]When can the Canadian government collect personal information about me?

Collection of Personal Information

The PA deals with the collection and sharing of personal information. The PA says that the government cannot collect personal information about you unless the information relates directly to an operating program or activity of the government institution.[33]

Purpose and Legal Authority for Collection

When it is collecting personal information from people, the government must usually tell people the purpose for which the information is being collected.[34]

Except in rare cases, the government is required to collect personal information from the person concerned, and not from anyone else. [35] The personal information collected is to be used only for the purpose for which it was collected, or a use consistent with that purpose.[36] Information may also be used by the government for some of the purposes that are outlined below under "Disclosure of Personal Information".

When can the Canadian government disclose personal information about me?

The PA allows disclosure of personal information if the person consents.[37] The PA allows disclosure of personal information without consent to someone other than the person it concerns in very limited circumstances. Situations when the PA allows disclosure of personal information include:

---

[32]PA, section 69.
[33]PA, section 4.
[34]PA, subsection 5(2).
[35]PA, subsection 5(1).
[36]PA, section 7.
[37]PA, subsection 8(1).

- when the individual consents to its release;
- for the purpose for which the information was obtained, or a use consistent with that purpose;
- when a federal law authorizes the disclosure;
- to comply with a court order, subpoena or warrant;
- to the Attorney General of Canada for use in legal proceedings involving the government;
- to the investigative bodies listed in the regulations[38] in order to enforce provincial or federal laws or to conduct investigations;
- to a provincial, federal or international government or institution for law enforcement reasons;
- to a member of Parliament in limited circumstances;
- for internal audit purposes;
- to the National Archives of Canada;
- for statistical or research purposes, under specified circumstances;
- in order to assist in researching aboriginal land claims;
- to collect a debt owed to the federal government; and
- in the public interest (in some circumstances).[39]

Personal information may be released for any purpose where the government decides:

- the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
- disclosure would clearly benefit the individual to whom the information relates.[40]

Does the Canadian government have any restrictions on how it stores or disposes of my personal information?

Yes. The PA sets out requirements for the storage and disposal of personal information.[41]

---

[38] *Privacy Regulations*, section 5, Schedule II.
[39] PA, subsection 8(2).
[40] PA, paragraph 8(2)(m).
[41] PA, sections 6, 11, and 77.

What if I want to correct personal information held by the federal government?

A government institution must make efforts to ensure the completeness and accuracy of personal information it relies upon to make decisions that directly affect you. If you discover that an error has been made in the information that the government institution has about you, you should notify the institution in writing. You may use the "Record Correction Request Form" provided by the government. The government institution may correct the information in the record, or, at a minimum, must include a notation in the record that you sought a correction. If you are unhappy with the decision not to change the information in the record, you may complain to the Privacy Commissioner.[42]

If a correction is made, the government institution must notify you that your requested correction has been made to your record.[43]

How can I gain access to my personal information held by the Canadian government?

The process for obtaining personal information from the Canadian government may be summarized as follows:

Step One: Determine which government institution should receive the access to personal information request.

Obtain a copy of *Info Source (Sources of Federal Government Information)* from a public library, constituency office or federal government office. *Info Source* is also available on the internet through the privacy commissioner's web site. [44]

- Find out which data bank(s) would likely contain the required information.
- Determine the name, address and phone number of the Access to Information and Privacy Coordinator for that particular data bank.

Step Two: Call the Access to Information and Privacy Coordinator to see if you can get the information without filing a formal information request.

---

[42] PA, subsections 6(2) and 12(2); *Privacy Regulation*, section 11.
[43] *Privacy Regulation***,** subsection 11(2).
[44] See: http://infosource.gc.ca/

Step Three: To proceed with a formal request, fill out the appropriate form and send in the application fee.

- Fill out a *Personal Information Request Form,* indicating specifically the records that are requested. Ask for the opportunity to clarify the request, if necessary. Ask to be informed about additional fees before the request is filled.
- Alternatively, write a letter to the appropriate Access to Information and Privacy Coordinator stating your specific request. Include your name, address and telephone number. Indicate whether you are a Canadian citizen, permanent resident, an "individual present in Canada" or a "corporation present in Canada". State whether you prefer to receive copies of the document or examine them. Indicate which official language you would like used in processing your request.
- If you are visually impaired or have a hearing disability, you may ask to receive the record in a suitable format.
- There is no fee payable for a request for personal information.

Step Four: Wait for a Response from the Government Institution

Possible responses by the head of the government institution include:

- a reply within 30 days granting access to the information or setting out the estimated costs of proceeding with the request;
- a transfer of the request to another government institution, which must reply within 30 days from the date the first government institution received the request;
- notification that an extension of the 30 day time limit is required; or
- a refusal of access to some or all of the record based on one or more discretionary or mandatory exemptions (e.g., it is third party information, etc.).

The requester then may review the response to determine whether a complaint to the Privacy Commissioner is necessary.

Step Five: If access is denied, or if there are other difficulties, complain to the Privacy Commissioner.

- You have one year after you receive the access decision from the government institution to appeal to the Privacy Commissioner.

- The Privacy Commissioner can receive and investigate complaints from persons who have been refused access to a record or part of it; from persons who consider that the time limit for an extension is unreasonable; and for other reasons.
- Write a letter to the Privacy Commissioner in which you outline your request for a review. Include your name, address, telephone number, reason for requesting a review, and the government institution to which your request was originally made. Enclose a copy of your original request, if available.

Step Six: The Privacy Commissioner can make recommendations to the head of the government institution regarding the access to information request.

- The Privacy Commissioner must report the results of his or her investigation to the complainant.
- The head of the government institution need not grant access to the information, even if the Privacy Commissioner so recommends.

Step Seven: If necessary, appeal to the Federal Court

- The requester, once he or she has received an answer to the complaint, can appeal a decision of the head of the government institution to the Federal Court within 45 days after receiving the results of the investigation of the Privacy Commissioner. The Commissioner may also initiate an appeal on behalf of an applicant. A third party may also apply to the court within 20 days after the head of the government institution gives notice of its decision to disclose the record.
- The Federal Court may order disclosure of the record. This order must be obeyed by the head of the government institution.

Step Eight: If necessary, there is a further appeal to the Federal Court of Appeal and, under certain circumstances, yet a further appeal to the Supreme Court of Canada.

Who can apply for access to personal information?

Access to personal information under the PA is available to individuals who are Canadian citizens or permanent residents, prison inmates, or individuals who are "present in Canada".[45]

Can I apply for access to personal information on behalf of another person?

To apply for personal information on behalf of another person, you will have to show that you are authorized to do so. One of these documents will be required:

- written permission from the individual;
- proof that you are a deceased person's representative seeking information relating to the estate; or
- proof that you are a person's guardian or trustee.[46]

What is Info Source and where can I access it?

Once a year, the Treasury Board publishes a catalogue (*Info Source (Sources of Federal Government Information)).* This publication:

- describes the organization and responsibilities of each government institution;
- describes all classes of records under the control of each government institution;
- describes all manuals used by employees of each government institution; and
- provides the title and address of the appropriate officer for each government institution to whom requests for access to records should be sent.

Info Source also contains a list of personal information data banks as required under the PA. Generally, privacy forms may be found with *Info Source.*[47].

Info Source is also available on the internet through the privacy commissioner's web site.

---

[45] PA, subsection 12(1); *Privacy Regulations*, Extension Order No. 1, section 2; Extension Order No. 2, section 2.
[46] *Privacy Regulation*, section 10.
[47] PA, section 11.

How do I know if I can gain access to my personal information from a particular government department?

The PA provides that personal information may be obtained from "government institutions". Requests for access to personal information may only be made to government institutions listed in the Schedule to the PA.[48]

What form do I fill in to start the process of accessing my personal information?

You may request access to your personal information under the PA by filling out a form called the "Personal Information Request Form".[49]

What happens after I make my access to personal information request?

The government institution has 30 days to respond to your request. [50] You may be asked to permit an extension. If the request is for access to non-personal information, the extension may be for a "reasonable period". If the request is for access to personal information, the extension will be for 30 days or a "reasonable period". If the government institution requests an extension, it will tell you why they want an extension. If you do not think that an extension is acceptable, you may appeal to the Privacy Commissioner.[51]

If I am able to get access to my personal information, will I be sent a copy of the record?

If your access request is successful, the government institution will tell you when you will receive copies or be able to review the records you are seeking. If the information you are seeking is your own personal information, you will have to show that you are the person named in the records.[52]

Although you may prefer to examine the record at the office of the government institution, perhaps to avoid copying charges, the government institution may insist on providing a copy of the record instead. The government institution may refuse to let you see the original record because giving access in that way would unreasonably interfere with government

---

[48] PA, section 3.
[49] PA, subsection 13(1); *Privacy Regulation*, subsection 8(1).
[50] PA, section 14.
[51] PA, section 15.
[52] PA, section 17; *Privacy Regulation*, subsection 8(2).

operations. Another reason to refuse to let you see the original record is to ensure that you do not see information that you are not allowed to have access to.[53]

Can I get my personal information in alternative formats?

If you are visually impaired or hearing impaired, you may request to receive the record in an alternative format, such as in Braille, in large print or on a tape.[54]

You may specify whether you would like the information to be provided in English or French.[55]

What is the best way to phrase my access to personal information request?

First, consider the scope of your request. The Access to Information and Privacy Coordinator may have some good suggestions for ways to phrase your question to obtain the information you want.

However, you should remember that the government has expressed concerns about the costs of responding to information requests. Coordinators are expected to discuss with applicants ways to narrow their requests, particularly when the request is rather vague or broad.

You should be as specific as you can about the information you are seeking. The request has to be specific enough so that the government institution can identify the records you seek.[56]

There are no provisions in the *Privacy Act* for the transferring of a request if it is sent to the wrong government institution.

Are there some types of personal information exempt from disclosure?

Yes. There are some types of information that the head of the government institution must not disclose. These are called "mandatory exemptions". Even if you are applying for personal information from a government institution that is listed in the Schedule, the government institution is forbidden to give you the following:

---

[53] PA, subsection 16.
[54] PA, subsection 17(3).
[55] PA, subsection 17(2).
[56] PA, paragraph 12(1)(b).

- information obtained from other governments (e.g., foreign, provincial or municipal);[57]
- information about individuals other than the requester;[58]
- information about investigations by the RCMP on behalf of a province,[59]
- information that was obtained or created during an investigation by the Privacy Commissioner,[60]
- information that was obtained or created during an investigation by the Public Sector Integrity Commissioner,[61]
- information that was created for the purpose of making disclosure under the *Public Servants Disclosure Protection Act,*[62] and
- information that was obtained or created by the Secretariat of the National Security and Intelligence Committee in the course of assisting the National Security and Intelligence Committee of Parliamentarians in fulfilling its mandate.[63]

The government institution has some discretion over other exemptions.

The head of the government institution is allowed to decide whether or not to give you access to certain information. These discretionary exemptions include:

- information held in an exempt data bank;[64]
- information related to federal-provincial government affairs;[65]
- information about international affairs and defence;[66]
- law enforcement and investigations;[67]
- security clearance investigations;[68]
- prisoner's files, if disclosure might affect the person's release or rehabilitation, or if it might reveal a confidential source;[69]

---

[57] PA, section 19.
[58] PA, section 26.
[59] PA, subsection 22(2).
[60] PA, subsection 22.1(1).
[61] PA, subsection 22.2.
[62] PA, subsection 22.3.
[63] PA, subsection 22.4.
[64] PA, section 18.
[65] PA, section 20.
[66] PA, section 21.
[67] PA, subsection 22(1).
[68] PA, section 23.
[69] PA, section 24.

- information, where disclosure could reasonably expected to affect public health or safety;[70]
- privileged legal advice provided to the government;[71] and
- medical records of the requester, if disclosure is not in the best interests of the individual.[72]

Who makes the decision about whether I can get access to my personal information?

The person who makes the final decisions about access to personal information in a government institution is the "head of the government institution". Usually, the head of the government institution is the Minister responsible for that body. Some government institutions have a president or other CEO who is the head of the institution. Although the head of the institution makes the final decision about access for that body, the Commissioner has the authority to review these decisions. *Info Source* lists the heads of all government institutions.[73]

What is the role of the Access to Information and Privacy Coordinator?

Each government institution has an Access to Information and Privacy Coordinator. *Info Source* provides their telephone numbers and titles.[74] A list of Access to Information and Privacy Coordinators can also be found at: http://www.tbs-sct.gc.ca/atip-aiprp/apps/coords/index-eng.asp.

The Coordinators oversee the application of the PA in their own departments. The requests for information are sent to the Coordinators, who decide which branch of government can respond to the request, and whether the information requested is accessible or not. Coordinators usually manage the request process from start to finish. However, the final decision-maker is the head of the government institution. Before you prepare your information request, you may wish to contact the coordinator to discuss what information you are seeking.

---

[70] PA, section 25.
[71] PA, section 27.
[72] PA, section 28.
[73] PA, section 3 "head"; section 73.
[74] PA, paragraph 11(1)(b)(ii).

The information you are seeking may have been made public by the government already, so you can obtain access without a formal request. The coordinator may even be able to provide the information without a formal request, or at least tell you where you might locate the information.[75]

Is there any fee charged to me for applying for access to personal information?

No.

What if the government institution refuses to grant access to my personal information?

If the government institution informs you that you have been refused access to requested records, the institution will give you reasons for the refusal. You will be informed that you have the right to challenge this decision to refuse access. The Information Commissioner or the Privacy Commissioner will review this decision.[76]

Even if you are refused access, the government institution may inform you whether a record exists or not. However, the government institution is not required to tell you whether a record exists.[77]

If you do not hear anything from the government institution within the 30 day period or any extended period that you have been notified about, you may treat the non-response as a denial of access.[78]

Can I appeal a decision to refuse access to my personal information?

Yes. The Privacy Commissioner can receive complaints about access to personal information, or the collection, retention or disposal of personal information.[79] There is no time limit for making a complaint to the Privacy Commissioner.[80] One person may complain

[75] PA, subsection 69(2).
[76] PA, section 16.
[77] PA, subsection 16(2).
[78] A, subsection 16(3).
[79] PA, subsection 29(1).
[80] PA, subsection 29(2).

on behalf of another person, or the Commissioner may initiate an investigation on his or her own.[81]

Complaints to the Privacy Commissioner must be in writing. A person wishing to appeal a decision may write a letter to the Privacy Commissioner (for decisions about personal information). Include your name, address, telephone number, the reason for requesting a review and the government institution to which your request was originally made. Enclose a copy of your original request.[82]

In making an appeal decision, what powers does the Privacy Commissioner have?

The Privacy Commissioner does not have the authority under the legislation to make orders that the government has to follow. After the Commissioner receives a complaint, it is investigated by an investigation officer. The Commissioner has broad powers of investigation. For example, they or their staff can enter government institutions and examine or obtain copies of records. They can compel persons to appear before them and receive evidence from them.[83]

Every investigation is conducted in private. The head of the government institution and the person who made the complaint are entitled to be heard by the Commissioner.[84]

The Commissioner must report any findings or recommendations to all concerned parties (for example, the person complaining and the head of the government institution). However, these recommendations need not be followed by government institutions.[85]

---

[81] PA, subsection 29(3).
[82] PA, section 30.
[83] PA, section 34(1)(a).
[84] PA, subsections 33(1) and (2).
[85] PA, subsections 35(1) and (2).

Can I appeal a decision of the Privacy Commissioner?

If you have been refused access to personal information, and if you have received an answer to a complaint about this refusal from the Privacy Commissioner, you may apply to the Federal Court, Trial Division, for a review of the decision.

You must apply to the Court for this review within 45 days after you receive the results of the Information or Privacy Commissioner's investigation.[86]

After the review hearing, the Court can order the government institution to release part or all of the record. Under the PA, the Court can order the government to remove records from the exempt banks.[87]

Generally, with a few exceptions, the review hearings at the Federal Court Trial Division are conducted in private.[88]

The decision of the Federal Court Trial Division may be appealed to the Federal Court of Appeal.[89]

In limited circumstances, such as if the Supreme Court of Canada grants leave to appeal, the matter may be appealed further.

There are some circumstances in which the PA does not provide for an appeal to the Federal Court. For example, you may not agree with the Privacy Commissioner's recommendations and the government institution's response to recommendations about matters other than a request for access to personal information (for example, decisions about disclosing or collecting personal information). Or, you may be concerned about the fact that the PA does not apply to a particular government institution. These issues cannot be appealed to the Federal Court. The only possibility you have is to apply to the Federal Court for judicial

---

[86] PA, section 41.
[87] PA, section50.
[88] See, for example PA, subsection 51(2).
[89] *Federal Court Act,* RSC 1985, c F-7.

review. An application for judicial review is used to challenge the fairness and legality of the process.[90]

What is the role of the Privacy Commissioner?

The Privacy Commissioner is responsible for compliance under the PA.

While recommendations made by the Commissioner to the heads of government institutions need not be followed, the opinions of the Commissioner are generally seriously considered. When conducting investigations, the Commissioner has significant powers.

The Privacy Commissioner is independent of the government of the day. He/she is appointed by the House of Commons and the Senate and report to Parliament through the Speaker, and not through a Minister. A Commissioner is appointed for a seven year term. [91] The address and other information about the Commissioner's offices are set out below.

Where can I get more information about Canada's privacy legislation?

The office of the federal Privacy Commissioner may be contacted at:

30, Victoria Street
Gatineau, Quebec
J8X 0A8
Phone **(819) 994-5444**
Toll-free 1-800-282-1376
Fax **(819) 994-5424**
TTY: (819) 994-6591
Web site: https://www.priv.gc.ca/en

PROVINCIAL PRIVACY LEGISLATION

Do all provinces and territories have privacy legislation?

Every province and territory in Canada has some form of access to information and protection of privacy legislation.[92] The legislation varies from province to province, but the rules regarding personal information are very similar in several. One significant difference is

[90] *Federal Court Act*, RSC 1985, c F-7.
[91] PA, sections 53(2).
[92] See previous note under section 1.1.

the role of the Commissioner. In some provinces and territories, the Commissioner has the authority to make decisions about access to information and privacy issues that government departments have to follow. In other provinces, he or she can only make recommendations that the government may or may not follow. The federal jurisdiction (discussed above) is an example where the Commissioner can only make recommendations to the appropriate government department. The access to information system in Alberta (discussed below) is an example of a province where the Commissioner can make decisions that the government has to follow.

The privacy legislation of all of the provinces and territories is listed in the appendix.

How does Alberta's privacy legislation work?

Access to information and protection of privacy in Alberta are governed by the *Freedom of Information and Protection of Privacy Act*[93] [the "FOIP Act"] and the regulations made under this Act. The stated purposes of the FOIP Act are:[94]

> 1. To allow any person the right to access records in the control of the government, subject to certain limited exceptions;
> 2. To regulate the manner in which the government collects, uses and discloses personal information in its custody;
> 3. To allow individuals the right to access information about themselves held by the government;
> 4. To allow individuals to request corrections to personal information held by the government; and
> 5. To provide for an independent review of decisions made by the government under this Act and for the resolution of complaints made under the Act.

What organizations are covered by the FOIP Act?

This legislation applies to government bodies in Alberta. These include: departments, branches or offices of the Government of Alberta; educational bodies, such as universities and school boards; health care bodies, such as hospitals, some nursing homes, and other regional health authorities; law enforcement bodies, such as city police departments; and local government bodies, such as cities and municipalities.[95]

---

[93] RSA 2000, c F-25.
[94] FOIP Act, section 2.
[95] FOIP Act, subsections 1(i) 1(j) and 1(p).

Municipalities (e.g., cities), schools, universities, police departments and health care bodies have been under the FOIP Act for only a few years. Each organization has its own special privacy issues and procedures. For example, in schools, one key issue is access to, collection of, disclosure of and correction of student records. Alberta Learning and various school boards have developed policies and procedures dealing with privacy issues. The following list of web sites provide some of the policies that pertain to the organizations listed above.

- City of Edmonton: https://www.edmonton.ca/city_government/city_organization/freedom-of-information-and-privacy.aspx
- City of Calgary: http://www.calgary.ca/CA/city-clerks/Pages/Freedom-of-Information-and-Protection-of-Privacy/Privacy-and-Access.aspx
- Calgary Board of Education: https://www.cbe.ab.ca/about-us/policies-and-regulations/freedom-of-information-and-protection-of-privacy-foip/Pages/default.aspx
- Alberta Education: http://education.alberta.ca/using/privacy.aspx
- University of Calgary: http://www.ucalgary.ca/hr/freedom_of_information_and_protection_of_privacy
- University of Alberta: http://www.ipo.ualberta.ca/

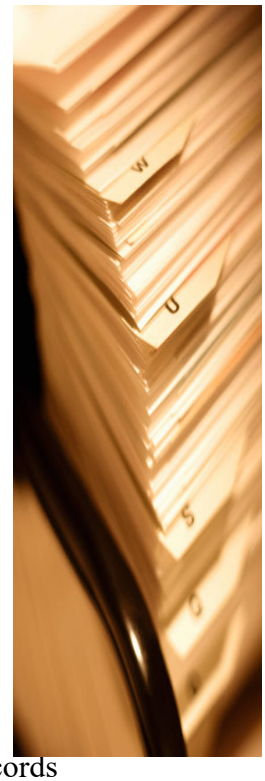
Although the FOIP Act applies to health care bodies, Alberta has separate legislation dealing with "health information", the *Health Information Act*.[96] Health information legislation is discussed below.

What is "personal information"?

The FOIP Act currently defines personal information as information about an identifiable individual, including:

[96] RSA 2000, c H-5.

- his or her name, home or business address, home or business telephone number, race, national or ethnic origin, colour, religious beliefs, political beliefs or associations, age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- health information about the individual, including information about a physical or mental disability ;
- educational, financial, employment, criminal history about the individual; anyone else's opinions about the individual; and
- the individual's personal opinions, except if they are about someone else.[97]



What kinds of personal information are held by the government?

Although the FOIP Act refers to "information" in its title, what the provincial government refers to are government **records.** The government provides copies of records in many different formats. Formats include: written, photographic, audiotapes, or electronic. They do not include software or any mechanism that produces records (e.g., computers).[98] The FOIP Act provides a list of the provincial government departments and other bodies whose records are accessible.[99]

You may obtain access to records in any format. However, the copying charges vary, depending upon the record's format. In the case of access to personal information, the government may only charge fees for copying the record if the copy charges will exceed $10.00[100]

The FOIP Act applies to government records that were created before or after the Act took effect.[101]

---

[97] FOIP Act, paragraph 1(n). This definition is likely to change because of technological and medical advances.
[98] FOIP Act, paragraph 1(q).
[99] *Freedom of Information and Protection of Privacy Regulation*, AR 186/2008, Schedule 1.
[100] *Freedom of Information and Protection of Privacy Regulation*, AR 186/2008, s 12, Schedule 2.
[101] FOIP Act, section 96.

What types of information are not covered by the FOIP Act?

In general, you will not be able to obtain records of Members of the Legislative Assembly or caucus offices of political parties. Records that have been created by or for an MLA are not accessible through the FOIP Act. Offices of MLAs are not included as "public bodies" that are subject to the Act.[102]

The FOIP Act specifically excludes some records. Thus, the FOIP Act does not apply to these records. For example, these records may be available from government bodies, but you **cannot** use the FOIP Act to obtain them. They include:[103]

- court records, other than court administration records;
- notes of a judge or someone in a judicial role;
- quality assurance records under the *Alberta Evidence Act*;
- some records held by Officers of the Legislature (e.g., the Ethics Commissioner);
- some archival records;
- post-secondary teaching and research materials;
- exam or test questions;
- prosecution records (if a prosecution has not been completed);
- personal records of a member of the Executive Council;
- health information;
- personal records of an appointed member of the governing body of a local public body or of an elected member of a local public body;
- records created by or for a Member of the Legislative Assembly (MLA), a cabinet minister, or a chair of a Provincial agency;
- some records of the Speaker and MLAs held in the custody of the Legislative Assembly Office;
- information communicated between a cabinet minister and MLAs;
- information in registries; and
- some treasury branch and credit union records.

[102] FOIP Act, paragraph 1(p)(vii) and 1(p) (viii).
[103] FOIP Act, section 4.

When can the provincial government collect personal information about me?

The FOIP Act recognizes that provincial public bodies may need to collect personal information in order to provide various government services. However, any provincial public body subject to the FOIP Act that is considering collecting personal information (e.g., by introducing monitoring programs, such as video surveillance), must see if its particular set of circumstances meets one of the three legislated conditions under which a public body may collect personal information. Personal information may be collected by a public body if:

- there is specific legislation allowing the collection of the personal information sought;
- the personal information is being collected for the purpose of law enforcement; or
- the public body can show how the personal information being sought directly relates to and is necessary for the public body's operating program or activity.[104]

Once it has been determined that a public body can collect personal information, the FOIP Act requires that the public body inform the persons from whom the personal information is being collected of the purpose and authority for the collection. The public body must also supply a contact person's phone number where a person can get more information on the information collection program.[105]

The public body must collect personal information directly from the individual, except in circumstances like:

- when another method of collection was authorized;
- when the personal information can legally be disclosed from another public body's collection;
- when the information is collected in a health or safety emergency;
- when the information concerns an individual who is designated as an emergency contact;

[104] FOIP Act, section 33.
[105] FOIP Act, subsection 34(2).

- when the information is collected from published or other public sources for the purpose of fund-raising; when the personal information is collected for enforcement purposes or correctional services programs; or
- when the personal information is necessary for determining the eligibility of an individual to participate in or receive the benefits of a program or service from the government of Alberta;[106]

The public body collecting the information must make a reasonable effort to ensure that the information being collected is accurate and complete.[107]

The FOIP Act also has procedures for people to follow in order to request access to the personal information that has been collected about them or to request corrections to inaccurate information. The FOIP Act states that the personal information collected must be used for the purpose it was originally obtained or compiled for,[108] for other programs consistent with that original purpose,[109] or for research or statistical purposes.[110] (Each of these reasons is outlined in greater detail in the FOIP Act.) Personal information that is used to make a decision that directly affects an individual must be retained for at least one year.[111]

When can the provincial government disclose personal information about me?

The FOIP Act allows disclosure of personal information to someone other than the person it concerns in limited circumstances. These include:

- when the individual provides written consent for its release;[112]
- if the disclosure would not be an unreasonable invasion of another person's privacy;
- for the purpose for which the information was compiled or for a use consistent with that purpose;
- to comply with a federal or provincial law or a treaty;

[106] FOIP Act, subsection 34(1).
[107] FOIP Act, section 35.
[108] FOIP Act, section 39.
[109] FOIP Act, section 41.
[110] FOIP Act, section 42.
[111] FOIP Act, section 35.
[112] FOIP Act, subsection 39(1); *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, section 7.

- to comply with a court order;
- to an officer or employee of the public body or a Cabinet Member to perform his or her duties or to deliver a program or service;
- to enforce a legal right of the Alberta Government or a public body;
- to collect a fine or debt or for making a payment;
- to determine suitability or eligibility for a program or benefit;
- for audit purposes;
- to Members of the Legislative Assembly, under some circumstances;
- to the Provincial Archives of Alberta or other public body archives;
- to assist in a law enforcement matter;
- to inform the next of kin of the injury, illness or death of the individual;
- when the information has been in existence for 25 years or more and concerns an individual, under certain circumstances;[113]
- to medical or other experts like physicians, chartered psychologists or psychiatrists to determine if disclosure of information would be harmful to individual's safety, mental or physical health;[114]
- for use in legal proceedings which involve the Government or a public body;
- when the information is available to the public;
- for managing Government personnel;
- when dealing with persons who are in detention;
- to a relative of a deceased person;
- to avert or minimize an imminent danger to public health or safety;
- to avert or minimize a risk of harm to the health or safety of a minor;
- for research purposes, if stringent security constraints have been met;[115] and
- in some other limited circumstances.

[113] FOIP Act, section 43.
[114] FOIP Act, sections 40, 18; *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, section 6.
[115] FOIP Act, section 42.

What if the public body collects, uses or discloses my information in a way that concerns me?

An individual may ask the Commissioner for a review if he or she believes that there has been any violation of privacy rights in the collection or disclosure of personal information.[116]

Does the provincial government have any restrictions on how it stores my personal information?

The public body that collects personal information must ensure that the data in their custody is kept secure.[117] If a person's information will be used by the government to make a decision that directly affects that person, the government must make every reasonable effort to ensure the information is accurate and complete and must also retain the information for at least one year (except in limited circumstances).[118]

What if I want to correct personal information held by the provincial government?

A public body must make efforts to ensure the completeness and accuracy of personal information it relies upon to make a decision that directly affects you.[119] If you discover that an error has been made in the information that the public body has about you, you should notify the body in writing.[120] You may use a form provided by the government or you may write a letter. The public body may correct the information in the record, or, at a minimum, must include a notation in the record that you sought a correction. If you are unhappy with the decision not to change the information in the record, you may complain to the Information and Privacy Commissioner.

How can I gain access to my personal information held by the provincial government?

The following steps provide a summary of the access to information process in Alberta. Before an individual submits a request for access to personal information, it may be desirable to attempt to initiate an informal request for the information by contacting the appropriate government department ("public body") directly.

---

[116] FOIP Act, subsection 65(3).
[117] FOIP Act, section 38.
[118] FOIP Act, section 35.
[119] FOIP Act, section 35.
[120] FOIP Act, section 36.

Step One: Determine which public body should receive the access to information request.

- If desired, obtain a copy of the *Alberta Directory* from a public library or the Queen's Printer.[121]
- If possible, ascertain which data bank(s), register(s), file(s), or database(s) would likely contain the required information.
- Determine the name, address and phone number of the Freedom of Information and Privacy Coordinator ("FOIP Coordinator") for that particular public body.

Step Two: Call the FOIP Coordinator to see if you can get the information without filing a formal information request.

- This could save you copying charges.

Step Three: To proceed with a formal request, fill out the appropriate form. There is no application fee for a request for personal information.

- Fill out a *Request for Access to Information Form,* indicating specifically the records that are requested. Ask for the opportunity to clarify the request, if necessary.
- Alternatively, write a letter to the appropriate FOIP Coordinator stating your specific request. Include your name, address and telephone number. State whether you prefer to receive copies of the document or examine them.
- Alternatively, if you are visually impaired or have a limited ability to read or write in English, you may make an oral request to the FOIP Coordinator.
- There may be fees for copying personal information.

Step Four: Wait for a Response from the Public Body.

Possible responses by the head of the public body include:

- a reply within 30 days granting access to the information or setting out the estimated costs of proceeding with the request;

[121] Note: this directory has been replaced by a computerized catalogue.

- a transfer of the request to another public body, which must reply within 45 days from the date the first public body received the request;
- notification that an extension of the 30 day time limit is required; or
- a refusal of access to some or all of the record based on one or more discretionary or mandatory exceptions (e.g., it is third party information etc.).

The requester then may review the response to determine whether a complaint to the Information and Privacy Commissioner is necessary.

Step Five: If access is denied, or if there are other difficulties, request a review by the Information and Privacy Commissioner.

- You have 60 calendar days after you receive the decision from the public body to appeal to the Commissioner, who is an independent officer of the Legislative Assembly.
- The Commissioner can receive and investigate complaints from persons who have made access requests. The complaints may be about any decision, act, or failure to act of the head of the public body that relates to the request (for example, a decision not to release a record or part of it). A complaint may also be that a public body has improperly collected or used personal information.
- Complete and send to the Commissioner a "*Request for Review"* form. Alternatively, write a letter to the Commissioner in which you outline your request for a review. Include your name, address, telephone number, reason for requesting a review and the public body to which your request was originally made. Enclose a copy of your original request, if available.

Step Six: The Information and Privacy Commissioner may appoint a mediator to investigate and settle the complaint.

The mediator may be someone from inside the Commissioner's office. That person will try to facilitate a settlement. In many cases, a settlement is reached.

Step Seven: If the matter is not settled, the Information and Privacy Commissioner may conduct an inquiry.

- The review must be conducted within a 90 day time frame and all orders issued by the Commissioner are legally binding.
- The Commissioner's order may require a head of a public body to grant access, confirm the original decision made by the head of the public body, or enforce other provisions of the Act. A copy of the order may be filed with the Court of Queen's Bench. This makes the order enforceable under Alberta law.

Step Eight: The Commissioner's order is final.
Applicants have the right to judicial review by the courts if they believe that the appeal process was not conducted in a legally fair manner.

Who can apply for access to personal information?

You can obtain your own personal information, with some exceptions.[122] Generally, only an individual or his/her representative may apply for access to personal information.

Can I apply for access to personal information on behalf of another person?

Yes. To apply for personal information on behalf of another person, you will have to provide one of these authorizing documents:[123]

- written permission from the individual;
- proof that you are a guardian or trustee under the *Adult Guardianship and Trustee Act* who has been given the power to apply for access to personal information;
- proof that you have been designated as an agent and are authorized to apply under the *Personal Directives Act*;
- proof that you are a deceased person's representative seeking information relating to the estate;
- proof that you are the person's attorney acting under power of attorney; or
- proof that you are the recognized guardian of a minor child.

[122]FOIP Act, subsection 6(1), 6(2) and 6(3).
[123]FOIP Act, section 84.

What is the Alberta Directory and where can I access it?

The ***Alberta Directory***[124] lists all of the government departments and other bodies subject to the FOIP Act. This directory provides a list of the type of information held by each branch of government.[125] The directory also includes a copy of the FOIP Act, sample forms that you can photocopy, information on how to make an information request or a correction request, and information on how to apply to the Commissioner for a review of a decision. The provincial government provides a copy of this directory to every public library in Alberta. It is also available in government offices and MLA offices. Copies can be purchased from the Queen's Printer (addresses are below). It is likely that this will be replaced by computer catalogues.

In the Alberta Directory, you will find that each branch of government has listed the information banks that include personal information.

How do I know if I can gain access to my personal information from a particular government department or agency?

The *Freedom of Information and Protection of Privacy Regulation* contains a list (Schedule 1), which sets out the public bodies from which information may be obtained.

Are there some types of personal information excepted from disclosure?

Yes. Even if you are seeking information from a public body that is covered by the Act (that is, one listed in Schedule 1), the public body is forbidden to give you the following:

- commercial information of a third party (trade secrets) including information collected on a tax return;[126]
- personal information about a third party (see "Third Party Notice");[127]
- law enforcement information, if a federal law deems it an offence to release the information;[128] and
- Cabinet or Treasury Board confidences that are less than 15 years old.[129]

---

[124]Government of Alberta, *Find a FOIP Office* (Edmonton: Government of Alberta, 2017), online: <https://www.servicealberta.ca/foip/find-a-foip-office.cfm>.
[125]FOIP Act, section 87.
[126]FOIP Act, subsections 16(1) and 16(2).
[127]FOIP Act, subsection 17(1).
[128]FOIP Act, subsection 20(4).
[129]FOIP Act, subsections 22(1) and (2).

Under some very limited circumstances (such as when the third party consents to disclosure), a mandatory exception may not apply.[130]

The head of the public body is allowed to decide whether or not to give you access to certain records. These discretionary exceptions include:

- information, where disclosure could threaten another person's health or safety or interfere with public safety;[131]
- personal information about an applicant, if, disclosure could reasonably be expected to result in immediate or grave harm to the applicant's health or safety;[132]
- confidential evaluative material compiled to determine a person's eligibility for employment, government contracts or other benefits;[133]
- information concerning a law enforcement matter;[134]
- information concerning intergovernmental relations that is less than 15 years old;[135]
- information concerning cabinet and treasury board deliberations that are less than 15 years old;[136]
- information concerning deliberations of local public body meetings that are authorized by law to be held in camera, if the record is less than 15 years old[137]
- policy advice from government officials that is less than 15 years old;[138]
- information that could harm government economic interests;[139]
- government testing or auditing procedures;[140]
- privileged legal advice provided to the government or a public body;[141]

[130] FOIP Act, subsection 16(3).
[131] FOIP Act, subsection 18(1).
[132] FOIP Act, subsection 18(2).
[133] FOIP Act, section 19.
[134] FOIP Act, subsections 20(1), (3), and (6).
[135] FOIP Act, section 21.
[136] FOIP Act, subsections 22(1) and (2).
[137] FOIP Act, subsection 23(1).
[138] FOIP Act, section 24.
[139] FOIP Act, section 25.
[140] FOIP Act, section 26.
[141] FOIP Act, section 27.

- information that could harm conservation of a heritage site;[142] and
- information that is or soon will be available to the public (i.e., within 60 days).[143]

Some government records will include some information that you are allowed to see, and other information that falls under an exception from disclosure (such as those listed above). In that case, the public body is expected to sever the excepted portions. This allows them to provide you with the information that you can have, by severing (e.g., blacking out) the information that they are not allowed to release.[144]

What does it mean when the law says that a public body may refuse to release information if individual or public safety could be harmed?

The FOIP Act permits the head of a public body to refuse to disclose information if the disclosure could be harmful to individual or public safety.[145] The harm must not be a mere inconvenience, but one likely to result in damage or detriment to an individual or the public. When deciding whether the release of an applicant's personal information would harm the applicant, the head of the public body must consult a qualified medical person such as a physician, chartered psychologist or psychiatrist to determine whether the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

Are there any other circumstances when public bodies can disclose my personal information?

Yes. Information, even personal information, must be disclosed if the disclosure is in the public interest. This is referred to as the "public interest override".[146] This means that in some circumstances a person's privacy interests will have to give way to the public interest or public safety. The release of the information must occur even if no one has made an access to information request. The circumstances where the public interest override will

[142] FOIP Act, section 28.
[143] FOIP Act, section 29.
[144] FOIP Act, subsection 6(2).
[145] FOIP Act, section 18.
[146] FOIP Act, section 32.

apply are those where there is a risk of significant harm to the environment or the health or safety of the public, or an individual or if the disclosure of the interest is clearly within the public interest. Before disclosing the information, the head of the public body must, where practicable, notify those people to whom the information relates and give those people the chance to make representations about the disclosure of the information.[147]

Who makes the decision about whether I can gain access to my personal information?

The person who makes the final decisions about access to information in a public body is the "head of the public body". If the public body is a department, branch or office of the government, the head of the public body is the Minister responsible for that body. If the public body is an agency, board, commission, corporation, office or other such body, the head of the public body is the Minister responsible for that body, or, if there is no such person, the head of the public body will be the person who is the chief officer. If the public body is a local public body (e.g., an educational institution, a health care body, or a municipality), the head of the public body is designated by the public body.[148] Although the head of the body makes the final decision about access for that body, the Commissioner has the authority to review these decisions.

What is the role of the Access to Information and Privacy Coordinator?

Each public body has a FOIP coordinator. Before you prepare your information request, you may wish to contact the coordinator to discuss what information you are seeking. FOIP coordinators for each public body are listed in the *Alberta Directory.*

The information you are seeking may have been made public by the government already, so that you can obtain access without a FOIP request.[149] The coordinator may even be able to provide the information without a formal FOIP request, or at least tell you where you might locate the information.

The FOIP Coordinators oversee the application of the FOIP Act in their own departments. The requests for information are sent to the FOIP coordinators, who decide which branch of

[147] FOIP Act, subsection 32(3).
[148] FOIP Act, paragraph 1(f).
[149] FOIP Act, section 88.

government can respond to the request, and whether the information requested is accessible or not accessible because one of the exceptions applies. FOIP Coordinators usually manage the request process from start to finish. However, the final decision-maker is the head of the public body.[150]

Is there any fee charged to me for access to my personal information?

There may be. There is no fee to apply for access to personal information. However, there are fees charged if the amount estimated to comply with the request exceeds ten dollars.[151] There is a schedule of fees for various services provided in the regulations.[152] In some cases, you can apply to the Information and Privacy Commissioner for a fee waiver.

What form do I fill out to start the process of accessing my personal information?

The provincial government has provided a simple form called the "Freedom of Information and Protection of Privacy Request for Access to Information Form". This form is available online through the government of Alberta's website.

As well, you may make your request by writing a letter to the appropriate public body. You should mention in your letter that this is a request under the *Freedom of Information and Privacy Act.* Include your name, address and telephone number. State whether you prefer to receive copies of the documents or to examine them. Sign and date the letter.[153]

The FOIP Act allows some people to make the request orally. It is recognized that some people will have difficulty exercising their rights if they must provide a written request. For example, a person who has a limited ability to read English, and people with disabilities, may make an oral request.[154]

What happens after I make my access to personal information request?

After you have mailed in your request for access to information, you will probably receive an acknowledgment from the public body that received your request. If you sent your

[150] FOIP Act, sections 6 to 15.1.
[151] *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, section 12.
[152] *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, Schedule 2.
[153] FOIP Act, section 7.
[154] *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, section 3.

request to the wrong public body, then that body has 15 days to transfer it to the government department that has the information you are seeking. You will be notified that the request has been transferred.[155]

If a fee is payable, you will also be given an estimate of how much it will cost to provide you with the information you are seeking. After you receive the estimate, you have two choices. You have 20 calendar days to inform the public body that the fee estimate is acceptable to you. You will be asked to pay 50 percent of the estimated fees immediately. You can pay the rest later, but once the information has been delivered the balance of any fees is payable. If you are unhappy with the estimate, you can discuss ways to modify your request so as to reduce the cost of the request.[156]

The public body has 30 days to respond to your request. You may be asked to permit an extension of 30 days, and the public body will explain why the extension is necessary. If you do not think that an extension is justified, you may appeal to the Information and Privacy Commissioner. The Commissioner will decide if the extension is justified. The Commissioner can grant an extension of more than 30 days if he or she thinks it is necessary.[157]

If your access request is successful, the public body will tell you when you will receive copies or be able to review the records you are seeking. If the information you are seeking is your own personal information, you will have to show that you are the person named in the records.

In some situations you may wish to obtain data that has not yet been completely compiled or that will be available in the future. The legislation permits you to file a continuing request in which you indicate that you want to receive information as it becomes available over a period of up to two years.[158]

---

[155]FOIP Act, section 15.
[156]*Freedom of Information and Protection of Privacy Regulation* AR 186/2008, sections 13 and 14.
[157]FOIP Act, section 14.
[158]FOIP Act, section 9.

If I am able to get access to my personal information, will I get a copy of the record?

Although you may prefer to examine the record at the office of the public body, perhaps to avoid copying charges, the public body may insist on providing a copy of the record instead.[159] The public body may refuse to let you see the original record because giving you access in that way would unreasonably interfere with government operations. Another reason to refuse to let you see the original record is to ensure that you do not see information that you are not allowed to have access to.[160]

Can I get my personal information in alternative formats?

No, unlike the federal government, the Alberta legislation does not allow for the receipt of information in alternative formats, such as in Braille.

What is the best way to phrase my personal access to information request?

The phrasing of the access to information request is important and may affect the quality and quantity of information that is received by the requester.

First, consider the scope of your request. The FOIP coordinator may have some good suggestions for ways to phrase your question to obtain the information you want. In fact, the head of the public body (who usually delegates this authority to the FOIP coordinator) has the duty to make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely.[161] It is often a good idea to discuss the request informally as this will help you to clarify the issues and to get useful admissions about the information from the public body.

You should be as specific as you can about the information that you are seeking. The request has to be specific enough so that the public body can identify the records you seek. Avoid drafting a request that is too broad or too vague. You do not want to be charged a high fee to obtain information that you did not really need or want.

---

[159] FOIP Act, section 13.
[160] *Freedom of Information and Protection of Privacy Regulation* AR 186/2008, section 4.
[161] FOIP Act, subsection 10(2).

What if the government refuses to grant access to my personal information?

If the public body informs you that you have been refused access to requested records, the body will give you reasons for the refusal. You will be informed that you have the right to challenge this decision to refuse access.[162] The person who reviews the public body's decision is the Information and Privacy Commissioner.

Even if you are refused access, the public body should inform you whether a record exists or not. However, in a few circumstances—such as law enforcement areas—the public body can refuse to tell you whether a record even exists.[163]

If you do not hear anything from the public body within the 30 day period or any extended period that you have been notified about, you may treat the non-response as a denial of access.[164]

Can I appeal a decision to refuse access to my personal information?

Yes. You have 60 calendar days after you receive the decision from the public body to appeal to the Information and Privacy Commissioner. The 60 day time limit does not apply in the case where you have not received a response within the legislated time limit. Your appeal to the Commissioner must be made in writing.

The review of your appeal must be complete within 90 days.[165]

If you have requested access to a record or correction of personal information, you may apply to the Commissioner to review any decision, act, or failure to act of the head of the public body.[166]

A person wishing to appeal a decision may complete and send to the Commissioner a "Request for Review" form. Alternatively, you may write a letter to the Commissioner in

[162]FOIP Act, paragraph 12(1)(c).
[163]FOIP Act, subsection 12(2).
[164]FOIP Act, subsection 11(2).
[165]FOIP Act, subsection 69(6).
[166]FOIP Act, sections 65 and 66.

which you outline your request for a review.[167] Include your name, address, telephone number, the reason for requesting a review and the public body to which your request was originally made. Enclose a copy of your original request, if available.

Your appeal is likely to begin with a staff member in the office of the Information and Privacy Commissioner, who may mediate your matter.[168] There are presently four portfolio officers. The portfolio officer's role is to try to mediate and resolve disputes before the question proceeds to a formal review. If the matter is not resolved, it will be dealt with by the Information and Privacy Commissioner.

In making an appeal decision, what powers does the Information and Privacy Commissioner have?

If the matter proceeds to a formal review, the orders of the Information and Privacy Commissioner are legally binding. The Commissioner will review the decision of the head of the public body. In dealing with the public body's decision to give or refuse access to all or part of a record, the Commissioner can:[169]

- confirm the decision of the head of the public body to refuse access; or
- ask the head to reconsider the decision to refuse access;
- require the head to give the applicant access to the record; or
- require the head to refuse to give the applicant access to the record.

Also, the Commissioner can generally enforce the provisions of the FOIP Act.[170] The Commissioner's order can be filed with the Court of Queen's Bench.[171] This means that the order is enforceable under Alberta law.

Can I appeal a decision of the Information and Privacy Commissioner?

If you do not agree with the Commissioner's decision, the only avenue you have is to apply to the courts for judicial review. An application for judicial review is used to challenge the fairness and legality of the appeal process.

---

[167] FOIP Act, section 66.
[168] FOIP Act, section 68.
[169] FOIP Act, section 72.
[170] FOIP Act, subsection 72(3).
[171] FOIP Act, subsection 72(6).

However, if either the applicant or the public body simply disagrees with the decision of the Commissioner, there is no right to appeal the Commissioner's decision. That decision is final.[172]

The public body is given 50 days to comply with the order, unless an application for judicial review has been made.[173]

What is the role of the Information and Privacy Commissioner?

The Alberta Office of the Information and Privacy Commission is responsible for watching over how the FOIP Act is being administered, in order to help ensure the goals of the Act are being met. In Alberta, as in many other provinces, one person is responsible for both access to information and protection of privacy. The Information and Privacy Commissioner has been given significant powers. He or she can make recommendations on things like records management, which then can become regulations.[174] The Information and Privacy Commissioner can conduct investigations to ensure compliance with the Act and to follow-up on complaints.[175] Any information given to the Information and Privacy Commissioner during an investigation or inquiry is privileged, meaning confidential or protected.[176] If the Information and Privacy Commissioner makes a decision in the complainant's favor, he may make an order correcting the wrongdoing.[177] The public body must comply with the order within 50 days or have formally requested for a court to review the matter.[178]

In Alberta, the Commissioner's office is independent of the government. To ensure that the Commissioner can act independently, the Commissioner is chosen by an all-party standing committee of the Alberta Legislature for a five year term.

How do I contact the Information and Privacy Commissioner?

You may contact the Information and Privacy Commissioner for Alberta by one of the following methods:

---

[172]FOIP Act, section 73.
[173]FOIP Act, section 74.
[174]FOIP Act, section 64.
[175]FOIP Act, sections 65 to 74.
[176]FOIP Act, section 57.
[177]FOIP Act, section 72.
[178]FOIP Act, section 74.

E-mail: generalinfo@oipc.ab.ca
Web Site: www.oipc.ab.ca/

Edmonton Office

Address: 410, 9925 - 109 Street Edmonton, Alberta T5K 2J8
Telephone: (780) 422-6860
Toll -Free: 1-888-878-4044
Fax: (780) 422-5682

Calgary Office:

Address: Suite 5460, 801 6th Avenue SW, Calgary, Alberta T2P 3W2
Phone: (403) 297-2728
Toll-Free: 1-888-878-4044
Fax: (403) 297-2711

Where can I get more information about provincial privacy legislation?

Several provinces have web sites. These are:
British Columbia: https://www.oipc.bc.ca/
Saskatchewan: https://oipc.sk.ca/
Ontario: www.ipc.on.ca
Manitoba: www.gov.mb.ca/chc/fippa
Nova Scotia: http://www.foipop.ns.ca/
New Brunswick: http://www.info-priv-nb.ca/
Prince Edward Island: https://www.princeedwardisland.ca/en/information/justice-and-public-safety/freedom-information-and-protection-privacy-foipp
Newfoundland and Labrabor: http://www.oipc.nl.ca/
Quebec: www.cai.gouv.qc.ca/

1.2 Specific Issues in Government Information and Privacy

The following materials deal with specific areas and issues in government information and privacy that are often of concern to the public.

1.2.1 Statistics Canada Surveys and the Census

What is the census?

The government of Canada conducts a survey of the whole population every five years. The reasons for conducting the census include to:

- determine how much federal money a province should receive because some social programs are based on population figures;
- determine the number of seats in Parliament allocated to a province as numbers depend on population figures;

- decide funding for programs and other policy choices; and
- provide the only source of detailed information about small populations, including lone-parent families, ethnic groups, industrial and occupational categories and immigrants.

The last census was held in May 2016. Most Canadians receive a short questionnaire but some receive a longer, more detailed form.

Is the government allowed to ask me all these personal questions?

Your responsibility to answer the questions on the census questionnaire comes from the *Statistics Act.*[179] If you do not answer the questions, you could be convicted and have to pay a $1,000 fine.[180]

However, whether you will end up being punished under the *Statistics Act* is not certain. There have been challenges made to the Act, which were upheld by the Courts.[181] After these challenges, the government has been careful to act within the limits of the *Statistics Act*.

How can I be sure my information stays confidential?

There are measures taken by the government to ensure the privacy of your information. The census workers who distribute and collect the surveys take an oath of secrecy and can be punished if they break this oath.[182] As well, the census form itself is considered privileged. This means that it cannot be used in any court proceedings against you, and a census worker cannot be compelled to testify about a census form.[183]

Generally, information collected is not to be disclosed.[184] However, there are several exceptions to the rule that your information cannot be disclosed.[185] For example,

- information can be disclosed if it is already available to the public under another law;

---

[179] *Statistics Act*, Revised Statutes of Canada 1985, chapter S-19.
[180] *Statistics Act*, sections 31 and 32.
[181] See B Foden, "B.C. Critic of StatsCan Wins Battle" July 10, 1998 *The Province*.
[182] *Statistics Act*, section 34. The current penalty is a fine of up to $5,000 or six months in jail or both.
[183] *Statistics Act*, section 18.
[184] *Statistics Act*, subsection 17(1).
[185] *Statistics Act*, subsection 17(2).

- information can be released if the individual or institution consents to the release; and
- certain information can be disclosed, like information relating to non-commercial institutions, as long as it does not relate to any individual in care of the institution.

Despite the precautions taken, occasionally, personal information is released or disclosed without consent. Census workers have in the past accidentally dropped forms on the sidewalk, or in some incidents, given an already filled out form.[186]
The Privacy Commissioner made recommendations that changed the way the census is organized to address invasion of privacy by census workers.[187] For example, during both the May 2001 and May 2006 Censuses, if a person knew his or her local census worker and wanted to keep the information private, he or she could call the national toll-free Census Help Line to find out other ways to return the questionnaire. Also, census workers are selected from locations outside of the Enumeration Area to ensure privacy. The forms that people receive clearly explain the role of the census workers and list the Help Line. The option introduced in 2006 Census, which allows respondents to give Statistics Canada explicit consent to obtain their income information from tax files rather than providing this information on the census questionnaire, is another way of ensuring privacy since sensitive income data will not appear on the Census questionnaire in the hands of Census workers.

In the last few years, proposals to release census records dating back to 1906 and 1911 from the National Archives have been made.[188] Historians sought access to the records containing personal census information in addition to the raw, census data that is allowed to be disclosed under the *Privacy Act*. The Privacy of Commissioner of Canada objected to this pressure, citing the obligation of the government to not disclose personal census information

[186] E. Shaw, J. Westwood and R. Wodell, *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How To Protect Them* (Vancouver: B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association, 1994) at 95 (hereinafter Shaw, Westwood and Wodell).
[187] "Your Privacy and the 2001 Census" Privacy Commissioner of Canada Website: http://www.priv.gc.ca/information/ar/02_04_08_e.cfm.
[188] See Editorial Staff, "The Past Belongs to All of Us: Denying Access to Census Data Reveals an Anti-Intellectual Bias" Friday November 12, 1999 *The Globe and Mail*; B. Phillips, Privacy Commissioner of Canada "I'm Proud to Keep the Census Secrets" Thursday, Nov. 11 1999 *The Globe and Mail*.

to anyone outside Statistics Canada. Other ways of releasing personal records could occur if consent was given by the individual on the original form. The Commissioner maintained that a person's privacy whether dead or very old, must be protected. He pointed out that privacy is a public right and a cornerstone of an effective democracy; thus, it is not up to individuals to decide whether it can be bartered away.[189] In June 2005 however, Parliament passed an amendment to the *Statistics Act* allowing for the release of census information by Library and Archives Canada after 92 years. For the 2006 Census and subsequent Censuses, only information for persons who have given explicit consent will be released 92 years following a Census.[190]

Where do I complain if I have concerns about the Census and my privacy?

The Federal Privacy Commissioner investigates complaints about the improper collection, use or disclosure of personal information, including that collected under the Census.

1.2.2 Canada Customs and Revenue Agency

How does Canada Customs and Revenue Agency collect information about people's income?

The collection of information by Canada Customs and Revenue Agency ("Revenue Canada") operates on a voluntary basis. This means that the government does not tell citizens how much they owe in taxes but provides guidelines for them to do their own calculation. However, because citizens are given this responsibility, the Minister of Revenue is granted broad powers to ensure that citizens are meeting these obligations to report their income.

What powers does Canada Customs and Revenue Agency have to make sure citizens correctly assess their tax status?

The penalties imposed on someone who does not file his or her information under the *Income Tax Act* (ITA),[191] are a $1,000 to $25,000 fine and/or up to 12 months imprisonment.

---

[189] B. Phillips, Privacy Commissioner of Canada "The Census Returns, Privacy and Questions of Governance" Submission by the Privacy Commissioner of Canada to the Expert Panel on Access to Historical Census Records, February 9, 2000 (Statistics Canada) Website: www.statcan/ca/english/census96/return.htm.

[190] Honourable D. Bhoudria, October 3, 2002.

[191] Chapter 1 (5th Supp.), Revised Statutes of Canada 1985.

Under the ITA there are three categories of investigative powers:

- inspections, audits or examinations;
- demands for documents; and
- searches and seizures.

Inspections, Audits or Examinations

Investigators can enter any place other than a home without a warrant to ensure people are complying with the ITA.[192] This power is limited in that the entry must be at a reasonable time, and for a purpose consistent with the ITA; such as to investigate for fraud. Before entering a private home, a search warrant must be obtained. Investigators are given broad powers to inspect, audit and examine items once on the premises, but they do not have the power to seize documents and remove them from the site.

Demand for Documents

The Minister of National Revenue may demand that information be supplied to the Department of Revenue. Before doing this, you must be notified of the request either in person or by registered mail. The demand for information must be for a purpose related to the ITA but need not be restricted only to the person under investigation. To request documents from a third person, though, a warrant must be obtained first.[193] If you did receive a demand for documents, you need only make them available to the Department.

Search and Seizure

Documents may be received during an audit or inspection where it appears that there was a violation of the ITA by the person under investigation. The investigator does not need reasonable and probable grounds to conduct an inspection but does in order to obtain a search warrant.

What does Canada Customs and Revenue Agency do to protect my privacy?

Revenue Canada employees are required to follow strict secrecy rules. Employees are trained to respect citizens' privacy. In addition, employees cannot be compelled to give evidence in court based on information they received in carrying out their work. However, this prohibition on disclosure of personal information only applies to tax officials. You can

[192] ITA, section 231.1(1).
[193] ITA, section 231.1(2).

still be required to disclose information in order to receive a certain benefit from the government or be compelled to disclose information at a trial.

You should also be aware that there are some exceptions to the requirement of information confidentiality under the ITA. For example, information collected may be shared within the department itself, with other departments, such as the Department of Finance, that may need bulk information to make policy, and to compile statistical data on citizens.

Thus, although tax legislation is fairly protective of citizens' privacy, it is important to keep in mind the limits and scope of the statute.

For information about Canada Customs and Revenue Agency and privacy, please see Chapter 4: Searches.

1.2.3 Protection of Health Information—The Alberta Example

What legislation regulates health information in Canada?

There are various pieces of legislation across the country dealing with health information. Sometimes the legislation deals with health information in both the private and the government sectors. This is unlike other privacy legislation, which tends to deal with information in one sector or the other.

For more information about the obligations of medical professionals to keep personal information private, see Chapter 2: Privacy and Canada's Private Sector.

What about health information in Alberta?

The *Health Information Act* (AHIA)[194] regulates personal information in the health sector in Alberta. AHIA deals with complex issues concerning the collection, use, disclosure and protection of personal health information in the health care system. The rights of many different peoples and groups must be balanced under the AHIA. The stated purpose of the AHIA is to achieve the best balance possible between the privacy of patients and the need

[194] *Health Information Act*, RSA 2000, c H-5, proclaimed in force April 25, 2001 [hereinafter AHIA].

for the collection, use and disclosure of information. It is important to note that AHIA does not apply to all health information about a person.[195]

What does AHIA do?

AHIA attempts to balance privacy and the interest society has in obtaining information. The introductory section of the AHIA sets out the purpose of the legislation and the remainder of the AHIA is divided into parts that deal with:

- a person's right to access and to amend his or her own information;
- creating offences to prevent breaches of the AHIA; and
- methods for reviewing decisions and resolving complaints.[196]

To whom does the AHIA apply?

AHIA applies to the public health sector. Some organizations, such as private insurance companies, may have health information about you, but the AHIA does not apply. AHIA applies to health care providers who are defined as a "custodian" or "affiliate" in the AHIA. A "custodian" is someone who monitors personal information.[197] A custodian remains responsible for information, even after the information leaves the custodian's care. For example, when information is disclosed to an individual's family member, the custodian is still responsible for that information.

According to the AHIA, there are over 20 types of custodians. Examples include physicians, their staff, provincial health boards, nursing home doctors and licensed pharmacies.[198] To determine if a health care provider is a custodian, you must consider not only what services are provided but also how the provider is paid for them. This is because the AHIA will apply to some individuals if they are paid under the Alberta Health Care Insurance Plan (AHCIP).

The Regulations also designate the following as custodians:[199]

---

[195] Office of the Information and Privacy Commissioner "Health Information-A Personal Matter: A Practical Guide to the Health Information Act" (Edmonton: Queen's Printer, 2010) [hereinafter "Health Information-A Personal Matter"].

[196] *Health Information-A Personal Matter*, at 5.

[197] AHIA, subsection 1(1)(f).

[198] AHIA, subsection 1(1)(f).

[199] AHIA Regulations, 70/2001.

- Alberta Rare Diseases Clinical Review Panel;
- claims reassessment committees established under the *Alberta Health Care Insurance Act*;
- Covenant Health,
- Health Advocates;
- Hospital Privileges Appeal Board;
- Mental Health Patient Advocate;
- Mental Health Review Panel;MS Drug Review Panel;
- Non-regional health authority Family Care Clinic approved by the Minister;
- Out-of-Country Health Services Appeal Panel;
- Out-of-Country Health Services Committee; and
- Regulated or registered members of specific specialized Alberta health care services.

An "affiliate" is:

- an individual employed by the custodian (for example, a receptionist);
- a person who volunteers, is appointed by or a student who performs a service for a custodian;
- an information manager;
- a person who performs a service under a contract; and
- a health services provider who has the right to admit and treat patients at a hospital.[200]

It is important for affiliates to determine if the AHIA applies to them and it is also very important for custodians to determine if a certain individual or group is an affiliate because they are responsible for the affiliates. This means that privacy is protected even when authority is delegated to an affiliate.

What information does AHIA protect?

AHIA protects three types of information but in different ways.[201] First, the AHIA protects diagnostic, treatment and care information, such as what drugs a patient is taking. This is

[200] AHIA, subsection 1(1)(a).
[201] See AHIA, Part 3.

very personal information. Second, the AHIA protects registration information, such as what you fill out on a form when you go to the hospital. This includes your name, address and health care number. When asking for your personal health care number, a custodian must advise you of his or her authority to do so. And finally, information collected about providers of health services is regulated.

Information must be contained within some form of record for it to be termed health information under the AHIA. Examples of records include x-rays, notes, reports and audio-visual recordings.[202] The AHIA also protects personal information given to a custodian that does not get written down. However, the AHIA is primarily concerned with protecting information that is identifiable to an individual. Accumulated data on many individuals that is not individually identifiable may be disclosed.

What are some of the responsibilities of custodians?

Custodians are responsible for:

- ensuring that their affiliates do not violate the AHIA;
- establishing policies for the way that the AHIA is carried out;
- collecting only as much information as is needed to carry out the intended purpose;
- using their best efforts to ensure the accuracy of the information;[203] and
- ensuring proper training of staff to respect privacy.[204]

What can custodians collect about me under AHIA?

AHIA allows collection of information only for certain purposes. Only essential information, with the highest degree of anonymity, collected in a limited manner is permissible. As well, the custodian must tell the person about the authority under which she collects individually identifying information and must collect it directly from the individual, unless indirect collection is authorized.

---

[202] AHIA, section 1(1)(t)
[203] "Health Information-A Personal Matter", at 17-18.
[204] AHIA, Part 6.

What uses can be made of identifiable health information?

AHIA allows custodians to use individually identifying health information for certain purposes.[205] Custodians can use identifiable health information:

- to provide a health service or to determine eligibility to receive a health service;
- when conducting investigations or research;
- in disciplinary proceedings;
- in educating health service providers; and
- in managing internal operations.

It is important to note that *use* and *disclosure* are two separate concepts in the AHIA. Disclosure occurs when one custodian gives health information to other custodians or outside parties. This should only occur in the way that is provided for in the AHIA. For example, a custodian could disclose general health information to a family member to advise the member that the patient was injured, ill or deceased. There are many other types of disclosure permitted in the AHIA.

Can I have access to my personal health information?

You have a right of access to any health information record in the custodian's control.[206] Custodians must make every reasonable effort to respond to a request openly, accurately and completely.[207] The custodian must tell an applicant whether he will grant access to all or part of the requestor's record and when that access will be granted. However, custodians are allowed to refuse access in some situations.[208] For example, if immediate and grave harm would result to the applicant or another's mental or physical health or safety, the custodian could be justified in denying the request. If the disclosure of your health information might be a threat to public safety, it may be denied.

What if I believe there is a mistake in my records?

If you believe that there is an error in your record, you can request in writing that the custodian who has control of the record change it.[209] The custodian has 30 days to make the correction, but may ask for more time to do so. A custodian may refuse to make the

[205] AHIA, Part 4.
[206] AHIA, section 7.
[207] AHIA, section 10.
[208] AHIA, section 11.
[209] AHIA, section 13.

correction if it involves a professional opinion. If the custodian does not make the amendments, they must tell the applicant about the refusal and explain why. If you are dissatisfied with the actions or inaction of a custodian, you can complain to the Privacy Commissioner. The Privacy Commissioner has certain powers to review complaints and make orders after investigating the complaint.[210]

1.2.4 Identity Cards

In the wake of September 11, 2001, several jurisdictions in Canada proposed the development of identity cards. For example, changes to Canada's immigration laws[211] require permanent residents to carry special status cards containing information about their immigration status. The government is developing a fraud resistant document using state-of-the-art security features, including a tamper proof photo image.

Several provincial governments have looked into the possibility of issuing every resident with high-tech, high-security photo identification cards. For example, in the past Alberta suggested that identification cards might contain fingerprints or DNA information. These cards will be used to replace drivers' licences and other government photo identification cards.[212] The privacy implications of such identity cards are significant.

1.2.5 Police Information Sharing

How do police get information about me?

In order to carry out their duties, police forces must collect and organize the information gathered in the course of their work. This information comes from any incidents that are reported to the police. It is important to remember that as a part of police duties, the police have been given the power of surveillance to enforce the law. However, with new technologies, the powers of surveillance have become more intrusive and more powerful. Two kinds of police surveillance have been described, including surveillance to:

- investigate specific incidents, or

[210] AHIA, Part 7.
[211] *Immigration and Refugee Protection Act*, Statutes of Canada 2001, chapter 27, section 31.
[212] "Critics Worry Alberta's Identity Card Plan Could Jeopardize Civil Rights" *Edmonton Journal* 2 November 2001.

- gather intelligence in general to prevent or control crime.[213]

Police organize the material gathered from surveillance into their information systems.

For more information on surveillance see Chapter 3: Surveillance.

What kind of information do the police collect?

When police respond to a call for assistance, they take notes on events that happened as described by witnesses, details of the scene of the incident and further information they can glean about who may have been involved. These notes are organized into an "Occurrence Report". As well, a "Persons Report" may be made to record details on persons being investigated.[214]

What happens to information collected from an incident?

The reports generated from an incident are entered into police information systems. One such system is the Police Reporting and Occurrence System ("PROS"). PROS is a database of information about crimes, people and other relevant details. Police files of all Royal Canadian Mounted Police ("RCMP") detachments are linked with this system, and other police forces can rent the system from the federal government. Only police officers and civilian staff who pass a security clearance have access, and access varies with the sensitivity of the information.

Another important database of information maintained by police forces is the Canadian Police Information Centre ("CPIC"). This centralized computer system allows police from across Canada to have access to information collected from a force in a different jurisdiction. It contains a variety of information on millions of Canadians; however, information on infractions of provincial legislation is an exception to access. As with PROS, the local police unit that responded to the incident enters the information in the system.

What type of information is contained on CPIC system?

Files contained on CPIC include:[215]

---

[213] S. A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (Toronto: The Carswell Company Ltd., 1983) at 56 (hereinafter Cohen).
[214] Shaw, Westwood and Wodell at 52.
[215] Royal Canadian Mounted Police, 2000-2001 Fact Sheet No. 36.

- Vehicle file: stolen, abandoned or wanted in connection with crime; stolen licence plates; validation tags, Vehicle Identification Number plates and parts;
- Persons file: wanted persons, parolees, accused persons, prohibited persons, parolees, probation, missing persons, body files (unidentified persons);
- Criminal Record Synopsis file: condensed version of criminal records and fingerprints;
- Property file: guns, stolen articles and stolen securities (stocks and bonds);
- Marine file: stolen boats, abandoned boats;
- Criminal Records file: full criminal records;
- Dental Characteristics file: dental records;
- Inmate file: persons incarcerated or on parole;
- Wandering persons registry: persons who are registered with Alzheimer's Society of Canada.

CPIC also has access to provincial motor vehicle information.

Who has access to police information systems?

The R.C.M.P., provincial police forces and approved municipal forces have direct access to the databases. The exception to this is that access to information gathered in the course of intelligence investigations, as opposed to a response to a specific incident, is not directly accessible.

Other groups have indirect access to police information systems, including for example, Ports Canada Police, Crown counsel, probation officers, Corrections staff, government officials and employers.[216] These groups must contact agencies that have direct access, such as the R.C.M.P., to obtain information from the systems. In the United States, the Federal Bureau of Investigation (FBI) has direct access to this Canadian system. Other U.S. agencies supposedly do not have access, although there have been indications that information has been obtained anyway.[217] On an international level, Interpol (International Criminal Police Organization) has direct access to CPIC, and other international agencies have indirect access by applying for information through Interpol.

[216] Shaw, Westwood and Wodell, at 47.
[217] Shaw, Westwood and Wodell, at 48. See also Cohen.

Why should I be concerned if different agencies have access to personal information about me on police information systems?

The information collected and entered into these systems is relied upon by investigating officers, who are sometimes far from the original location of the incident. The data tends to be viewed as accurate even though it is just a broad collection of unverified information, which is sometimes based on witness statements made at the time or on impressions of the police officer at the scene. The structure of the police information system encourages the collection of quantity over the quality or accuracy of information, but this fact can be forgotten when other officers use the databases.[218] With the advent of computer technology in police cars, one concern is that officers may access information and seize the opportunity to act before verifying the accuracy of that information. CPIC is only to be used for investigations and officers who access the system are required to verify the record before acting on it.[219]

Another concern is that there is no *Criminal Code* provision that would allow an individual to complain that someone has used his or her information improperly, unless the person has sold it. There are provisions in privacy legislation allowing complaints to the appropriate privacy commission if personal information is released improperly by the government (or the police), but the *Criminal Code* does not deal with this situation.[220]

Can I find out what information the police have on me in their systems?

Citizens may be able to find out what information is stored about them in police information systems under access to information legislation. You will usually wish to contact the police force that originally collected the data, as this was the force that entered the information into the system. If the R.C.M.P. collected the information, then you will wish to apply under federal privacy legislation, as this police force is under federal jurisdiction. If it was a municipal police force, then you will look to provincial legislation.[221] You should also be aware that you may not have access to all information held about you if the secrecy of this information is necessary to prevent damage to an ongoing investigation or would reveal the

[218] See K. Friesen, "Protection of Confidential Sources of Law Enforcement and FOIP" 52 *Advocate* (1994) Part I, January, at 110.
[219] Shaw, Westwood and Wodell, at 47.
[220] Shaw, Westwood and Wodell, at 53.
[221] In Alberta, this would be the FOIP Act.

identity of a confidential source.[222] If you think you are unfairly denied access to information, you can appeal to the federal or provincial privacy commissioner, depending on which police force is involved.

Can I get information on police databases corrected, changed or deleted?

Under the *Criminal Records Act*,[223] if a person has received a pardon, information about the offence must be removed from CPIC. In addition, the government has various "purge" policies. This means that certain information, such as summary conviction offences, must be removed from CPIC or PROS after a period of time has passed.

If police charges did not result in a conviction, but your record (e.g., fingerprints, photograph or other information) is in the police system, you can ask the arresting police force to request that the R.C.M.P. return your fingerprints and all information taken at the time of arrest for destruction. Under the current law, the police force does not have to agree to this request. Additionally, you may be able to obtain access to, or correction of, personal information held in a police database under the applicable privacy legislation. However, there are a number of exceptions or exemptions in federal and provincial privacy legislation, which may affect your success.

Conclusion

The police require powers of surveillance and investigation in order to carry out their responsibility of maintaining peace and order in society. Although some may advocate for increased police powers for the prevention or elimination of crime, careful consideration should be given to ensure that this will be an effective and acceptable increase in power when weighed against citizens' right to privacy. To some degree, society also bears responsibility in ensuring that crime is kept to a minimum, and passing more of this burden on to the police may not be the most effective method of controlling crime in the long term. Thus, police use and access of information systems should be monitored and under the control of privacy legislation. Information should only be used where permissible under legislation and its accuracy should be verified before action is taken.

---

[222] Shaw, Westwood and Wodell, at 49.

[223] Revised Statutes of Canada 1985, c C-47, section 6.1.

1.2.6 Data Sharing and Data Matching by the Government

With the advent of new technologies, some people have become quite concerned about the ability of governments (and others) who hold information to match and compare data about us.

1.3 CANADIAN SECURITY INTELLIGENCE SERVICE

The name of this agency is usually shortened to "CSIS", which is pronounced 'see-sis.'

What is CSIS' purpose?

Since 1984, CSIS has been Canada's spy agency. It is primarily responsible for helping ensure Canada's national security.[224] Before that, the RCMP Security Service branch of the Royal Canadian Mounted Police did this job.[225] Unlike the RCMP, CSIS is not a police force. CSIS agents do not have the power to arrest or detain people. They do not carry weapons and do not enforce the laws like police officers do. CSIS agents protect Canada's national security by collecting and analyzing information about possible threats to Canada's security and then passing this information on to the government and various law enforcement agencies for them to follow up on. CSIS agents get their powers to investigate such matters from the *Canadian Security Intelligence Service Act (*"the CSIS Act"*)*.[226]

CSIS does some of its investigations openly, and some secretly. Open investigations include having interviews with people who CSIS agents believe may have valuable information for their investigations.

Am I legally required to talk to a CSIS agent if I do not want to?

A CSIS agent does not have the power to take you anywhere for questioning and you do not have to answer an agent's questions.[227] If you do not want to talk with CSIS agents, then just politely tell them so. If the agent insists on questioning you or threatens you, you may wish to talk to a lawyer. You may also want to write a letter to the Director of CSIS,[228]

---

[224] For more information on CSIS visit website www.csis-scrs.gc.ca/index-eng.asp See also: Shaw, Westwood and Woddell.
[225] I. Leigh, "Secret Proceedings in Canada" (1996) 34(1) Osgoode Hall Law Journal 113-173 (hereinafter Leigh).
[226] *Canadian Security Intelligence Service Act*, Revised Statutes of Canada 1985, c. C-23.
[227] Shaw, Westwood and Wodell.
[228] Mailing address for complaints to CSIS: Director of CSIS, P.O. Box 9732, STN T, Ottawa, Ontario, K1G 4G4.

complaining about this CSIS agent bothering you. If the Director does not answer your letter, you may complain to the Security Intelligence Review Committee (SIRC).[229]

Is it okay for CSIS to have such wide and strong secret investigation powers?

In May, 1989, the Canadian Civil Liberties Association (CCLA) started a court case challenging that CSIS has "excessive and needlessly broad" intrusive covert investigative powers under the CSIS Act.[230] To help show this, CCLA claimed that CSIS had abused their powers when three organizations who were carrying on lawful activities reported that they had each been subject to some form of CSIS surveillance, which in some cases meant knowing their membership lists. CCLA suggested that in allowing CSIS to do this type of surveillance, the CSIS Act was violating the guarantee of freedom of expression, peaceful assembly, association and the right to be free from unreasonable search and seizure. CCLA argued that CSIS' surveillance techniques stop or deter people from expressing themselves freely and participating in activities that are legal. Since many of CSIS surveillance activities are done secretly, it is unlikely that those individuals whose rights and freedoms have been violated will be able to gather the necessary proof that they were part of CSIS' unconstitutional investigations.

The Ontario Court of Appeal, however, said that the CCLA could not offer any actual proof that CSIS was going outside of their powers and breaking the law. The Court of Appeal further said that CSIS was not to be stripped of any of its powers to investigate Canadians, including citizens who were doing legal activities. CCLA wanted the Supreme Court of Canada to review the case, but they declined to hear it, which suggests the lower courts handled the case correctly.

No one will dispute that terrorism is a threat to the security of many nations, including Canada. Clearly, it is in our national interest that information concerning these types of threats be investigated. To do so, Canada has the capability to spy on virtually every type of communication—from long-distance phone calls to e-mail. But it is also in our best interest

[229] Mailing address for complaints to SIRC: Director of SIRC, P.O. Box 2430, Station D, Ottawa, Ontario, K1P 5W5.
[230] *Corp. of Cdn. Civil Liberties Association v Canada (Attorney General),* [1998] 126 Canadian Criminal Cases (3d) 257 (Ont CA), [1998] SCCA No. 487.

that we continue to ensure that the powers given to investigate such threats only be used for the purpose for which they were given.

1.3.1 Security Intelligence Review Committee

What does the Security Intelligence Review Committee do?

The Security Intelligence Review Committee is a CSIS watchdog. This committee, whose name is often shortened to "SIRC," is an independent body established under the CSIS Act. SIRC is made up of 5 Privy Councillors who are not members of either House of Parliament and who are chosen by the Prime Minister after some discussions with the Leader of the Opposition. It reviews the performance of CSIS to help ensure that CSIS does not go beyond the powers that the government has given it in the CSIS Act. More specifically, SIRC's job is to:

1) hear and investigate complaints made about the alleged actions of CSIS;
2) review complaints about the refusal of security clearances; and
3) review how CSIS is using its powers to get surveillance warrants by randomly reviewing four of CSIS' warrant applications every year to ensure that CSIS "fairly and completely" represented the information that CSIS had at the time.

In order to do its job, SIRC has extensive powers under the CSIS Act which includes access to all the information CSIS has.[231]

What kinds of complaints can SIRC investigate?

SIRC is supposed to watch whether CSIS is doing what it is allowed to legally do. SIRC will investigate complaints about CSIS and make recommendations to the Director of CSIS, but CSIS does not have to follow these recommendations.[232] SIRC's recommendations are only advice; they give a second opinion.[233] In a large majority of the cases that SIRC has reviewed, however, their recommendations have been followed.

Each year, SIRC conducts a series of reviews on CSIS cases. These cover warrants, surveillance, targeting authorizations, community interviews and other matters.

---

[231] Leigh.
[232] *Thomson v Canada (Deputy Minister of Agriculture),* (1988) 31 Administrative Law Reports 184 (FCTD), (1988) 31 Administrative Law Reports. 14 (Fed. C.A.), affirmed [1992] 1 Supreme Court Reports 385 [hereinafter Thomson].
[233] Thomson.

Occasionally the committee prepares reports on special cases that come to the Committee's attention. Examples include the attack on the Iranian Embassy, the Air India tragedy and the Heritage Front Affair.

A summary of each SIRC's review, with all classified information removed, is included in the Committee's Annual Report to Parliament and is available online.[234]

SIRC has reviewed complaints that during CSIS' screening of refugee claimants, CSIS agents have tried to recruit some of them as CSIS informers in exchange for CSIS' help with the immigration process. There have also been allegations that in some cases CSIS has broken these promises to help. CSIS agents do not have the authority to make such promises, but a former top-ranking CSIS official admitted that the agency would in fact "pull strings" with the immigration department for a refugee who was helpful to them. The present CSIS organization does not deny asking newcomers for help, but it insists that these people are told they are under no obligation to speak to the agency and that the agency never offers to help with the immigration process in return for information.[235]

How is a SIRC hearing run and what happens in the end?

There is not one strict format for a SIRC hearing.[236] This flexibility allows for a quicker process in fairly straight forward matters, and for a more formal process for the hearing of more complicated matters. Generally, SIRC enlists the help of a lawyer from a security-cleared panel of lawyers in private practices to assist in the hearing. Present at the hearing will be SIRC, the SIRC appointed lawyer, CSIS, the complainant and the complaint's lawyer—if the complainant has one. All the lawyers involved in the hearing meet sometime before the hearing to ensure they understand what the main areas of disagreement are and what specific ground rules will be used in this particular case.

Once the actual hearing starts, CSIS usually makes an application to have its evidence given *in camera*, which means without other people present. CSIS asks for this in order to help protect police sources and keep information on investigation techniques secret. Although the

[234] See http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html.
[235] A. Thompson, "CSIS Refugee Spy Probe Demanded" 5 April 1998 *Toronto Star* [Toronto] A10.
[236] Leigh.

complainant can oppose this application, it is usually granted and the complainant will have to leave the hearing while CSIS presents its evidence. The complainant's lawyer will help ensure a fair process is followed in the hearing, and will cross-examine the evidence put forward. If the complainant does not have a lawyer, if the lawyer is inexperienced with SIRC hearings, or if the complainant's lawyer is also excluded, the SIRC appointed lawyer may help to ensure the complainant gets a fair hearing. Usually the complainant is provided with a summary of the evidence CSIS presented, in which the sensitive information of specific informants and various investigative techniques have been edited out. The complainant will have a chance to challenge the truth of this information and present any additional information they have.

The Supreme Court of Canada reviewed SIRC's hearing procedures in a case where they were reviewing a deportation order of a landed immigrant who had been convicted of a serious offense and was further suspected of involvement with organized crime. In this set of circumstances the court determined SIRC's hearing procedures were good in that they did not violate the right to have a fair hearing or natural justice. The court held that by providing the services of a review committee like SIRC, the government had not only done more than required, but further, SIRC's procedures allowed for balancing what is good for the country with what is good for the individual.[237] So far, no one has challenged in court whether or not SIRC's hearing procedures are also fair for cases other than those involving deportation.

At the end of the SIRC hearing, SIRC recommends to the Director of CSIS what the outcome of the disagreement should be.

1.3.2 Security Clearance Checks

What is a security clearance check?

Another part of CSIS' job is to do the security clearance checks that people require in order to work at many federal government jobs or airports. The greater the level of security clearance required, the more thorough the security check by CSIS will be. A person might be denied security clearance because there are reasonable grounds for believing that they

[237] *Chiarelli v Canada (Minister of Employment and Immigration),* [1990] Federal Court Judgments No. 157 (FCA) affirmed, [1992] 1 Supreme Court Reports 711.

may carelessly show or talk about things classified as secret, or that they might otherwise be easily persuaded to do so. CSIS also does security checks for citizenship and immigration purposes.

What happens if I am denied a security clearance check by CSIS and what can I do about it?

If you have been denied this type of required security clearance or a particular level of security clearance it may mean that you could be denied a specific job, a promotion, a transfer, or be denied the status a newcomer needs to stay in Canada. If this were to happen, you could complain to SIRC who will investigate the complaint. SIRC will hold a hearing and make recommendations to the Director of CSIS as to whether or not you should be granted this clearance. Once again, however, CSIS does not have to follow SIRC's recommendations.

1.3.3 The Privacy Act and CSIS

Can I find out if I am or ever was under investigation by CSIS and what they found?

While the job of ensuring national security is important, knowing that you are under investigation and for what reasons is also important, so that you can have a chance to challenge or explain CSIS' findings. You can apply under Canada's *Privacy Act* to see all the records that CSIS and the RCMP may have that relate to you.[238] If, however, the information CSIS has on you falls within one of the exemptions in the Act which permit the government to withhold the release of information, CSIS would not have to show you what they have found or even admit that they have collected information about you. Some of these exemptions are designed to protect Canada from subversive activities, threats to its security, or to protect informants.

What can I do if CSIS refuses to give me information about my file?

You can appeal CSIS' decision not to share information with you to the Privacy Commissioner and ultimately to the Federal Court, but if the information touches on national security, it will still probably not be disclosed. The courts must balance the interests of an individual against the interests of an entire country. Therefore, because the time and

[238] Shaw, Westwood and Wodell.

effort put into the process of gathering investigative information is high, courts are often reluctant to order the release of such information. More often than not, in this type of challenge, the public interest in not disclosing the evidence is determined to outweigh the public interest in disclosing.[239] The judge, however, can review the withheld documents to ensure they properly fit within one of the exemptions in the *Privacy Act*.[240] Arguing for documents to be disclosed is difficult, because you are usually arguing it is important that you see these documents without you actually knowing what exactly is in the documents. To help your argument you are usually given just enough information about the documents to know the type of information they contain (e.g., a union membership list).[241]

1.4 Conclusion

This chapter demonstrates the complexity of privacy issues in Canada, and that privacy has become increasingly important as technological advances have occurred. The following chapters in the handbook deal with specific issues of privacy in Canada.

---

[239] *Haroutine (Harout) Kevork, Raffic Balian and Haig Gharakhanian v The Queen and Mel Deschenes, Director of the Bureau of Counter Terrorism, Canadian Security Intelligence Service,* [1984] 2 Federal Court 753.

[240] *Privacy Act*, section 45. See also: *Hoogers v Canada (Minister of Communications),* [1998] Federal Court Judgments No. 834 (FCTD), where the Court reviewed the documents in question when an application was made under Canada's *Access to Information Act,* Revised Statutes of Canada 1985, c. A-1, for access to archives held by CSIS.

[241] See: *Ruby v Canada (Solicitor General); Ruby v Canada (RCMP),* [2000] Federal Court Judgments No. 779 (FCA), where the court held that the exemption under section 22(1)(b) does not permit the refusal to disclose information where disclosure would have a chilling effect on CSIS' investigative process in general.

1.5 CASE STUDIES

1.5.1 The Charter and Privacy

R v Dyment, [1988] 2 Supreme Court Reports 417

Dyment was taken to the hospital after crashing his car into a ditch and suffering a head wound. A doctor at the hospital collected a sample of free-flowing blood from Dyment's head wound for medical purposes while he was unconscious. Shortly after, Dyment woke up and admitted to drinking a beer and taking some antihistamine tablets before the accident. The doctor had a conversation with a police officer, who had returned to the hospital with Dyment, and the blood sample was handed over to the police officer. Neither the doctor nor the officer had suspicions that Dyment was possibly impaired and the police officer did not ask for Dyment's consent nor get a warrant to obtain a blood sample. The officer later had the sample analyzed and because of the results, Dyment was charged and convicted under Criminal Code section 236 with being in care and control of a motor vehicle having consumed alcohol in a quantity that exceeded the legal limit.

Dyment appealed his conviction on the ground that the taking of blood violated his section 7 and 8 Charter rights. The blood was taken without his consent or knowledge and this was a violation of his security of the person and an unreasonable search or seizure. The lower court held there was no violation of Dyment's Charter section 7 rights but there was a violation of his section 8 rights. The Crown appealed to the Supreme Court of Canada and so the issue was whether the taking of the blood sample by the police officer from the doctor who had obtained the sample violated section 8 of the Charter. The Court also had to determine if the evidence should be excluded under section 24(2) of the Charter.

The Court reviewed the importance of privacy to the individual. Privacy was more than just security of the physical person but also went deeper to the dignity of the person. The Charter was meant to be interpreted in a manner that embraced the ideas behind Charter rights instead of in a constricted fashion. Also, privacy related to information and not just physical space and human dignity. However, claims to privacy must be balanced with other needs in society, such as law enforcement. Finally, the Court stated that the protection of

privacy could not be retroactive. People have a right to be secure from invasions of their privacy at the outset.

Based on these principles, the Court found that there was no consent to take the blood sample and consent could not be implied beyond taking the sample for medical reasons because the patient was unconscious. A doctor has a duty to ensure the privacy of patient information. Even if the doctor has a duty to abide by the law and provide information when a crime has been committed, this does not extend to supplying material collected from the unknowing patient. Thus, the officer breached Dyment's privacy interests under section 8.

The breach was held to be unreasonable because the violation of privacy was not a minimal intrusion. In order to justify a breach of Charter rights, the Crown must meet a high standard and this was not done. It is important that the police have clear guidelines on what are acceptable methods of legal enforcement. The Court noted that public trust in the administration of medical systems would be undermined if the free-flow of very personal health information and physical substances in particular were tolerated. Thus, because the breach of Charter rights was a serious one, striking at the very dignity of human beings, the Court held that the appropriate remedy was to exclude the evidence under section 24(2) and dismiss the appeal.

Her Majesty The Queen (Respondent) v Captain M. Savaria (Applicant)
Canada Court Martial (2008)[242]

Captain Savaria was a pilot with the Canadian Forces. As part of a consultation for re-enrolment (transfer) from the Reserve Force to Regular Force, Captain Savaria met with Major Descoteaux, a flight surgeon in December 2004 to conduct a medical assessment of Captain Savaria and his fitness to once again become a pilot with the Canadian Forces. The issue of Captain Savaria's psychological health came up during this consultation, as his medical record referred to a previous question in this regard. Based on the information provided by Captain Savaria, Major Descoteaux concluded that Captain Savaria's previous psychological problem was resolved and that he was fit to serve once again as a pilot in the Regular Force of the Canadian Forces.

On August 29, 2005, Major Descoteaux, now the Senior Medical Officer of the Valcartier Garrison, received an invoice from the Department of Veterans Affairs for the cost of 30 consultations which Captain Savaria had with a psychologist, Mr. Carol Girard, from July 9, 2003 to March 11, 2005. She also received a consultation report from the same psychologist, which read that Captain Savaria's psychological condition was not in any way resolved. Due to this contradiction, Major Descoteaux conducted a complete review of Captain Savaria's medical record to determine if there was anything written about the contradiction. At the completion of the review she sent a memo to her medical superior concluding that the diagnoses were modified and signatures of some physicians, including her own, were forged and that Captain Savaria had apparently given false or misleading information about his state of health at his medical examination for re-enrolment in December 2004 and in the beginning of 2005.

To follow up on the memo, a lead investigator, Sergeant Paré, a military police officer with the detachment of the Valcartier Garrison, was assigned to this file. He applied to a federal investigative body under paragraph 8(2) (e) of the Privacy Act ("PA") to obtain certain medical records of Captain Savaria and Major Descoteaux's memo. This application was refused because the Acting Director of the Directorate Access to Information and Privacy of the Department of National Defence needed more information and details on the documents.

[242] *R c Savaria,* Canada Court Martial (2008) CarswellNat 5680.

After a subsequent successful application under paragraph 8(2)(e) of the PA, Sergeant Paré obtained disclosure of 21 documents which were later seized and three of which were submitted to an expert for handwriting comparison. Vickie Mercier, a document specialist who examined the three documents, submitted that the signatures on the documents were not those of the physicians in question and this led to Sergeant Savaria's subsequent charge of committing forgery contrary to section 367 of the Criminal Code and alternate charge of altering documents made for Military purposes with intent to deceive contrary to Paragrah125(c) of the National Defence Act.

At trial, Captain Savaria argued that due to his reasonable expectation of privacy in connection with his medical records at the Valcartier Garrison medical clinic, that the court should exclude under subsection 24(2) of the Canadian Charter of Rights and Freedom ("Charter"), the document expert's report and the documents used as a basis for the document expert's report which were obtained by Sergeant Paré under the PA, because they were subject of an unreasonable seizure and an infringement of his right to be secured against unreasonable seizure under section 8 of the Charter. The Court held that Captain Savaria had a reasonable expectation of privacy regarding some of the documents seized but not on the document expert's report and the documents used as a basis for the expert's report. The Court pointed out that because a document is in the medical records of a Canadian Forces member does not necessarily mean that the document contains medical information automatically covered under a reasonable expectation of privacy. The Court also pointed out that a person cannot have a reasonable expectation of privacy in connection to a document which apparently contains precise medical information about the person but is in fact incorrect because of an alleged commission of a criminal offence or of a military offence in connection with that document. Captain Savaria's application under subsection 24(2) of the Charter for the exclusion of all the evidence on the condition that they were obtained in conditions that infringed his right to be secure against unreasonable seizure under section 8 of the Charter was thus dismissed.

1.5.2 CSIS and Security Issues

Ruby v Canada (Solicitor General), [2002](Supreme Court of Canada)[243]

A case on CSIS' refusal to disclose information.
Clayton Ruby ("R"), in pursuant to section 12(1) (a) of the Privacy Act ("PA"), requested access to personal information held in personal information banks-Bank 010 and Bank 015 maintained by the Canadian Security intelligence Service ("CSIS"). CSIS refused to confirm or deny the existence of information with respect to Bank 010, but said that if such information did exist, refused to disclose it, claiming exemptions under sections 19, 21, 22 and 26 of the PA. With respect to Bank 015, CSIS disclosed 41 pages information with portions excised claiming exemption under sections 21 and 26 of the PA. Ruby complained to the Privacy Commissioner, who investigated the complaint. As a result of the investigation, CSIS disclosed an additional four pages, portions of which were again excised as exempted under Sections 21 and 26 of the PA. At the conclusion of the investigation, the Privacy Commissioner found that CSIS' refusal to comment on the existence of information in Bank 010 was well founded, and, that except for two documents, the undisclosed information held in Bank 015 was properly exempted under the PA. The Privacy Commissioner asked the Solicitor General to disclose the two documents, but this request was refused. Ruby subsequently filed an application in the Federal Court, under section 41 of the PA, requesting a review of CSIS' refusal to disclose the information. Prior to the review, however, Ruby brought a motion challenging the constitutionality of sections 51(2) (a) and (3) of the PA, which allow the application of a government institution claiming a national security or foreign confidence exemption(s) to he heard in camera (without the public present) and ex parte (without the other party present). The constitutional challenge was on the ground that the exemption sections violate sections 2(b), 7 and 8 of the Charter. The motion judge ruled that the sections infringed section 2(b) of the Charter but that the infringement was justifiable under section 1 of the Charter, and that the sections 51(2) (a) and (3)of the PA did not violate section 7 of the Charter. The Federal Court of Appeal upheld this decision. Ruby appealed to the Supreme Court of Canada, and

[243] *Ruby v Canada (Solicitor General)* [2002] S.C.J No. 73.

CSIS cross-appealed on an issue regarding the interpretation of section 22(1) (b) of the Act. The Supreme Court held that sections 51(2) (a) and 51(3) of the Privacy Act do not violate s.7 of the Charter. On the issue of fair hearing, the Court stated that allowing a government institution to make ex parte submissions under section 51(3) is not contrary to the principles of fundamental justice. The Court also stated that the general rule of fair hearing which must include an opportunity for parties to know the opposing party's case, in order to address evidence prejudicial to their case, and bring evidence to prove their case, tolerates exceptions in some situations, requiring a measure of secrecy. In such situations, fairness can be met through procedural safeguards such as subsequent disclosure, judicial review and right of appeal. With respect to the in camera provision of section 51(2), the Supreme Court held that the provision violates section 2(b) of the Charter, to the extent that it excluded both Ruby and the public from the proceeding and cannot be saved by section 1. Given that section 51(2) mandates the entire hearing of a section 41 matter to be in camera, without limiting the in camera requirement to only the parts of the hearing involving the merits of an exemption, the Supreme Court held that section 51(2) must be read down so that it applies only to ex parte submissions mandated by section 51(3). On the cross appeal, the Supreme Court held that the exemption under section 22(1) (b) of the PA is not limited to current investigations or identifiable prospective investigation, and that CSIS was justified in claiming the exemption as it has established a reasonable expectation of probable injury to investigations in general.

Segasayo v Canada (Minister of Public Safety and Emergency Preparedness), [2008] 1 Federal Court Report 121[244]

A case on non-disclosure of materials.

The Applicant, a former Rwanda ambassador to Canada from 1991 to 1995 and his family, who were previously granted Convention refugee status by the Immigration and Refugee Board (the Board), applied for permanent residence. Before the determination of their application, the Minister of Citizenship and Immigration Canada ("CIC") designated the Rwandan government as a regime that engaged in homicide and crimes against humanity from October 1990 to April 1994, and from April 1994 to July 1994. Subsequently, the Applicant was advised by CIC that he was inadmissible to be landed in Canada, due to his prior status as the Rwandan ambassador of two regimes designated as having engaged in crimes against humanity. The Applicant sought ministerial relief under subsection 35(2) of the Immigration and Refugee Protection Act on the basis that he was not complicit in the crimes committed during the Rwandan genocide. The Minister of Public Safety and Emergency Preparedness ("the Minister"), in reliance on secret evidence, denied the application. The Applicant further sought judicial review of the Minister's decision. At the judicial review, the Board ("the Respondent") in support of its case produced a redacted certified tribunal record on the ground that disclosure of the redacted portions would be injurious to national security. The Respondent brought a motion before the court, asking for

[244] *Segasayo v Canada (Minister of Public Safety and Emergency Preparedness) (F.C.),* [2008] 1 F.C.R. 121

the non-disclosure of the secret evidence to the Applicant, his lawyer and the public, and for the secret evidence to be returned to it after the court proceeding rather than forming part of the Court file. In response to the motion for non- disclosure the Applicant brought a motion requesting a summary of the undisclosed evidence. Three issues were considered in this case. First, whether the Minister was entitled to rely on the secret evidence in deciding the application for ministerial relief. Second, whether the Minister breached the duty of fairness by not disclosing the secret evidence relied upon in deciding the Applicant's application for ministerial relief, and third, whether the Applicant was entitled to a summary of the secret evidence if non disclosure was ruled. On the first issue, both the Applicant and the Respondent agreed that the Act made no explicit provision on the authority of the Minister to rely on undisclosed secret evidence in reaching a decision on ministerial relief. However, the Court pointed out that there is also no limitation placed on the Minister in the Act, regarding what he or she is allowed to consider when making a decision. The Court considered two recent cases which have permitted the non disclosure of confidential material due to potential effect on national security, and ultimately held that the applicant failed to cite any jurisprudence disallowing the Minister from considering the information in making his decision. On the second issue, the Court held that there was no breach of the Applicant's right to procedural fairness. The Court emphasized that in reaching this decision, it weighed the duty of fairness to the Applicant to provide full and frank disclosure against the public interest in protecting information injurious to national security, and also considered that the secret evidence represented a very small portion of the information regarding the Applicant. Finally, on the last issue of providing the Applicant with a summary of the secret evidence, the Court held that importing the requirement to provide a summary of confidential information into the section at issue would be inconsistent with the legislative intent of the Act, and that, given the context and the nature of the information, providing a summary of the confidential information to the applicant may jeopardize foreign relations, betray the identity of informants, reveal sensitive national and foreign policy information and possibly endanger the lives of third parties. The Court upheld the motion for non-disclosure and dismissed the motion for a summary of the secret evidence.

1.5.3 Provincial Privacy Decisions

Order 2008-025 *Alberta Freedom of Information and Privacy Commissioner*

Attendance Board

The Edmonton Catholic Separate School District No. 7 ("The School Board") made a referral relating to the Complainant's son to the Attendance Board ("the Board" or "Public Body"). During the second hearing of this referral, the Attendance Board accepted into evidence a Psychological Assessment Report of a psychologist ("the Report") which contained the personal information of the Complainant, his son and a family member. The Board also ordered that a copy of this report be provided to the Complainant's son's school, ("the School") where it was placed in his son's file. The Complainant expressed concern about the Report being in his son's school file in a later hearing and subsequently filed a complaint that his personal information had been collected and disclosed by the Board in a manner contrary to the Freedom of Information and Protection of Privacy Act ("FOIP" or "the Act"). The complaint was assigned to a mediator but mediation was unsuccessful, and the matter proceeded to an inquiry. There were two issues to be decided at the inquiry. First, did the Public Body collect the Complainant's personal information in contravention of Part 2 of the FOIP? Second, did the Public Body disclose the Complainant's personal information in the contravention of Part 2 of the FOIP? On the first issue, the Board's argued that it collected the personal information of the Complainant in reliance on a combined reading of sections 127(e) and (h) of the School Act and sections 33(b) and (c) of the FOIP.

Section 127(e) of the School Act provides that the Board shall receive any relevant evidence presented to it, and section 127(h) provides that all documentary evidence received at a hearing forms part of the record of the proceeding. Section 33(b) permits collection for the purposes of law enforcement while section 33(c) permits collection of information that relates directly to and is necessary for an operating program or activity of a Public Body. The adjudicator accepted the Board's contention and found that collecting the Complainant's personal information by accepting the psychologist Report in evidence was in compliance with Part 2 of the Act. The adjudicator pointed out that admitting evidence

that is relevant to a matter before it, including evidence that consists of someone's personal information, relates directly to and is necessary for the operating program or activity of the Attendance Board in making the decisions, and issuing the orders, that it was constituted to make, and thus rightly within the terms of section 33(b) and (c) of the FOIP. The adjudicator also accepted that the parts of the Report that consisted of the Complainant's personal information were evidence that was relevant to the kinds of things the Board was empowered to decide in the case involving the Complainant. On the provision of section 127 of the School Act, the adjudicator opined that a provision which requires the admission of relevant evidence expressly authorizes the collection of any relevant evidence, including evidence that consists of any kind of personal information. On the second issue, the adjudicator rejected the Board's argument that its primary reason for disclosing the information was to give the School an opportunity to review the psychologist's recommendation, because the psychologist's recommendations were all contained in the final paragraph of the report and the disclosure of that part alone would have been adequate to achieve this objective. The adjudicator found that the disclosure of the Complainant's personal information by providing the psychologist's Report to the Complainants son's school contravened Part 2 of the FOIP as the connection between disclosure of this information to the School and the Boards' purpose for collecting the information- which was to inform its decision as to what directives to issue to the son and the parents respecting his attendance- was not sufficiently close to constitute a reasonable and direct connection within the terms of section 40(1) (c) of the FOIP, nor was the disclosure necessary within the terms of section 41 (b) of the FOIP for the Board to perform its statutory duties or operate its program of deciding how to enforce attendance requirements. Given that the School has already returned the Report to the Attendance Board, the adjudicator ordered that the Board refrain from making any such disclosure about the Complainant to the school in future.

Order F2009-005 *Alberta Freedom of Information and Privacy Commissioner*

University of Alberta

The Applicant submitted a proposal to the University of Alberta ("University") (the Public Body) for changes to a course, in the spring of 2007 and was informed by the Chair and Associate Chair of the department that there were numerous complaints about his proposal. The Applicant requested access to the written complaints about the proposed changes under the Freedom of Information and Protection of Privacy Act (the FOIP Act) and for the Teaching and Learning Enhancement Fund ("TLEF") grants application that he made. The University provided records it considered responsive to the two portions of the Applicant's request, but the applicant was dissatisfied and maintained that the University had not searched adequately for the records relating to the first part of his access request for the complaints about his proposed course changes. Given that mediation was unsuccessful in resolving the dispute, it was scheduled for inquiry.

The issue for the inquiry was whether the Public Body met its duty to the Applicant, as provided by section 10(1) of the FOIP Act. The University advanced evidence to establish that both the Chair and the Associate Chair of the department searched for the records, but the evidence showed that the University's search was limited to only those records located in the offices and computers of the Chair and the Associate Chair of the department. The adjudicator found that the University had not established that it had conducted an adequate search for responsive records in relation to the first part of the access request and therefore had not met its duty to assist the Applicant under section 10 of the FOIP Act. Part of the adjudicator's reasoning was that the Applicant's email which invited comments about the proposed course changes was sent to the entire department for comment and consequently, any complainants or response regarding the proposal in the email would come from members of the department. The adjudicator also pointed out that the Applicant did not limit his request to only those complaints that contained his name and in physical custody of the Chair or Associate Chair, because the Applicant's access request specifically requested for copies of all written complaints, notes of oral complaints and any other documentation including emails between the Chair and Associate Chair or anyone else pertaining to the proposed course changes. The Adjudicator ordered the University to conduct an adequate

search for responsive records in relation to the first part of the Applicant's access request including searching through its electronic back up files, if responsive records possibly existed in such files and to expand its keyword search for its electronic records. The adjudicator also ordered the University to expand its search to other employees in the department, if it determined that such search would locate further files, and if not, to communicate that conclusion and the basis for the conclusion to the Applicant. The University was given 50 days to notify the adjudicator in writing that it has complied with the Order.

The matter was appealed to the Alberta Court of Queen's Bench. Justice Don Manderscheid quashed the Adjudicator's decision to order a search of the backup records and remitted it back to the Adjudicator to receive evidence on whether the University could reasonably create the records (see: University of Alberta v Alberta (Information and Privacy Commissioner) 2010 Alberta Court of Queen's Bench 89.)

2.0 PRIVACY AND CANADA'S PRIVATE SECTOR

What privacy legislation regulates the private sector in Canada?

There are provisions in Canadian laws that protect Canadians from invasions of privacy by other individuals or companies. Common law rules govern the invasion of privacy. Also the *Criminal Code*[245] provides some protections. Finally, provincial and federal governments have passed some legislation that deals with the invasion of privacy by the private sector.

In 1994, the province of Quebec passed laws about the protection of privacy in the private sector.[246] In 1996, the Canadian Standards Association used the OECD Guidelines as the basis for development of a *Model Code for the Protection of Personal Information*.[247] Since 1996, The Uniform Law Commission of Canada has been working to develop a model law to regulate personal information in the non-governmental private sector. In 2000, the federal government passed the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").[248] The PIPEDA governs the collection, use and disclosure of personal information in the private sector.

Additionally, some provinces have introduced legislation dealing with health information and the private sector.[249] **Health information is discussed in detail in Chapter 1: Privacy Protection and the Government.**

2.1 CRIMINAL CODE

What privacy protections are there in the Criminal Code*?*

Section 184 makes it an indictable offence to willfully intercept (listen to, record, or acquire) a private communication using electro-magnetic, acoustic, mechanical or other device(s). There are some exceptions. It is not illegal if:

- one or all of the originators of the communication consent to it being intercepted;

---

[245] *Criminal Code of Canada*, Revised Statutes of Canada, 1985, chapter C-46.
[246] *An Act Respecting the Protection of Personal Information in the Private Sector*, SQ 1993, c P-39.1.
[247] Canadian Standards Association (1996). Model Code for the Protection of Personal Information (hereinafter CSA Model Code). Available online: https://privacyhorizon.wikispaces.com/CSA+Model+Code+for+the+Protection+of+Personal+Information
[248] *Personal Information Protection and Electronic Documents Act*, Statues of Canada 2000, Chapter 5 (hereinafter PIPEDA).
[249] See Chapter 1 section 1.2.3 (Protection of Health Information-The Alberta Example).

- the interceptor is a person who is providing telephone, telegraph or other services; or
- the interception is authorized (e.g., it is done by the police with court approval).

For a discussion of the rules and duties regarding police wiretaps see Chapter 3: Surveillance.

2.2 PROVINCIAL PRIVACY LEGISLATION

Is there any provincial legislation dealing with invasion of my privacy?

In four provinces—British Columbia, Manitoba, Saskatchewan and Newfoundland—legislation has been passed that permits individuals to sue others civilly for the invasion of privacy.[250] Under these laws, you can sue a person for violating your privacy, "willfully and without claim of right."[251] It is not necessary for the victim of an invasion of privacy to prove that there have been damages. Although "privacy" is not usually defined in these laws, conduct that could be an invasion of privacy includes:

- Surveillance of others,[252]
- Listening to or recording private conversations,[253]
- Using another person's name or likeness for commercial purposes,[254] and
- Making use of another person's diaries or letters (or other personal documents).[255]

---

[250] *Privacy Act,* Revised Statutes of British Columbia 1996, Chapter 373; *The Privacy Act,* Revised Statutes of Manitoba 1987, Chapter P125; *Privacy Act,* Revised Statutes of Newfoundland 1990, Chapter P-22; *Privacy Act,* Revised Statutes of Saskatchewan 1978, Chapter P-24.1. Quebec's *Civil Code* (Art 1457) has been used to award damages to someone for an invasion of privacy (see: *Robbins v C.B.C.* (1957), 12 Dominion L aw Reports (2d) 35 (Que.)), and the Quebec *Charter of Human Rights and Freedoms*, R.S.Q., c. C-12, guarantees to everyone the right to respect for his private life (see: *Aubry v Édition Vice-Versa Inc,* [1998] 1 Supreme Court Reports 591 – publication of a photograph was an invasion of privacy).

[251] In *Peters-Brown v Regina District Health Board* (1996), [1997] 1 Western Weekly Reports 638 (SKCA), the unauthorized publication of an employee's health status to others was a breach of privacy, but the defendant was not liable because the disclosure was not willful.

[252] In *L.A.M. v J.E.L.I,* [2008] BCJ No. 1612, the plaintiff was awarded general damages of $20,000, loss of earning opportunity of $5,000 and punitive damages of 35,000 against the defendant, for secretly videotaping her and her young daughter in the bathroom of his house through a peep hole. In *Malcolm v Fleming*, [2000] British Columbia Judgments Number 2400 (BCSC), the plaintiff was awarded $15,000 in compensatory damages and $35,000 in punitive damages when her landlord secretly videotaped her dressing and toileting herself over several years.

[253] In *Watts v Klaemt* [2007] BCJ No. 980, the plaintiff was awarded $30,000 in damages as against the defendant, for unlawfully invading her privacy by intercepting and recording cordless telephone conversations, and presenting the incriminating recorded conversations to the plaintiff's employer which resulted to her job termination.

[254] The publication of the name of a crime victim that was subject to a court-ordered publication ban was found to be an invasion of privacy in *F (JM) v Chappell* (1998), 158 Dominion Law Reports (4th) 430 (BCCA).

[255] In *Milton v Savinkoff*, (1993), 18 Canadian Cases on the Law of Torts (2d) 288 (BCSC) the circulation of a topless photograph of the plaintiff, which had been left in the possession of the defendant by accident, was held not to be a violation of her privacy. See also: P.H. Osborne, "Case Comment on Milton *v* Savinkoff" (1993) 18 Canadian Cases on the Law of Torts (2d) 292.

The legislation states that people are entitled to expect an amount of privacy that is reasonable under the circumstances.[256] Courts are instructed to look at the nature and impact of the conduct of the person who is accused of invading the privacy of another, the relationship between the people involved,[257] and any offer of apology or other amends for the conduct offered by the defendant.

The person sued for an invasion of privacy can rely on several possible defences to such a suit. These include:

- the plaintiff consented to the activity,
- the defendant was exercising a lawful right of defence of property or person,
- the defendant had legal authorization,
- it was a reasonable police investigation,
- it was reasonable news gathering,[258]
- the publication of the information was either in the public interest or fair comment on a matter of public interest, and/or
- the publication of the information would be a privileged communication within the law of defamation (see below).

When it is proved that there has been an invasion of privacy, the legislation permits several different possible remedies. These include:

- Damages;
- An injunction;
- An accounting for the profits that have been made as a result of the invasion of privacy; and/or

[256] For example, personal investigations and surveillance are permissible so long as a legitimate interest is at stake and the investigator is discreet and reasonable: *Davis v McArthur* (1970), 17 Dominion Law Reports (3d) 760 (BCCA). However, when an investigation intrudes into areas unrelated to its legitimate purpose, privacy may be violated: *Insurance Corp. of BC v Somosh* (1983), 51 British Columbia Law Reports 344 (BCSC).

[257] In *Pateman v Ross* (1988), 68 Manitoba Reports (2d) 181 (QB), the harassment of a newly married couple by the husband's ex-girlfriend was held to be actionable.

[258] In *Silber v British Columbia Broadcasting System Ltd*. (1985), 25 Dominion Law Reports (4th) 345 (BCSC), television coverage of a fight during a labour dispute was found not to be an invasion of privacy because it was newsworthy and it took place during the day at a public location. On the other hand, in *Hollinsworth v BCTV,* (1998), [1999] 6 Western Weekly Reports 54 (BCCA), the unauthorized release for television of a broadcast of a videotape of a person undergoing surgery designed to secure an artificial hairpiece was held to be an actionable invasion of privacy.

- An order for the surrender of the articles or documents that have been obtained through a violation of privacy.

There are relatively few reported decisions involving the invasion of privacy laws in these four provinces.

2.3 COMMON LAW AND PRIVACY

Do I have any other protections if the invasion of my privacy is not covered by legislation or the Charter of Rights*?*

Yes. Canadian common law has started to recognize that individuals may be able to sue others who have violated their right to privacy.[259] In the United States, a separate right to privacy has existed for many years.[260] However, in Canada, it is still developing. Traditionally, courts relied upon well-established torts (civil wrongs) to provide an indirect protection of privacy rather than to create the independent tort of invasion of privacy. Thus, in some cases involving invasion of privacy, lawsuits were usually based on actions in trespass to land, nuisance,[261] the intentional infliction of nervous shock, negligence, appropriation of one's personality[262] and trespass to chattels.[263]

The Supreme Court of Canada has not yet considered whether a common law tort of invasion of privacy exists in Canada. However, some lower courts have recognized the tort of intrusion upon seclusion which is when someone intentionally intrudes upon another's private affairs.[264] This, so far, has been the closest the common law has come to recognizing the tort of invasion of privacy. Other examples of similar invasion of privacy torts include being found liable for the unauthorized taping and publication of a private conversation,[265] the intrusive aiming of a surveillance camera

[259] See generally: Craig.
[260] A. Linden, *Canadian Tort Law*, 6th ed. (Toronto: Butterworths, 1997) at 56.
[261] See, for example, *Motherwell v Motherwell*, (1976), 73 Dominion Law Reports (3d) 62 (Alta CA), where the court held that harassing telephone calls fell within the law of nuisance, thus causing the plaintiffs to lose the enjoyment of their property.
[262] *Krouse v Chrysler Canada Ltd.*, [1970] 3 Ontario Reports 135 (ONHC).
[263] Osborne.
[264] *Jones v Tsige*, 2012 ONCA 32, 108 OR (3rd) 241.
[265] *Watts v Klaemt,* [2007] BCJ No 980.

into a tenant's suite,[266] harassment,[267] harassment by a debt collector,[268] and the disclosure of a sexual assault on an undercover officer.[269]

When it has been proven under common law that a person is liable for the invasion of privacy of another, the usual remedy is an award of money damages.

What about the duty of confidentiality on professionals?

While confidentiality and privacy are not exactly the same thing, the duty of confidentiality is closely related to privacy. Professionals, such as doctors and lawyers, are generally under a duty to keep the information they get about their patients or clients confidential.[270] At common law, the duty of confidentiality can be found in contract law and in tort law. First, in every contract between a patient (or client) and a professional, there is an unwritten understanding that the professional will keep the patient's confidences. If this is broken, the patient or client could sue for breach of contract. Second, if a physician negligently discloses a patient's information and it causes some foreseeable injury to the patient, the patient could sue (in tort law) for the professional's negligence. Third, the Supreme Court of Canada has also recognized that the relationship between a physician and a patient is one in which a patient's trust and confidence are both placed in the physician.[271] Because the patient is vulnerable in this type of relationship, it is a special relationship called a fiduciary relationship. This type of relationship places certain duties on the physician including the physician's duty to keep any information she gets from or about her patient as confidential. Should the physician break this confidence, the patient could also sue for the physician's breach of a fiduciary duty.

In addition to a professional's common law duties in contract law and tort law, there are also a variety of professional rules that impose the duty on professionals to keep their patients 'or clients' information confidential. In these rules, professional bodies are given the power to punish any

---

[266] *Heckert v 5470 Investment Ltd.,* [2008] BCJ No. 1854

[267] *Roth v Roth* (1991), 4 Ontario Reports (3d) 740 (Gen Div); *MacKay v Buelow* (1995), 24 Canadian Cases on the Law of Torts (2d) 184 (Ont Gen Div); *Nagy Farms Ltd v Repsys,* [1987] Ontario Judgments Number 1987 (Ont Dist Ct).

[268] *Tran v Financial Debt Recovery Ltd.,* [2000] Ontario Judgments Number 4293 (Sup Ct); *Dawe v Nova Collection Services* (Nfld) Ltd., [1998] Newfoundland Judgments Number 22 (Prov Ct).

[269] *R(L) v Nyp* (1995), 25 Canadian Cases on the Law of Torts (2d) 309 (Ont Gen Div).

[270] W. F. Flanagan, "Genetic Data and Medical Confidentiality" (1995) 3 Health Law Journal 269 at 270 (hereinafter Flanagan).

[271] *McInerney v MacDonald* (1990), 103 New Brunswick Reports (2d) 423 (NBCA); affirmed [1992] 2 Supreme Court Reports 138 (SCC).

professional misconduct by professionals under their review, which usually includes a breach of a patient's or client's confidentiality. To help define what inappropriate conduct is, these disciplinary bodies usually put out a code of ethics or a book of standards, which is a guide book of the way members of the profession are supposed to act. Punishments from these types of bodies may vary from reprimands to removal from the association.

Are there exceptions to the duty of confidentiality?

Yes. A professional can disclose a patient's information without his patient's consent in some situations. The following provide examples where medical professionals may break their duty of confidentiality without their patient's consent: [272]

- In Court: For example, courts have never recognized that medical professionals enjoy any particular privilege of silence in court proceedings.
- When a Specific Law Requires It: Some laws may require that a professional disclose a client's information, with or without the client's consent, in order to further some very important public good. This type of legislation is most common in the area of communicable diseases. The legislation not only permits a physician to disclose the information, but often there is a penalty for not disclosing the information you were supposed to.
- To Protect a Paramount Public Interest: Disclosure may also be necessary in order to prevent harm to others, even though there may not be a specific law saying that it is allowed or necessary. In these cases the courts attempt to strike a balance between the confidentiality/privacy interests of the patient/client with the public's interest in preventing harm to others.
- When an Identifiable Third Party Is At Risk: Older court cases show that a physician may be held liable for the foreseeable injury that one of her patients/clients causes to a third party who could be identified as being at risk. The older cases in this area of exceptions have mostly involved psychiatric patients who presented a reasonably foreseeable risk of violent assault or reckless behaviour. The risk to the third parties was immediate and life threatening.

[272] Flanagan, at 274 - 279.

For more information about the collection, use and disclosure of health information, see Chapter 1: Privacy Protection and the Government.

2.4 DATA PROTECTION ACT

Does privacy legislation ever apply to people and organizations outside of the government?

Yes. In 2000, the federal government passed legislation dealing with privacy and the private sector. This is called the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").[273] Some provinces have also passed or are working on legislation dealing with privacy and the private sector.

PIPEDA gives you the right to see and ask for corrections to information that an organization may have collected about you.[274]

What is the purpose of the PIPEDA?

The purpose of the PIPEDA is stated to be:

> [t]o 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.

What does the PIPEDA cover?

There are five parts to the PIPEDA. Part 1 refers to the *Model Code for the Protection of Personal Information*, also known as the *Canadian Standards Association Model Code* ("CSA Model Code"), reproduced in Schedule 1, and deals with the protection of personal information in the private sector. Parts 2 to 5 deal with federal legislation in electronic format. These sections largely deal with providing for electronic filing of legal documents and with giving legal effect to electronic documents, and are not discussed in this book.

---

[273] *Personal Information Protection and Electronic Documents Act*, Statutes of Canada 2000, Chapter 5 (hereinafter "PIPEDA").

[274] Office of the Privacy Commissioner of Canada, *Your Privacy Rights*, 2001.

Part 1 sets ground rules for how organizations may collect, use or disclose information about you in the course of commercial activities.

What is the CSA Model Code?

This was drafted from 1993 to 1995 by Canadian businesses, with input from provinces, consumer groups and provincial privacy commissioners.[275] The CSA Model Code was developed to help businesses and other organizations manage personal information in a way that respects the privacy rights of the people with whom they deal.[276] The CSA Model Code contains ten principles. Each principle is followed by paragraphs that explain the principle further. The CSA Model Code is reproduced below, following a brief description of the ten principles. They are:

Accountability — each organization is responsible for information in its care and must appoint someone to be responsible for complying with the principles in the Model Code.

Identifying Purposes — organizations must identify the purposes for which they are collecting, using and disclosing personal information, at or before the time the information is collected.

Consent – the individual's knowledge about the personal information and the consent of the individual are required before it is collected, used or disclosed.

Limiting Collection — collection of personal information is limited to that which is necessary for the purposes and the purposes must be specified. Information must be collected by fair and lawful means.

Limiting Use, Disclosure and Retention — personal information must not be used or disclosed other than for the purposes for which it was collected — except as required by law or if the individual consents. Personal information must only be retained as long as necessary to fulfill the purposes for which it was collected.

Accuracy — personal information must be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.

Safeguards — personal information must be protected by safeguards appropriate to the sensitivity of the information.

Openness — there is an obligation to make specific information available about policies and practices relating to the management of personal information.

---

[275] S. Perrin, H. Black, D. Flaherty and T. M. Rankin, Q.C. *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law Inc., 2001) at 4 and 11 (hereinafter Perrin).

[276] Perrin, at 13.

Individual Access — organizations must inform people, on request, about the information that the organization holds about them, and what use is being made of it. Individuals have the right to find out to whom the information has been disclosed and they can challenge the information's accuracy and completeness.

Challenging Compliance — individuals have the right to challenge an organization's compliance with any of the ten principles, and the individual complaining does not have to be the subject of the information in question.

THE CSA MODEL CODE IS REPRODUCED IN THE APPENDIX.

How does the CSA Model Code relate to the PIPEDA?

The CSA Model Code was used as the basis for the PIPEDA. It is included in a Schedule to the Act. The provisions in the PIPEDA add to, modify and clarify the CSA Model Code.

What is "personal information" under the PIPEDA?

"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. It includes health information. Unlike the definitions of personal information found in governmental privacy legislation, "personal information" is not limited to information that is recorded. Thus, tissue information and bodily fluids, such as blood and urine samples are considered "personal information."[277]

What information is not covered under the PIPEDA?

The PIPEDA does not apply to:[278]

- any government institution to which the *Privacy Act* applies (**see Chapter 1**);
- individuals who collect, use or disclose personal informational for purely personal or household purposes (e.g., personal address book); or
- organizations that collect, use or disclose personal information solely for journalistic, artistic or literary purposes (e.g., newspapers, publishing houses, artists, writers).

[277] Perrin, at 53.
[278] PIPEDA, subsection 4(2).

To whom does the PIPEDA apply?

The PIPEDA applies to any personal information that an organization collects, uses or discloses in the course of a commercial activity.[279]

"Organization" includes an association, a partnership, a person and a trade union.[280] A "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.[281]

The PIPEDA also applies to information about an employee of an organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.[282] A "federal work, undertaking or business" means any work, undertaking or business that is within the legislative authority of Parliament.[283] Examples of federal works include navigation and shipping businesses, railways, telegraphs, canals, ferries, aircraft, radio and television broadcasting, banks, and other works.

If the information is exchanged over a provincial or federal border, there is a good chance that the PIPEDA applies.

The PIPEDA also applies to the Atomic Energy of Canada Limited, the CBC and the Enterprise Cape Breton Corporation.[284]

Why does the PIPEDA only apply to personal information about the employee of a **federal** *work, undertaking or business?*

Making laws about personal information collected in the course of commercial activities is within the trade and commerce power of the federal Parliament. However, laws regarding personal information about labour relations and employment issues are within the jurisdiction of the

[279] PIPEDA, paragraph 4(1)(a).
[280] PIPEDA, subsection 2(1).
[281] PIPEDA, section 2(1).
[282] PIPEDA, paragraph 4(1)(b).
[283] PIPEDA, subsection 2(1).
[284] *Order Binding Certain Agents of Her Majesty for the Purposes of Part 1 of the Personal Information Protection and Electronic Documents Act* (SOR/2001-8).

provinces (dealing with property and civil rights).[285] However, the labour relations or employment issues arising in the context of a federal work, undertaking or business are under the jurisdiction of the federal government.

Note, however, if the personal information is collected as part of a *commercial activity,* the PIPEDA will apply, whether or not the business is under federal jurisdiction.

I heard that the PIPEDA does not apply to provincial organizations. Is that correct?

The PIPEDA came into effect in three stages. In 2001, PIPEDA applied to federally regulated industries (such as airlines, banking and broadcasting). In 2002 the law was expanded to include the health sector. Finally in 2004, any organization that collects personal information in the course of commercial activity was covered by PIPEDA, including organizations under provincial jurisdiction. However, if the organization carries on business within a province that has substantially similar law, and the province has been exempted by an order of the Governor in Council, the PIPEDA will not apply to the organization for any collection, use and disclosure of personal information within the province. The PIPEDA will still apply to any interprovincial and international collection, use and disclosure of personal information.[286] Four provincial privacy laws have been declared by the federal Governor in Council to be substantially similar to PIPEDA:

- *An Act Respecting the Protection of Personal Information in the Private Sector* (Quebec).
- The *Personal Information Protection Act* (British Columbia).
- The *Personal Information Protection Act* (Alberta).
- The *Personal Health Information Protection Act* (Ontario).
- The *Personal Health Information Privacy and Access Act* (New Brunswick).
- The *Personal Health Information Act* (Nova Scotia).
- The *Personal Health Information Act* (Newfoundland and Labrador).

[285]Some provinces have indicated that they may challenge the constitutionality of using the trade and commerce power to deal with privacy in the private sector: See Perrin, at 58.
[286]Perrin, at 159-60.

How does an organization know what its obligations are under the PIPEDA?

The PIPEDA states that every organization must comply with the obligations set out in Schedule 1.[287] These are the ten principles from the CSA Model Code. The PIPEDA also states that when the CSA Model Code says "should", it is merely a recommendation and not a legal obligation. This is because in legislation the word "should" usually imposes a strict legal obligation. However, the CSA Model Code is a list of recommendations, not obligations.[288] Nevertheless, obligations under the CSA Model Code are indicated when the words "shall" or "must" are used.

If an individual is designated by an organization as the person responsible for the organization's accountability, the organization as a whole is still obligated to comply with the CSA Model Code.[289]

When can an organization collect, use or disclose personal information about me?

The PIPEDA provides that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.[290] The reasonable person test is an objective test that has been used in law for many years. This means that an organization must be able to justify why it is collecting, using or disclosing personal information.

Are there situations when an organization can collect, use or disclose my personal information without my consent?

Yes. The PIPEDA is based on the principle of consent. The basic requirement is that the knowledge and consent of the individual are required for the collection, use and disclosure of personal information, except where inappropriate.[291] The PIPEDA sets out three lists defining circumstances where it might not be appropriate to seek the individual's consent.

Collection:

First, an organization may collect information without your consent only if:[292]

- the collection is clearly in the interests of the individual concerned and consent cannot be obtained in a timely way (e.g., obtaining a family member's cell phone number in order to inform him or her of a medical emergency);

[287] PIPEDA, subsection 5(1).
[288] PIPEDA, subsection 5(2).
[289] PIPEDA, section 6.
[290] PIPEDA, subsection 5(3).
[291] PIPEDA, section 3.
[292] PIPEDA, subsection 7(1).

- it is reasonable to expect that the collection with consent or knowledge would compromise the availability or accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of a law (e.g., in investigating a potential insurance fraud, to obtain a claimant's employment records);
- the collection is solely for journalistic, artistic or literary purposes (this makes a distinction for information that is collected for these purposes from when it is disclosed or used for another purpose);
- the information is contained in a witness statement and is necessary to asses, process, or settle an insurance claim;
- the information is publicly available and is specified by the regulations. Information specified by the regulations includes:[293]
    - the name, address and telephone number of a subscriber that appears in a public telephone directory;
    - the name, title, address and telephone number of an individual that appears in a professional or business directory, that is available to the public, where the collection, use and disclosure of the personal information relates directly to the purpose for which the information appears in the directory;
    - personal information in a registry collected under law and to which a right of public access is authorized by law, where the collection use and disclosure relates directly to the purpose for which the information appears in the directory;
    - personal information appearing in a record or document of a judicial or quasi-judicial body, where the collection use and disclosure relates directly to the purpose for which the information appears in the directory;
    - personal information that appears in a publication, such as a magazine, book, or newspaper, that is available to the public, where the individual has provided the information.

Use:

Second, an organization can use personal information without your knowledge or consent only if:[294]

- the organization becomes aware of personal information that it has reasonable grounds to believe could be useful in the investigation of a federal, provincial or foreign law. The

[293] *Regulations Specifying Publicly Available Information* (SOR/2001-7).
[294] PIPEDA, subsection 7(2).

contravention must have been committed, be about to be committed or be in the course of being committed;

- the personal information is used by an organization in an emergency that threatens your life or someone else's life;
- the information is contained in a witness statement and use is necessary for an insurance claim;
- information was produced by the individual in the course of business or employment
- the personal information is used for statistical purposes, or scholarly research or study and
    - the statistical purpose, study or research cannot be achieved without using the information;
    - the organization uses the information in a way that ensures it stays confidential;
    - it is impractical for the organization to obtain consent (e.g., the information is old and the people are hard to trace); and
    - the organization informs the Privacy Commissioner of the use before it happens.
- the personal information is publicly available and is specified by the regulations (see discussion above about regulations); or
- the personal information was collected without the knowledge or consent of the individual under PIPEDA paragraphs 7(1)(a) [collection clearly in the individual's interest and consent cannot be obtained in a timely way], 7(1)(b) [collection with knowledge or consent would compromise the availability or accuracy of the information and the collection is reasonable for purposes related to a breach of an agreement or contravention of federal or provincial law] or 7(1)(e).

Disclosure:

Third, an organization can disclose personal information without your knowledge or consent only if the disclosure is:[295]

- made to a lawyer who is representing the organization;
- for the purpose of collecting a debt owed by you to the organization;
- to comply with a subpoena, warrant, provincial Rules of Court, or order issued by a court, person or body with jurisdiction to compel production of information;

[295] PIPEDA, subsection 7(3).

- made to a government institution or part of a government institution that has requested the information, has identified its lawful authority to obtain the information and that it has the right to the information, and has indicated that:
    - It suspects the information relates to national security, to the defence of Canada or to the conduct of international affairs;
    - The disclosure is requested for the purpose of enforcing federal, provincial, or foreign law, or carrying out an investigation relating to these laws, or gathering intelligence in order to enforce these laws (these are activities that would occur before a warrant is issued);
    - The disclosure is requested for the purpose of administering any provincial or federal law;
- made to the Financial Transaction and Reports Analysis Centre of Canada established under the *Proceeds of Crime* (*Money Laundering) Act.*[296] This Act requires banks, financial institutions, lawyers, accountants and others to report suspicious transactions, as well as regular transactions involving dollar amounts over certain limits);
- made on the initiative of the organization to an investigative body, a government institution or part of a government institution if the organization:
    - Has reasonable grounds to believe that the information relates to the breach of an agreement or private contract, or to the contravention of federal, provincial or foreign laws; or
    - Suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
- Necessary to identify the individual who is injured, ill or deceased made to a government institution;
- made to a person because of an emergency where your life, health or security are in jeopardy. The organization must inform you of the disclosure in writing without delay;
- for statistical or scholarly study or research. It must be demonstrated that the purposes cannot be achieved without disclosing personal information, it is not practical to obtain consent and that the Privacy Commissioner has been informed before the information is released;

[296] Statutes of Canada 2000, chapter 17.

- to an archival or historical institution in order to conserve the information;
- made after the earlier of
    - one hundred years after the record containing the information was created, and
    - twenty years after the death of the individual whom the information is about;
- of information that is publicly available and is specified by the regulations (see above under collection); or
- required by law.

These exceptions to the requirement of consent and knowledge apply despite what is stated in the CSA Model Code in Schedule 1.[297]

How do I gain access to my personal information under PIPEDA?

A request for access to personal information about yourself must be made in writing.[298] It may be done electronically.[299] Organizations must assist you in preparing your request if you ask them to.[300]

An organization must answer your request for access to information promptly and not later than thirty days after receiving the request. The organization may extend the time required to respond for an additional thirty days if meeting the original time limit will unreasonably interfere with the activities of the organization or if the organization needs to make consultations in order to meet your request.[301] Organizations can also extend the period in order the convert the personal information into an alternative format (e.g., into a format that allows a person with a sensory disability to read or listen to the personal information). If an organization is extending the time limit, it must notify you and provide a reason why it needs an extension. The organization also has to inform you of your right to complain to the Privacy Commissioner about the extension.[302] If the organization does not respond to you within the time limit, the organization will be deemed to have refused access to the information.[303]

[297] PIPEDA, section 7.
[298] PIPEDA, section 8.
[299] PIPEDA, section 41.
[300] PIPEDA, subsection 8(2).
[301] PIPEDA, subsections 8(3) and (4).
[302] PIPEDA, subsection 8(4).
[303] PIPEDA, subsection 8(5).

Organizations must provide access to personal information in an alternative format (e.g., in Braille or on a tape) if the person asks. The organization must give access in the alternative format if the information exists in the alternative format or if it is reasonable to convert it and conversion is necessary for you to have meaningful access to the information.[304]

Organizations must provide reasons in writing for a refusal to grant access to personal information and must also inform you that you have a right to complain to the Privacy Commissioner.[305] If an organization decides not to give access to personal information under some circumstances, the organization must notify the Privacy Commissioner.[306]

An organization must retain any personal information that is the subject of a request for as long as necessary for you to exhaust your possible recourses under the PIPEDA (e.g., to complain to the Privacy Commissioner).[307] If the organization knowingly breaks this law, it is guilty of an offence under the PIPEDA.[308]

Can I be charged a fee for access to my personal information?

Yes. However, organizations are usually expected to charge nothing or very little. If they charge you, they must first inform you of the approximate cost and then must not charge the fee until you have advised the organization that the request is not withdrawn.

Are there any circumstances when I cannot gain access to my personal information?

Yes. There are circumstances when the organization must not release personal information, circumstances when the organization may not release personal information and circumstances when, if you request access to personal information, the organization must notify the government.

The organization must not release personal information if doing so would likely reveal personal information about another person unless:[309]

- the two pieces of information can be severed from each other;

[304] PIPEDA, section 10.
[305] PIPEDA, subsection 8(7).
[306] PIPEDA, subsection 9(5).
[307] PIPEDA, subsection 8(8).
[308] PIPEDA, section 28.
[309] PIPEDA, subsections 9(1) and (2).

- the other person consents to the release; or
- the information is needed because someone's life, health or security is threatened.

The organization may not release personal information if:[310]

- The information is protected by solicitor-client privilege;
- To do so would reveal confidential commercial information, provided the information could not reasonably be severed;[311]
- To do so could reasonably be expected to threaten the life or security of another individual, provided that the information could not reasonably be severed;
- The information had been collected under s. 7(1)(b), which deals with investigating the breach of an agreement or law, provided that the information could not reasonably be severed;
- the information was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act;*
- The information was generated during a formal dispute resolution process.

Nevertheless, if an individual needs the information because an individual's life, security or health is threatened, access must be provided.[312]

There are several steps an organization must follow if:

- you ask an organization whether it has disclosed your personal information to a government institution because of a warrant or subpoena, for national security or law enforcement reasons, or to report a suspicious transaction;
- you want to know if there is information about any such disclosure; or
- you ask for access to information that would reveal a request made by a law enforcement or national security agency.

First, the organization must inform the government institution of the request and must not respond to your request until the government approves the release of or access to the information.

---

[310] PIPEDA, subsection 9(3).

[311] In February, 2002, the federal Privacy Commissioner received a complaint that a bank would not release an internally generated credit score to a customer. The Commissioner found that the internal credit scoring system was confidential commercial information and did not have to be revealed. See: "Privacy Commissioner releases his finding on a bank's refusal to release credit score" (https://www.priv.gc.ca/en/).

[312] PIPEDA, subsection 9(4).

Alternatively, if thirty days have passed since the government institution was notified, and the government has not notified the organization, the organization can release the personal information.

Second, the government's grounds for objecting to the release of the information in these circumstances (when you have asked an organization if it has released information to the government about you) are that allowing release could reasonably be expected to injure:[313]

- national security, the defence of Canada or the conduct of international affairs;
- the detection, prevention or deterrence of money laundering; or
- enforcement of Canadian, provincial or foreign law or intelligence gathering for the purpose of enforcing these laws.

Third, if the government institution objects to the release of this information within the thirty day period, the organization must refuse access to any personal information that would reveal that the organization had formed a suspicion, considered whether to make a report, made a report, notified the government institution, and that the government had objected to the release of the information. Further, the organization must inform the Privacy Commissioner that it has refused to release all of this information, and it cannot tell you that it has informed the Privacy Commissioner.[314]

Thus, if these events have occurred, you will never know that a suspicious transaction report has been made.

What if I have a complaint under PIPEDA?

First, you will use the complaint process established by the organization itself. If that does not resolve the problem, you can file a written complaint with the Privacy Commissioner.[315] Any complaint about a refusal to give access to your personal information must be filed within six months of the refusal. The Privacy Commissioner might allow for a period longer than six months.[316] Once the Privacy Commissioner receives the complaint, he or she will notify the organization against which you have complained.[317] The Privacy Commissioner must then investigate the complaint.

[313] PIPEDA, subsection 9(2.3).
[314] PIPEDA, subsections 9(2.4) and (5).
[315] PIPEDA, section 11.
[316] PIPEDA, subsection 11(3).
[317] PIPEDA, subsection 11(4).

When investigating a complaint, the Privacy Commissioner has numerous powers, including the ability to issue a summons and enforce the appearance of persons, to compel them to provide oral evidence under oath, and to compel persons to produce records and other things necessary to investigate the complaint. The Privacy Commissioner can also enter the organization, after satisfying any security requirements of the organization. The Commissioner can speak privately with other people on the organization's premises and can look at paper or computer files. The Commissioner is allowed to take copies of any relevant records he or she finds on the premises.[318]

The Privacy Commissioner can seek to resolve complaints using dispute resolution mechanisms such as mediation and conciliation.[319]

Within one year after the complaint is initiated, the Commissioner must prepare a report that contains his or her findings and recommendations, any settlement that was reached by the parties and a request that the organization provide the Commissioner with a time limit for when it will implement any changes the Commissioner has recommended.[320] The report must also list any recourse that is available to the complainant, such as an appeal to the Federal Court.

Can I get fired if I blow the whistle on my employer on a privacy issue?

The PIPEDA has whistleblower protections for individuals or employees. Anyone complaining about a contravention of the PIPEDA can request that the complaint be kept confidential.[321] Also, the PIPEDA says that the employer cannot fire, suspend, demote or otherwise discipline you because you reported to the Privacy Commissioner in good faith about your belief that your employer has or is going to contravene the PIPEDA, sections 5 to 10.[322]

[318] PIPEDA, subsection 12(1).
[319] PIPEDA, subsection 12(2).
[320] PIPEDA, subsection 13(1).
[321] PIPEDA, section 27.
[322] PIPEDA, section 27.1.

Also, if a person knowingly contravenes the whistleblower provision with regard to an employee, he or she can be fined up to $10,000 if the offence is summary conviction and $100,000 if it is indictable.[323]

What is the role of the Privacy Commissioner under the PIPEDA?

In addition to investigating complaints made by others, the Privacy Commissioner can initiate complaints, if he or she is satisfied that there are reasonable grounds to do so.[324]

Any recommendations made by the Privacy Commissioner after an investigation does not have to be followed by the organizations. However, the Privacy Commissioner can apply to the Federal Court, which can make binding decisions. Also, the Privacy Commissioner can perform audits on organizations and the results can be reported to Parliament.

Can I appeal the decision of the Privacy Commissioner?

Yes. Once receiving the Privacy Commissioner's report, the complainant can apply to the Federal Court Trial Division to review any matter complained of or that is referred to in the Commissioner's report and referred to under section 14 of the PIPEDA. Examples include whether an organization has taken the necessary steps to safeguard the information, whether the information was collected, used or disclosed without the consent of the individual in circumstances not authorized under the PIPEDA, or whether an organization refused to provide service because a person would not provide more information than was necessary to fulfill the legitimate purposes. The Privacy Commissioner may also apply to the Federal Court for a review in these matters.[325]

Applications for review must be made within one year after the report is sent. The court may grant an extension if it is applied for within the one year period.[326]

The Federal Court Trial Division has general power to grant remedies, and some special powers under the PIPEDA. The Court can also:[327]

- order an organization to correct its practices in order to comply with the PIPEDA;

[323] PIPEDA, section 28.
[324] PIPEDA, section 11(2).
[325] PIPEDA, section 14.
[326] PIPEDA, subsection 14(2).
[327] PIPEDA, section 16.

- order an organization to publish a notice of any action taken by the organization or which the organization proposes to take to correct its practices, whether or not it was ordered by the court to do so; or
- award damages to the complainant, including damages for any humiliation that the individual has suffered.

The decision of the Federal Court Trial Division may be appealed to the Federal Court of Appeal.[328] In limited circumstances, such as if the Supreme Court of Canada grants leave to appeal, the matter may be appealed further.

What are audits used for?

The Privacy Commissioner has the power to audit the personal information management practices of an organization if:[329]

- reasonable notice is given to the organization;
- the audit takes place at a reasonable time (e.g., during business hours); and
- the Commissioner has reasonable grounds to believe that the organization is contravening Division 1, sections 5 to 10, or that is not following a recommendation listed in Schedule 1.

In conducting an audit, the Commissioner has the same powers that she or he has when investigating. Also, the Commissioner has the power to make public any information about the personal information management practices of an organization if the Commissioner thinks it is in the public's interest to do so.[330]

Once the audit is complete, the Commissioner must provide the organization with a report, which contains the findings of the audit and the Commissioner's recommendations. The Commissioner can include an audit report in his or her annual report to Parliament.[331]

---

[328] *Federal Court Act,* RSC 1985, c F-7.
[329] PIPEDA, section 18.
[330] PIPEDA, subsection 20(2).
[331] PIPEDA, section 19.

2.5 SPECIFIC ISSUES IN PRIVATE SECTOR INFORMATION AND PRIVACY

2.5.1 Social Insurance Numbers

What are Social Insurance Numbers used for?

A Social Insurance Number ("SIN") is an identifying number given by the government to citizens who apply, usually once they reach an age when they can be formally employed. The SIN is used by the government to collect taxes and to administer some other social programs. Originally, the SIN was created in 1964 to replace the national unemployment insurance number and for a new pension plan. From these original two purposes, the SIN has become the most common unique personal identifier in Canada.[332]

Who can ask for my Social Insurance Number?

Although anyone can ask you for your SIN, only certain individuals or organizations can do so legitimately. Primarily you will provide your SIN to the government for the administration of social programs and for tax purposes. Instances when you will be required to provide your SIN include:

- for Old Age Security, Employment Insurance and Canada Pension Plan contributions or claims;
- for Income Tax identification;
- to your employer for government tax and benefit programs;
- to banks and other financial institutions if you receive revenue from a product or service;
- for Canada Student Loans; and
- for some Native peoples' programs.

Employers and financial institutions are prohibited from sharing your SIN with anyone who is not allowed to receive it under the law. Frequently, you are asked for you SIN because it is a useful identification number that is widely used. Sometimes you may be asked for your number so that a credit check can be performed on you as credit bureaus use SINs as identification. When an organization or individual asks you for your SIN, you do not have to

[332] D. Johansen, *Social Insurance Numbers: Regulating Their Use* Background Paper, Law and Government Division BP-206E (Library of Parliament, 1989 revised 1992).

provide it. Unfortunately, though, there is no law that forbids someone from refusing you a service if you do not give them your number, but there are good reasons to ensure that you give your SIN to only qualified recipients.

If a SIN is just a number, why should I care about whether others use it or not?

The SIN is powerful because it is so widely used. A great deal of information is thus accessible through the number. Computer technology makes it possible to use the SIN to match files from different sources to create one detailed and comprehensive file on an individual. This is a common worry that arises when proposals for a national identification card are discussed. Your privacy may be violated when there is a concentration of personal information to which you have no access and over which you have no control about its use.

There are also many abuses of SINs because they are used too frequently and freely. When people defraud the government by using a SIN that is not their own, all of society pays because service programs are more expensive to deliver. It is in everyone's best interest to ensure that SINs are used only when required by law.

What can I do to limit the use of my SIN?

If someone asks you for your SIN and you are not certain if they are legally allowed to request it, you can first ask the person if it is required by law that you give your SIN. This forces the person to justify the request. You can also ask why the person needs it, how it will be used, and to whom it will be given. This ensures company policies are well thought out. If giving your number is not required by law and you are not satisfied with the explanation given, you can decline to give your SIN and offer other identification in its place. Providing an alternative means for the company to meet its policy goals will hopefully allow you to still receive the product or service. If you are denied the product or service because you did not give your SIN, you may complain to management. You can also pursue a complaint through your provincial or federal privacy commissioner or contact your Member of Parliament.

2.5.2 Credit Bureaus

Introduction

Many people are unaware of how the credit industry works. Even if they go through a credit check at the bank before being approved for a credit card, they may not be fully informed about what

information is collected and how it is stored. Decisions made about your credit history can have a large impact on your ability to purchase items or take out a loan.

Who is involved in the credit industry?

The credit industry consists mainly of credit reporting agencies, also known as credit bureaus. Credit reporting agencies collect personal and financial information on individuals' borrowing and re-payment histories from other businesses involved in the credit industry—such as retail stores, landlords, employers, insurance companies, banks and trust companies. These businesses then pay a fee to obtain access to the information about consumers after it is compiled and updated by a credit reporting agency.[333] Because you apply for credit at one of these businesses, they are known as credit grantors.

There are two major credit reporting agencies in Canada: Equifax and Trans Union Corporation.[334] According to Equifax, its customers include banks, retailers, wholesalers manufacturers, government agencies, insurance companies, public utilities and other financial service companies.[335] Trans Union describes itself as a "clearinghouse" that collects and stores factual information about credit and financial history. In addition to information supplied by businesses such as those described by Equifax, Trans Union also collects public record information obtained from courthouses.[336] It is evident then that the amount of information available to these companies is diverse and detailed. All this data is collected in a consumer's credit file.

---

[333] E. Shaw, J. Westwood and R. Wodell, *The Privacy Handbook: A Practical Guide To Your Rights in British Columbia and How To Protect Them* (Vancouver: B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association, 1994), at 155 (hereinafter Shaw, Westwood and Wodell).

[334] Contact the companies for a complaint or to see your credit file.

Equifax Credit reporting agency
110 Sheppard Avenue East
Toronto, ON M2N 6S1
1-800-465-7166 or
(416) 227-5290

Trans Union Canada Inc.
Consumer Relations Centre
P.O. Box 338, LCD 1
Hamilton ON L8L 7W2
1-800-663-9980 or (905) 525-0262

In Quebec, see Northern Credit Bureaus
336 Rideau Boulevard
Rouyn - Noranda, QC J9X 1P2
Fax: 1 (800) 646-5876

[335] See Equifax's website at www.equifax.com?EFX_Canada/welcome/overview_e.html.

[336] See Trans Union's website at https://www.transunion.ca/ . Other agencies may also use public records as a source of information on consumers.

What is my credit file?

A credit file is created when you first borrow money or apply for credit—for example, when you first apply for a credit card. Information about your history with credit grantors, including when you pay your bills, if you file for bankruptcy and how much you borrow are compiled in this file by credit reporting agencies. When you apply for a loan or a job, the bank or employer may access this information through a credit check to determine if you are eligible under the institution's policies for the loan or job.

Can I see what is in my file?

Not only do many credit reporting agencies have policies allowing consumers access to their credit file, it is also in consumers' best interests to check their files for accuracy because of the profound effects credit information can have on people's lives. As well, your credit file may contain information that is out of date—such as non-current employment history or an old address. You must contact the credit reporting agency to request a copy of the credit report that is sent out upon inquiry by a credit grantor, employer or landlord or other qualified person. This credit report will usually include:

- personal identification such as your name, address, birth date and Social Insurance Number;
- lists of individuals or organizations who have requested a copy of your credit file in the past three years;
- public record information such as bankruptcy judgments;
- any involvement with a third party such as a collection agency;
- details of your credit transactions such as if bill payments are made on time; and
- a consumer statement, if you choose to add one.

A credit report should not contain medical history information, items you purchased with cash, credit scores from credit grantors or any information relating to race, ethnicity or political affiliations.[337] This is personal information that is not relevant to your credit history and so your privacy in such areas should be preserved by the credit reporting agency.

What if I find an error or something I want to explain?

If you find an error in your file or disagree with some of the facts found in the file, you can notify the credit reporting agency and it may choose to investigate the matter. The credit reporting agency cannot simply alter information at your request as it receives the data from credit grantors and other members

[337] Both Equifax and Trans Union state on their websites that their credit reports only contain information that is relevant to business transactions and permissible to collect.

of the credit industry and must verify with them that the information is correct. You can also include a short statement protesting or explaining information in the credit file, which will be released with other information whenever a credit grantor or other qualified individual requests a credit report. If you are still dissatisfied with a decision or action of the credit reporting agency, depending on where you live in Canada, you may be able to complain to a provincial registrar of reporting agencies or other similar government agency.[338]

You should also be aware that credit reporting agencies do not rate the information in your file; this is done by credit grantors when they check to see if you are likely to pay the money back. As well, certain information is kept on file for a specified period of time. For example, if you filed for bankruptcy, this information could be contained in your file for six or seven years. A credit reporting agency does not deny you credit but merely provides information for other groups to make that decision based on their own policies.

Who else can see my credit file?

Only businesses that are part of the credit industry can access your file. This means that they must have a legitimate business reason and a permissible purpose to request a credit report. Common examples of a legitimate business reason to access your file include when you are applying for a loan from a bank or applying to rent an apartment or house. The business must also have your consent. Every time someone accesses your file, it is recorded in your credit file, so that you can see who has requested your credit file and when.

If I am a student, should I worry about my credit file?

Since it takes a long time to erase unfavorable information in your file, you should start early to build a good credit history. This involves paying your bills on time and checking your credit file. Changes to the way student loans are administered are also of interest to students. Because it is legal to collect credit information as soon as you are involved in a credit transaction, it is important to assert as much consumer control over this information as soon as possible.

What legislation exists to control the credit industry?

In previous years, the credit industry was largely self-regulated. Private companies could decide their own policies in relation to the collection and dissemination of personal information. Now, however,

[338] For information see: http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/h_ca02149.html .

most provinces have enacted consumer reporting legislation to regulate the credit industry. In addition, new federal privacy legislation may also apply to the credit industry.

In Alberta, the *Consumer Protection Act* ("CPA") regulates credit information.[339] In Part 5 of the Act, the legislation defines "credit information" and "personal information". Credit information includes things like your occupation, age, marital status, employer and income and any debts or assets you may have. Personal information includes details relating to your health, reputation, mode of living and other personal characteristics.

Section 44(1) states that a credit report may only be given when it is to be used in connection with:

- giving credit or collecting on a debt;
- renewing or beginning a tenancy agreement;
- in matters relating to employment or insurance; and
- in some cases where the government or a court seeks the information.

The section is specific in listing who can access a credit report, but it is important to note that credit reporting agency need only believe on reasonable grounds that the requestor intends to use the information for the acceptable purposes. The requestor does not need to conclusively demonstrate that the information will not be used improperly.

The CPCPA also specifies in detail what the reports may not contain. There is a duty on the credit reporting agency to make sure the information is reasonably accurate and stored in a way that an individual can have access to it, unless the individual does not pay the required fee or produce identification to prove that he or she is the person described in the credit file.[340] The CPCPA also allows an individual to provide an explanation of no more than 500 words about any information in the file and this must be included with any reports issued on that individual.[341] Under section 50 allows an individual who has suffered loss or inconvenience to sue a person who has breached a section of the CPCPA. Other provinces have similar legislation that regulates the credit industry.[342]

---

[339] *Consumer Protection Act*, Revised Statutes of Alberta 2000, chapter F-2.
[340] *Consumer Protection Act*, section 45.
[341] *Consumer Protection Act*, section 47.
[342] See, for example: *Credit Reporting Act*, Revised Statutes of British Columbia 1996, chapter 96; *Consumer Reporting Act*, Revised Statutes of Ontario 1990, chapter C-33; *Consumer Protection Act*, Revised Statutes of North West Territories 1988, chapter C-17; *Credit Reporting Agencies Act*, Revised Statutes of Saskatchewan, 1978, chapter 44; *Consumer Reporting Act*, Revised Statutes of Nova Scotia 1989, Chapter 93.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) (discussed earlier in this chapter) imposes requirements on the collection and management of personal information by credit reporting agencies.

Conclusion

As with many other aspects of the marketplace, the interests of credit reporting agencies and credit grantors must be balanced with the privacy interests of the public. Efficiency and profit do not have to be reduced in order to ensure privacy. In fact, the best way to ensure a long term healthy industry is to respect consumer rights such as privacy. The credit reporting agencies and credit grantors are increasingly protecting their consumer's privacy through their companies' policies. The federal and provincial governments are taking more active roles in regulating the collection of personal information in areas where there may not be enough protection in the credit industry. Consumers should also protect their privacy by contacting credit reporting agencies and ensuring that the information in their credit file is correct, up to date and allowed to be collected by the credit agency.

2.5.3 Financial Institutions

Introduction

Could this be you? In the morning, you scan the stock market report over breakfast to check how your investments are doing. Later that day, you run to the grocery store after work to pick up some items for dinner. You pay with your debit card at the till. Tomorrow, you and your spouse are going to apply for a mortgage for a new house. You figure that in a year you will have the car loan paid off and so now is a perfect time to plan for that new house.

Behind all these normal activities—checking stocks, paying with a debit card, obtaining a loan or mortgage—is your bank. To control your finances and plan for the future in today's world, you pretty much need to have some interaction with a financial institution. To perform the many functions that it does, your bank collects some personal information about you and even your family—including contact information, data on how much you earn and what assets you own. It is therefore very important to your privacy that the bank keeps your personal information secure and confidential. In fact, one court noted that an individual's financial records reveal many aspects of

that person's private life.[343] Despite this, in the past there was no privacy legislation to ensure banks were held to a high standard. Today, banks are becoming even more diversified in the services offered to customers: some banks offer auto and life insurance in addition to the usual savings account or loan transaction.[344] As well, recent bank mergers tend to solidify power within one large powerful company.[345] These new developments require strong privacy policies and practices.

How do banks protect my privacy?

Banks and other financial institutions will protect your privacy because they:

- have policies that deal with privacy;
- have obligations under the common law; or
- are required by privacy legislation to protect your privacy.

How do bank policies protect my privacy?

Financial institutions pride themselves on their tradition of respecting customer privacy as a key component of carrying on business. The Canadian Bankers Association (CBA) notes that Canada's banks have always been committed to ensuring that customers' personal information is accurate, confidential, secure and private.[346] Most banks have their own privacy policies. You can find out more about these policies by calling your bank or by finding the policy on the bank's website. In addition, the CBA created a voluntary policy code in 1986 and revised it in 1996.[347] This code contains ten principles that banks are to follow when they create and implement their own privacy codes. The ten principles are derived from the CSA Model Code for the Protection of Personal Information. As banks are federally regulated private businesses, they are subject to the PIPEDA (discussed earlier in this chapter) .

---

[343] *Del Zotto v Canada* (1997), 116 Canadian Criminal Cases (3d) 123 (FCA) in V. Rondinelli, "Are Financial Records Private and Confidential? Don't Bank on It" (December 1997) 18, 6 *Newsletter of Ontario Criminal Lawyers' Association* 17 (hereinafter Rondinelli).

[344] For example, Canadian Imperial Bank of Commerce offers auto insurance.

[345] Some of the stories in the news as the question of mergers has arisen are: P. Waal, "Size Over Substance: Does the Proposed Bank Merger Offer Canadians a Better Bank, or Just a Bigger Headache?"(February 13, 1998) 71, 2*Canadian Business* 18; S. Rubin, "Investors Banking on at Least One More Merger (Bank of Nova Scotia and Canada Trust)" *Financial Post* (18 April 1998) 4; H. Scoffield, "Bank Merger: Martin Fires Back at Banks. Finance Minister Wants Lower Consumer Costs, No Job Loss, Benefits for Small Business" (27 January 1998) 1.

[346] "Canadian Bankers Association—Privacy Model Code" Canadian Bankers Association Website https://www.cba.ca/Assets/CBA/Files (hereinafter CBA Privacy Code).

[347] CBA Privacy Code.

The reason that it is good business to protect consumer privacy stems from the common law. When you deposit money with a bank or take out a loan you sign a legal contract with the bank. For example, you promise to repay the money plus interest in exchange for a loan from the bank. There is an implied duty of confidentiality in your contract with the bank.[348] This means that personal information which you and the bank would describe as private should be treated as confidential information. Courts have recognized this implied term of confidentiality.[349] But this duty does not mean that as soon as you are no longer a customer, your personal information can suddenly be used by the bank in any way it desires, nor does it mean that information a banker obtains from a source other than you is not privileged.[350]

What legislation applies to banks?

The *Personal Information Protection and Electronic Documents Act*[351] (PIPEDA) applies to federally regulated organizations that collect, use or disclose personal information during commercial activity. This wide scope captures private sector industries such as banks that used to be exempt from such government laws. As mentioned above, the Act draws heavily on principles explained in the Canadian Standards Association (CSA) Model Code. There are ten principles listed in the privacy legislation that strive to protect personal information, including making organizations accountable, minimizing collection and obtaining consent for use. Banks must incorporate these principles into their privacy policies.[352]

Provincial privacy legislation, such as the Alberta *Personal Information Protection Act*, applies to business organizations under provincial jurisdiction including provincially regulated financial institutions such as credit unions.

Are there any circumstances when a financial institution under provincial jurisdiction may disclose some of my personal information without my consent?

Generally, there are three situations when provincially regulated financial institutions must disclose your personal information, despite their duty of confidentiality.[353] First, the bank may have to

---

[348] This principle is derived from the English case *Tournier v National Provincial Bank*, [1924] 1 KB 461 (CA) as discussed in S. Crawford, "Keeping It To Themselves: Bank Privacy Towards 2000" (1997-98) 29 *Ottawa Law Review* 425 (hereinafter Crawford).
[349] *R v Lillico* (1994), 92 Canadian Criminal Cases (3d) 90 (Ont (Gen Div)).
[350] Crawford.
[351] Statutes of Canada 2000, Chapter C-5.
[352] "Info: The Fair Information Practices" Industry Canada Web site:https://www.priv.gc.ca/en/privacy-topics.
[353] Crawford.

release customer records to the police or to assist taxation authorities when there is a law that requires disclosure. Banks must follow the laws of the country just as ordinary citizens must. In one case, the court held that a customer does not have a reasonable expectation that the following are private:

- the physical location of bank records about that person;
- or the fact that a customer has an account with a certain bank.[354]

However, this does not mean that the police can obtain more information than is needed without a search warrant to investigate suspicious activities in a bank account.[355] Revenue Canada may also require access to personal information to fulfill its mandate to ensure people are paying their taxes.[356]

Second, if there is a danger to the public, the bank may be required to disclose information because of the public interest. For example, in one case the court decided that disclosure of confidential information to prevent fraud was in the public interest.[357] This is different from the disclosure of information when an individual is already charged with fraud because the bank can decide when it will release information to the authorities.

The third situation where banks may disclose private information is when it is in the bank's interest to do so. The most common instance of this is when a bank must release the details surrounding an overdue debt in order to collect on the debt.[358] Courts prefer to limit this power so the bank does not have a stronger interest than its contractual partner, the customer. It is not clear whether a bank's interests can extend to disclosure of confidential information to affiliates in order to protect that third party's interests.[359] As banks become more diverse, the potential for sharing of confidential information increases.

If I have a complaint about my bank, what do I do?

If you feel that your bank is not following the Privacy Code created by the CBA, you should first voice your complaint within your bank branch. If you are dissatisfied with efforts made at this level,

[354] *Canada (Department of National Revenue) (Re,)* [1998] Ont. J. No. 3517 (Ont Ct Prov Div).
[355] *Lillico* in Rondinelli.
[356] Crawford.
[357] *Canadian Imperial Bank of Commerce v Sayani* (1993), 11 British Columbia Law Reports (2d) 23 (BCCA) in Crawford.
[358] Crawford.
[359] Crawford.

contact your bank's ombudsman. If the issue is still unresolved, take your complaint to the Canadian Banking Ombudsman—an individual appointed by a collection of participating banks to handle complaints that reach this level. Although this person cannot make participating banks follow recommendations, banks do because they are interested in resolving the issue just as you are. Finally, you may be able to bring a complaint to the attention of the Privacy Commissioner of Canada, if the bank falls under PIPEDA—and most banks do. The Privacy Commissioner can investigate and take the matter to the Federal Court of Canada if needed.[360]

Conclusion

Banks have been quick to protect the privacy of customers by developing and following voluntary privacy codes and policies. As well, there is a common law duty of trust and confidentiality between customer and banker that courts have recognized and upheld. Despite these traditional safeguards, some remain concerned about privacy because of improvements in data transfer technologies and the very nature of banking itself. As banks diversify into other services, the temptation to exchange or sell valuable, detailed and personal information about clients between affiliates and departments may be stronger than the commitment to privacy.[361] It is this concern especially that customers should be aware of and that privacy legislation should address.

2.5.4 Direct Marketing

What is direct marketing?

Direct marketing is bulk mail sent out automatically to individual people's homes. Instead of waiting for a customer to contact a business, a company seeks to reach out directly to the customer. Usually, we learn about products and services on television, through the phone book, in advertisements on billboards and in magazines, and through word of mouth. Direct marketing attempts to be more specific in its target audience in the hopes of reaching more people who are interested in the product or service.

How did a company I have never heard of get my name?

The collection and selling of lists of consumers' names is a lucrative industry. Some companies only collect personal information so that other companies can purchase this information to improve their own sales. Lists are compiled by grouping together individuals with similar tastes and habits. This is

[360] "The Banking Privacy Protection Guide" Industry Canada Web site: http://strategis.ic.gc.ca/ .
[361] R. Wright, "In Strictest Confidence?" (Nov./Dec. 1996) 103, 6 *Canadian Banker*, at 24.

all done by computer which allows even longer lists and a much wider target audience than if a human had to actually group people into categories. The information is initially obtained when you provide information for another reason, such as by filling out a warranty card or by taking out a magazine subscription. Also, private registry companies make money by selling personal information provided by motorists to private investigators, lawyers and commercial parking-lot companies.[362] You also give out a great deal of information on the internet.

Will the PIPEDA or PIPA stop junk mail or spam?

Clearly, you can complain about the use of your name and address or e-mail address by an organization sending junk mail. However, it may be difficult to track down where the organization got the information.[363] Some of the pointers below may help in minimizing the amount of junk mail or spam you receive.

How can I minimize the amount of direct mail I receive?

First, you can take steps to minimize the amount of information collected about you.

- Whenever you order a product or service, fill out a warranty card or donate money, mark on the form in large letters "Please do not sell my name or address".
- Avoid filling out warranty cards as they are often not required anyway.
- On the telephone, ask that your name be marked as not one to be traded or sold.
- Ask your credit card company not to sell your name.
- Avoid contests that promise a vacation or free product because it is usually just a way of getting consumers to volunteer personal information.[364]

Second, you can write to the Canadian Marketing Association[365] or, to get off lists from companies in the United States, write to Mail Preference Service, c/o Direct Marketing Association.[366] You may not be able to stop all mail, but you should be able to limit the amount you receive. If you are bothered by local flyers delivered to your mailbox, contact the company directly and ask to be

---

[362] L. Johnsrude, "Registry Information Becomes An Issue" (23 April 1998) Edmonton Journal online Web site: www.edmontonjournal.com/nfews/alberta/042398ab5.html .
[363] Perrin, at 161.
[364] See "Do It-Yourself: Stop Junk Mail, Email and Phone Calls" Web site: http://legacy.obviously.com/junkmail/ Although this site is American, it has some general handy tips.
[365] Canadian Marketing Association, MPS/TPS Deletion (416) 391-2362, 55 University Avenue Suite 603, Toronto, ON, M5J 2H7. E-mail: info@theCMA.ca
[366] Direct Marketing Association (U.S.) (212) 768-7277; 225 Reinekers Lane Suite 325, Alexandria VA, 22314.

removed from the mailing list. This allows you some control as junk mail is only junk when you do not want to receive it.

2.5.5 The Media and Privacy

Introduction

A disabled woman witnesses a murder in a parking lot outside her doctor's office in British Columbia. She is interviewed by the press afterward, and reports of the interview are published in two daily Vancouver newspapers and broadcast by the Canadian Broadcasting Corporation. She is shown to be a patient at the centre where her doctor works and is identified as a witness to the murder by name and picture. She sues for psychological illness suffered as a result of the reports being published when the murderer is still at large.

A teenager is sitting on the steps of a building in downtown Montreal when a magazine photographer takes her picture without her consent and publishes it in an arts magazine. Seven hundred and twenty-two issues containing the photo are sold, and the young girl learns of its existence when a friend draws her attention to the photo.[367]

The media plays an important role in society in keeping people informed of current events and ensuring that government activities are carried out under the public eye. One of the checks on power in a democratic system is the freedom given to the press to report on events as they occur. However, the above examples illustrate that, in some circumstances, tension arises between an individual's privacy and the desire by the media to publish a newsworthy story. These concerns may arise when a newspaper, magazine, or television program publishes personal details about a person, or when the details of a crime are particularly horrific or embarrassing to a victim.

There is no legislation making it a crime for the media to publish something that is correct but personal about an individual. On the other hand, if the media publishes something that is personal, but incorrect, there may be criminal charges laid against them and/or they may be sued.

There are two other limits on the media. First, as discussed earlier, some provinces have passed privacy laws that recognize invasion of privacy as a tort. In these provinces, a person who feels that

[367] See *Pierre v Pacific Press* (1994), 92 BCLR (2d) 223 (BCCA); and *Aubry v Editions Vice-Versa*.

his or her privacy has been invaded by the media can seek compensation by suing the publisher. Second, if a judge feels that publication of some details about a trial will not be in the interests of justice, he or she may order a publication ban that prohibits the media from publishing some details.

These situations will be discussed in more detail below.

What rights do the media have in Canada?

The media's right to publish information is protected by the Canadian *Charter of Rights and Freedoms*:[368]

> 2. Everyone has the following fundamental freedoms…
> (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.

Before the *Charter* was enacted, it was generally understood as a principle of a democracy that the press should be able to report on events and government activities without fear of censure. Scholars have written about the principle of free speech for many years.[369] Free speech is essential to good democracy.

However, the ideals of a principle and what occurs in reality sometimes do not coincide. The information age has led to new ways to collect and distribute personal information about people on a large scale.[370] Celebrities are popular targets of relentless members of the press known as *paparazzi*. An extreme example of the effect paparazzi can have is the death of Diana, Princess of Wales in 1997. The media did not cause the accident that killed Diana, but many believe the pursuit of the media may have been a contributing factor.[371] However, celebrities may have a reduced expectation of privacy because their work necessarily puts them in the public eye.[372]

Second, because most media are large corporations, some people question whether the media really

---

[368] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act*, 1982, being Schedule B of the *Canada Act 1982* (UK), 1982, c 11, (hereinafter "Charter" or "Charter of Rights and Freedoms").
[369] See G. S. Adam, "The Charter and the Role of the Media: A Journalist's Perspective" in P. Aniseman and A.M. Linden, eds., *The Media, The Courts, and The Charter* (Canada: Carswell, 1986) at 39-56.
[370] Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (New York: Alfred Knopf, 1995) at 151.
[371] See, for example, Time at:http://time.com/4914324/princess-diana-anniversary-paparazzi-tabloid-media/
[372] A. W. Branscomb, *Who Owns Information*? (New York: Basic Books, 1994) at 74-5.

is neutral in its selection of stories or an effective watchdog on the powerful.[373]

Can the media rely on the Charter *to say that it has the right to invade my privacy?*

Some people are concerned that the *Charter* has given the media more protection when it invades the privacy of individuals in pursuit of a story. If the media can argue that "the spirit of the *Charter*" can be read into provincial privacy laws, then individuals arguing that the media has invaded their privacy may have a harder time being successful.[374] This is because the person who wants to limit the media's *Charter* right to freedom of expression must prove in court that this right should be limited. As the media is owned more and more by large corporations, this person is faced with a legal battle with a powerful corporation as well as with having to prove that the media's right to freedom of expression should be limited.[375]

What are some examples where the media has published personal information about someone? What did the courts do about it?

There are examples of cases where people have sued the media for invasion of privacy in those provinces with privacy laws. In one case,[376] the employees of a furniture store were on strike and two reporters were sent from a TV station to get an interview. The owner of the store would not give an interview and told the reporters not to trespass on his property and, when he later found the reporters in his parking lot filming, a struggle ensued for the microphone. The scuffle was filmed and broadcast, and the owner sued for trespass and invasion of privacy. The court said that although there was a trespass in the case, there was no invasion of privacy because the parking lot was a public place and the owner had voluntarily gone there and voluntarily participated in the scuffle. Also, the court decided that the broadcast was fair comment on a matter of public interest.

Whether or not the media knows or should know that publication of personal information would be an invasion of privacy seems to be one factor the courts consider when dealing with these issues. A man who was balding underwent surgery for hair grafts. He signed a consent form allowing his doctor

---

[373] H. J. Glasbeek, "Comment: Entrenchment of Freedom of Speech for the Press-Fettering of Freedom of Speech for the People" in P. Anisemen and A. M. Linden, eds. *The Media, the Courts and the Charter* (Canada: Carswell, 1986) at 100-118.

[374] S. Lawson, "Privacy v. Freedom of the Press" (1995) 1 *Appeal* 46-49.

[375] Lawson, at 48.

[376] *Silber (c.o.b. Stacey's Furniture World) v British Columbia Television Broadcasting System Ltd.,* [1985] British Columbia Judgments Number 3009. See also *Belzberg v British Columbia Television Broadcasting System Ltd*. [1981] British Columbia Judgments Number 1568; *John Doe v Canadian Broadcasting Corp. (C.B.C.,)* [1993] British Columbia Judgments Number 1869.

and the company providing the technology to record the procedure for instruction purposes. The man who made the tape worked for a media company but was not acting in this capacity at the time. Years after the tape was made, the man who recorded the video was doing a story with a journalist on hair replacement. The doctor and the company were contacted and had no objections to the use of the tape. No one knew the whereabouts of the man who had undergone the treatment, and the journalist was told consent had been obtained. The story was aired and the man's face was fully identifiable for three seconds. He sued for invasion of privacy, but was unsuccessful. The court held that the media believed he had consented and had no way of determining otherwise as he could not be located. Also, the doctor and company had assured the media that consent had been obtained. It was also a true account and not defamatory or false in any way.

On the other hand, another case[377] provides an example of courts limiting what the media can do with personal information. The defendant CBC had a television show that carried sensationalistic stories. A 79 year old doctor wrote to the producer commenting on the general poor quality of the show. He ended his letter by wondering if the producers would publish his letter on the show as they did with other letters. In a subsequent broadcast, the show commented on the letter, televised his name and address and requested the viewing audience to write to him to "cheer him up". The doctor was snowed under by letters and phone calls. He had to take time off work and change his phone number. He eventually sued for invasion of privacy and the court agreed that the show had, under Quebec law, given out too much personal information. The company should have known of the large number of people who would view the show and follow up on the request.

In the example given at the start of this section, where the picture of a teenager in a public place was taken and published in an arts magazine without her consent, the courts held that this was a violation of her privacy.[378] In that case, the privacy interests of the teenager came into conflict with s 3 of the Quebec Charter,[379] which protected freedom of expression. Although in some instances the public's right to information will limit respect for an individual's private life, in this context, the artist's right to expression was not absolute nor was the public interest in seeing the photo stronger than the privacy rights of the young girl.

[377] *Robbins v Canadian Broadcasting Corp. (Que.)*, [1958] Quebec Superior Court Reports 1073 (Que Superior Ct).
[378] *Aubry v Editions Vice-Versa*.
[379] *Charter of Human Rights and Freedoms*, Revised Statutes of Quebec, c C112.

In summary, in those provinces where there are privacy statutes (laws), the media may rely on the defence(s) that:

- the report was in the public interest;
- it was a matter of fair comment, that is, a true account and not defamatory;
- there was consent to publish the details; and
- the publication was authorized by law.

(These same defences could be used by anyone who has been sued for an invasion of privacy. **See the discussion above under 2.2 Provincial Privacy Legislation.**)

How else can the media be limited in publishing personal information?

In addition to being allowed to sue the media for invasion of privacy using legislation in some provinces, you may also be able to sue the media for defamation if what is said about you is untrue and harms your reputation. Defamation is not strictly a privacy issue, but privacy concerns may arise when the media seeks to uncover and then publish personal information. The media is more vulnerable to a suit of defamation because it is a clearly recognized crime under common law and the *Criminal Code* (section 298). Journalists may not publish information about a person that the person claims injures his or her reputation by holding him/her up to ridicule, scorn or contempt, even if the journalist did not intend for the report to be defamatory.[380] The media can argue in its defence that the statement was true, was an honestly expressed opinion based on true facts, or was "privileged" (protected from liability by law).[381]

Members of the media are also subject to their own code of ethics.[382] Journalists strive to be professional and rules of conduct help ensure the integrity of their work. Ideally, a journalist should weigh the public interest served against the privacy of the individual when deciding to pursue or publish certain facts. If the details do not add anything to a story, and may even be harmful, then the journalist should not publish those details.[383]

What information can the media obtain from the police for a story?

Crime forms a large part of the daily news, as it is a topic of continuing interest to the public. In many

[380] *Criminal Code*, section 301.
[381] *Criminal Code,* sections 305 to 315.
[382] See, for example: Canadian Daily Newspaper Association *Statement of Principles*, adopted in 1977, revised in 1995; Radio television News directors Association of Canada *Code of Ethics*, 1986.
[383] *JMJ v Chappell,* 1998] British Columbia Judgments Number 276.

provinces, the police services are governed by freedom of information law. In addition, police forces set their own policies regarding the release of information to the media. For example, in Edmonton, Alberta, the police disclose personal information (that which tends to identify an individual and her relation to a crime) when:

- it is in the public interest to do so because of a grave environmental, health or safety hazard to the public;
- the individual consents to the release of her personal information;
- an individual's health or safety is in danger;
- next of kin need to be contacted;
- the records are available to the public; or
- the facts or circumstances of the particular case warrant disclosure.[384]

At the same time, police forces have policies regarding the types of information they will not release to the media. Edmonton's police force, for example, will not release the following types of information about accused persons:

- the existence of an alibi, admission, confession or statement;
- the reputation, character, or criminal record of an accused;
- any tests taken by, refused by, or offered to the accused; and
- any evidence on information that may prejudice a trial.[385]

These guidelines attempt to strike a balance between the public's right to know and the privacy of an accused or a witness.

What about when a person is accused of a crime? Are there any limits on the media?

Section 11(d) of the *Charter* guarantees every individual the right to a *public* trial in front of an impartial tribunal. This section is often cited as authority for the media to report on matters of importance before the courts. It is in the interest of the public that justice is rendered in an open and public manner to ensure that the law is being applied fairly and is not arbitrary or biased. However, there are some things journalists are not to do. Journalists are not to portray a person as guilty as they report on a trial.[386] This is a reflection of the right to be presumed innocent until proven guilty in

[384] Staff Sergeant I. Shoaf, "Disclosing Personal Information to the Media From the Edmonton Police Service Perspective" Presentation to FOIPP '99 (June 8, 1999) Edmonton, Alberta (Workshop E2) at 4 to 8 (hereinafter Shoaf).
[385] Shoaf, at 8.
[386] Shaw, Westwood and Wodell, at 173.

Canadian law. Journalists are not to report on the names of witnesses or victims of sexual assault if the court orders them not to. This type of order is called a publication ban.

What is a publication ban?

The media can report on most court happenings. However, it is up to the court to determine if it would be in the best interests of the accused to ensure a fair trial or for a witness to protect privacy to restrict some details that the media would otherwise publish. This is done in the form of a publication ban. In the *Criminal Code*, section 486(4.1) allows judges to order that the identity of a victim or witness, or any information that could reveal that person's identity, not be published. Under section 486.31(3) a judge will consider several factors when making this order, including:

- the right to a fair and public hearing,
- the risk publication would bring to a victim or witness,
- society's interests in encouraging the reporting of offences,
- alternatives, and
- the effect on freedom of expression.

In addition, *Criminal Code* s. 517 provides for a mandatory publication ban of evidence heard in bail hearings, if an accused person requests a ban. This section has recently been found constitutional by the Supreme Court of Canada.[387]

Sometimes the media will disagree with a publication ban order and challenge the order in court. For example, a court ordered a publication ban on the name of a victim of sexual assault but a newspaper published this information anyway.[388] The report was accurate and published in a public newspaper. The issue in the case was whether the defendants were immune from liability because the victim's name was a matter of public interest or because the publication was privileged. The court held that, generally, the public had no interest in the name of a victim of sexual assault and that here, although the victim's name had been publicly heard in open court, the publication ban still prevented the press from invading the victim's privacy.

The media may also seek access to court records. Under Nova Scotia's freedom of information laws,

[387] *Toronto Star Newspapers Ltd. v Canada,* 2010 SCC 21.
[388] *JMJ v Chappell,* [1998] British Columbia Judgments Number 276. See also *R v Canadian Newspapers Co. Ltd.* 43 Canadian Criminal Cases (3d) 24.

a newspaper sought access to evidence used in some trials that were over. The court held that allowing the newspaper access to the evidence would violate the principles in the legislation because it would be a disclosure of personal information that would be an invasion of privacy.[389]

What happens when the media disobey a publication ban?

If media disobey a court order, they may be found in contempt of court.

What is contempt of court?

The crime of contempt of court is not codified in the *Criminal Code* but derives from the common law. This means that there is no clear definition, as courts have shaped the meaning through the years. The *Dictionary of Canadian Law* states that it is contempt when:

- an order is made against a person and the person fails to comply with it or
- when the person does an act that shows disrespect for court authority or that tends to hinder justice.[390]

There are several ways that members of the media might be found in contempt. For example, the media may be found in contempt of court for statements made outside of court that present a judge or the process of a trial in a very biased, negative or derogatory way. The media must also be wary of interfering with an accused's right to a fair trial by suggesting the accused is guilty, publishing detailed information about the person's 'bad character' or criminal record or suggesting in any way a particular result.[391] The power of the court to find members of the media in contempt has been criticized by many as a restriction on freedom of expression. On the other hand courts are worried that the public stories will influence the jury's decision or opinion. In one case, wide media coverage of a trial was considered by a trial judge as a factor that may lessen the sentence given to a convicted accused.[392]

2.5.6 Information gathering by an employer

What information can an employer collect about me when I apply for a job?

In addition to the usual information collected by a potential employer, such as name, address and work experience, some employers may inquire further into your background. They may ask if you will consent to a criminal record check or will undergo psychological testing. As well, you may be

[389] *Halifax Herald Ltd. v Nova Scotia (Attorney General) [re R v Barrow],* [1992] NSJ 301; See also *London Free Press Printing Co. v Ontario (Attorney General)* (1988), 66 OR (2d) 693. .
[390] *The Dictionary of Canadian Law* (Ontario: Carswell, 1991).
[391] M. Crawford, *The Journalist's Legal Guide* 3rd (Ontario: Carswell, 1996) at 124-128.
[392] *R v Storring* in *The Lawyers Weekly* 11 January 1991 .

required to take a lie detector test (polygraph) either before or, if circumstances warrant, during your employment. These procedures are often implemented in sensitive jobs requiring a high degree of trust in the employee, such as in some government positions or in jobs involving handling of large amounts of money. Sometimes, laws require that prospective employees have a criminal record check. For example, the Alberta *Protection of Persons in Care Act*[393] requires persons working or volunteering in designated agencies (hospitals, nursing homes, lodges, group homes, etc.) to provide results of a criminal record check. Therefore, whether you are required to undergo these tests depends on the facts of your situation.

What information can my employer get from a criminal record check?

A criminal record check may tell an employer if you were ever charged with an offence, if you were ever convicted of an offence, or if you currently have a matter before the criminal courts. What will be released by the police varies with agencies: some agencies release only convictions under the *Criminal Code* and similar federal legislation while other agencies include convictions under provincial laws and even pending charges.[394]

Can I do a criminal record check on myself?

Yes. Contact your local police department (security clearance department) to find out how this is done.

When can my employer ask for a criminal record check?

The most common form of pre-employment screening, criminal record checks, are used by a variety of employers and volunteer organizations. A check can only be conducted if the employer has the consent of the job applicant or employee. However, sometimes an applicant or employee may have no choice but to give consent or feel that he has no choice but to give consent, if he wants the job. If consent is given, the police agency to whom the written consent is submitted will search police databases like CPIC, PROS or other local storage systems to determine if any information is in the system on the job applicant. If no criminal record is found, the employer will be informed. If a record is found, the police will usually request fingerprints to verify that the identity of the job applicant matches the profile in the record before information is released to the employer.
For more information about CPIC and PROS, see Chapter 1: Privacy Protection and the Government – Police Information Sharing.

---

[393] *Protection of Persons in Care Act*, Statutes of Alberta 2009, c P-29.1.
[394] Shaw, Westwood and Wodell, at 141.

What if the employer is discriminating against me on the basis of criminal history?

There are no specific laws relating to criminal record checks. In some provinces and in federally regulated industries, there are laws in place to prohibit discrimination against employees for their criminal records. For example, the *Canadian Human Rights Act*[395] applies to those who work in federally regulated industries, such as in banking. The Act prohibits discrimination against an applicant on the basis of a criminal record, but only if that person has been pardoned of the conviction.

Generally, as long as an employer is not violating human rights legislation, there is little you can do to challenge the required criminal record check. If an employer refuses to employ you or fires you because of information contained in a criminal record check, you *may* be able to complain in some provinces to their human rights commissions. However, this does not mean that a commission can dictate to employers what their security policies should be. If you apply for a federally regulated job, there is little you can do except to withdraw your application, because government jobs often require a high degree of trust of employees who handle information about the public. If you are a union employee, you may be able to have the union argue that the employer is acting outside of the collective agreement.

Are there other types of background checks that my employer can do?

Employers can hire a private investigator to check out your personal history. There are also a number of public records and commercial databases, which contain personal information about people. However, under the PIPA (or its equivalent in other provinces) private investigators and commercial databases may have to obtain your consent, if they charge to obtain information about you.

What types of things do employers use psychological tests for?

Various questions on psychological tests may be asked to measure such things as the employee's:

- skill and knowledge;
- aptitude;
- intelligence;
- personality, and;

[395] Revised Statutes of Canada 1985, c 24 (4th Supp.).

- vocational preferences.[396]

Employers may use these tests to screen out prospective employees.

How reliable are psychological tests?

Psychological tests can vary greatly in form and result, so it is difficult to determine their legitimacy. Whether these tests reliably convey information to an employer is questionable. For example, the racial or cultural identity of the employer who scores the test may be influenced by prejudice or bias against an employee taking the test if she has a different ethnic background, even if this is unconsciously done.[397] Further, people who administer the tests may not have the proper training to interpret the results.[398]

What if I disagree with the results of a psychological test?

There is usually little you can do except discuss your concerns about the validity of the psychological test with the potential employer and attempt to convince her to alter or cancel the test.

What laws that apply to psychological tests and how the results are used and stored?

If you apply for a federal government job, your employer must comply with federal privacy laws and you can complain to the Privacy Commissioner if you believe the federal law has been broken. If the employer is the provincial government, you will be protected by provincial privacy laws.

If your prospective or current employer is not the government, other federal or provincial privacy laws may apply. These privacy laws were discussed earlier in this chapter.

Finally, provincial human rights legislation may apply to psychological testing by both private sector and public sector employers. For example, if you could show that the employer did not hire you because the psychological testing revealed a mental disability, which would not affect your ability to perform the job, you may have a valid complaint to the human rights commission.

---

[396] Shaw, Westwood and Wodell, at 151.
[397] W. MacKay and P. Rubin, *Study Paper on Psychological Testing and Human Rights in Education and Employment* (Ontario Law Reform Commission, 1996) (Hereinafter MacKay and Rubin).
[398] MacKay and Rubin, at 121.

What is graphology? Why would an employer want to use graphology?

Graphology is the use of a person's handwriting to estimate her character. Employers may claim that it gives information about applicants or employees on their personality. However, there is dispute over whether analyzing someone's handwriting actually reveals any conclusive information about that person. There are no standardized qualifications for graphological analysts and graphology is a completely subjective process, which is subject to inaccuracy.[399] Similar to psychological testing and criminal record checks, an applicant may have few options if he objects to his handwriting being analyzed as part of the pre-employment process. However, he may have the same legal protections as those subject to psychological testing (discussed immediately above).

Why would an employer want me to take a polygraph test?

Polygraphs, or lie detector tests, are often justified on the basis that they provide insight into the truthfulness of answers given by the test taker. Employers may use polygraph tests to weed out prospective employees or as a tool for solving work-related crimes.

A polygraph is based on the idea that when a person tells a lie, there is an identifiable and measurable bodily response, which a skilled test giver will be able to detect and separate from bodily responses to other stimuli, such as stress.

However, the accuracy of these tests may depend on several factors, such as the mental or emotional state of the test taker and the skill of the test giver. Test results may be influenced by the ethnicity of both test taker and giver. Also, the test taker may have training in being able to defeat a polygraph.

Can my employer require me to take a polygraph test while I am employed?

There is no restriction on the use of polygraph tests by employers under Alberta employment legislation, although there is a restriction in Ontario legislation.[400] This means that in provinces like Alberta, where polygraph tests are not prohibited, employers may decide to use such tests.

However, arbitrators have not agreed on the questions of whether and when employers can use polygraph tests. A federal case[401] held that an employer can give polygraph tests, in some

---

[399] Barbara Hill, *Graphology* (Great Britain: Robert Hale Limited, 1981) at 7-8.
[400] *Employment Standards Act*, 2000 Statutes of Ontario, section 69.
[401] *Loomis Armored Car Service Ltd. and National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada) local 4266A* (1996) 57 Labour Arbitration Cases (4th) 305.

circumstances, in the absence of a federal law prohibiting them. In this case, it was significant that the employee had signed a form saying he was willing to take a polygraph test if needed, and the arbitrator ruled that this amounted to an implied term of the collective agreement (to undergo the test if asked). However, a similar case that arose a couple of years later in British Columbia was decided differently.[402] The arbitrator felt that a polygraph test was a significant intrusion on a person's privacy rights, like being physically searched by a medical examiner. In order to justify infringing the right to privacy, clear and unmistakable words from the employee are needed. Thus, the arbitrator would not imply into the collective agreement a term that employees must submit to a polygraph in appropriate circumstances.

If the jurisdiction where you work does not prohibit the use of polygraph tests, it is not clear whether you can be required to submit to a polygraph test—either before being employed or for a work-related issue. The answer seems to depend on the circumstances and on balancing the rights of the employer and employee in the situation.

2.6 CONCLUSION

The laws around protection of personal information in the private sector are changing. In addition to the common law protections for privacy, PIPEDA now covers any organization that collects personal information in the course of commercial activity, except in provinces that have "substantially similar" privacy laws. As more Canadians are becoming aware of the importance of protecting their personal information, Organizations are now exerting more effort to adapting their business practices to comply with PIPEDA and the similar provincial Acts. The Office of the Privacy Commissioner of Canada ("Office") has investigated over 3,000 individual complaints since the inception of the PIPEDA, and has issued findings on many precedent-setting issues arising from the Act. As a way of sharing the insight it has gained in the first seven years of PIPEDA the Office launched: *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA),* on May 23, 2008.This document highlights some of the of leading cases and findings of the office in several important issues. A printable copy of the publication can be found at: https://www.priv.gc.ca/en/privacy-topics/.

[402] *Re Loomis Armored Car Service Ltd. and Independent Canadian Transit Union, Local 1* (1998), 70 Labour Arbitration Cases (4th) 400.

Additionally, every year since its inception the Office has released an Annual Report detailing the yearly statistics and success of the PIPEDA.

2.7 CASE STUDIES

Aubry v Editions Vice-Versa, 1998 (Supreme Court of Canada)[403]

A photograph taken of a teenager in a public place is then published in an arts magazine without the teenager's consent.

In Quebec, a publisher of an arts magazine took a picture of a sole 17-year-old teenager sitting on some steps in a public place. The teenager was unaware the picture was taken and to be published in an arts magazine. 722 issues of the magazine were sold. The teenager became aware of his picture being published when a friend of his drew it to his attention and other people at his school laughed at him.

In reviewing this case, the court pointed out that in Quebec's Charter of Human Rights and Freedoms[404]*, it explicitly states that every person has a right to respect for his private life, and that this included one's right to his or her image. Here this right came into conflict with the right to freedom of expression, another right also protected by the Quebec Charter. In deciding this case, the court commented that when an individual's own action places him in a photograph in an incidental manner, like in a crowd at a sporting event, he is regarded as an anonymous element of the scenery and the photographer and publisher are able to legally use this type of photograph. But the court also stated that a photographer's right is not unlimited when publishing pictures taken in a public place if it infringes on a person's right to privacy. Here the photograph was published when the teenager was identifiable and the principal subject of the photo. The error here was not the taking of the photograph, but its publication without the sole, identifiable subject's consent. The teenager was able to prove he suffered injuries in the form of some discomfort and upset, and the court awarded him $2,000 in damages.*

[403] *Aubry v Editions Vice-Versa,* [1998] 1 Supreme Court Reports 591.
[404] *Charter of Human Rights and Freedoms,* Revised Statutes of Quebec, c C-12, sections 5, 9.1.

LAM v JELI, [2008] B.C.J. No. 1612

Videotaping through a peephole.

This was an action by the plaintiff for damages for breach of her privacy. The plaintiff brought the claim on the basis of section 1 of the Privacy Act, R.S.B.C. 1996C. 373, which made it an actionable tort without proof of damage to willfully violate the privacy of another. The plaintiff sought general damages in the range of $20,000, punitive damages in the range of $40,000 and loss of capacity to earn income damages for approximately one year in the range of $10,000-$20,000.

The plaintiff was a 35 years old mother of two children - a boy born in 1990 and a girl born in 1997. She began an intimate relationship with the defendant in the middle of the 1998, and moved into his house with her children around August 1998. They broke up in August 1999 for a short period and continued cohabiting until September 1999. Thereafter the plaintiff and defendant continued in an on-and-off relationship and finally parted ways for good in January 2002. According to the plaintiff, the defendant had renovated his bathroom within months of her first moving in with him in 1998.

During the on-and-off relationship in January 2002, the plaintiff went over to the defendant's house and saw a stalk of videotapes on his coffee table. A verbal dispute resulted over a previous sex tape they had made and the plaintiff ended up taking a number of the videotapes to her place to view. One tape which appeared to be a number of different tapes spliced together showed the plaintiff in different stages of undress going to the bathroom and doing a number of bathroom functions. It also showed the plaintiff and her young daughter when her daughter was still in diapers and a nude scene of her daughter alone in bathroom, a year later. The plaintiff called the police who took possession of the videotapes and arrested the defendant. The defendant was subsequently charged and convicted of possessing child pornography because of the videotaping of the children. All of the tapes except the spliced one were destroyed. The defendant could not be charged criminally with videotaping the plaintiff or having tapes showing her in the nude, as section 162 of the Criminal Code, which makes it an offence to make a visual recording of a nude person in circumstances giving rise to a reasonable expectation of privacy, was not included in the Criminal Code until 2005. That left the plaintiff with only a civil recourse.

The plaintiff was awarded punitive damages against the defendant in the sum of $35,000 and general damages of $20,000 and loss of income earning opportunity of $5,000. Although the defendant never conceded that he made the videotapes, the court was satisfied from the facts that the videotapes were made in his house, of the interior of his bathroom, through a hole that he knew

existed below a built-in cabinet that he put in his bathroom with the use of mirrors enabling a full view of the bathroom. The defendant was found liable for willfully and without claim of right violating the privacy of the plaintiff. The court directed that the names of the plaintiff and defendant be identified only by initials in the reasons for judgment to protect the privacy of the plaintiff.

***Warman v Grosvenor**,* [2008] OJ No. 4462

A case on internet postings and personal emails.

The plaintiff, Richard Warman, was a lawyer, who resided in Ottawa, Ontario and worked extensively for the Government of Canada in the area of human rights relating to hate propaganda in the internet. The defendant, William Grosvenor, resided in Edmonton Alberta. The plaintiff commenced an action against the defendant, seeking general, aggravated and punitive damages of $50,000 for defamation, assault and invasion of privacy.

The defendant started a two-year campaign of terror against the plaintiff achieved through threatening and intimidating internet postings and e-mails. The defendant's postings on several internet websites, referred to the plaintiff amongst other things, as a dishonest man, lair, scumbag, pimp and disgusting maggot. The emails repeated the same themes of the internet postings. The plaintiff sought for damages for invasion of privacy on the fact that he had removed his address from telephone listing and had maintained an unlisted telephone number due to his extensive human rights work relating to hate propaganda, a purpose defeated by the defendant's internet posting—which published the plaintiff's personal information including an aerial photograph and map to locate the plaintiff's residence.

The action was allowed, and the plaintiff was awarded total damages of $50,000.00. The award comprised of $20,000 as general damages for defamation, $10,000 as aggravated damages for defamation, $15,000 as general damages for assault and $5,000 as aggravated damages for assault. The court found that the internet was a means of publication like no other, given its ability to instantaneously send words throughout the world and that the postings were threatening and intimidating. By virtue of their repetitiveness, their details regarding the plaintiff's address, and the level of malevolence led the court to conclude that they were more than empty threats and insults, as the publications made the plaintiff apprehensive of imminent physical harm. The court could not find that the damages claimed by the plaintiff for the tort of invasion of privacy were distinct from those flowing from the torts of defamation and assault. It observed that there was no tortuous conduct amounting to an invasion of privacy that is separate from the conduct making the defendant liable for defamation and assault, hence there was no separate harm that is recoverable by the plaintiff for a tort of invasion of privacy.

Watts v Klaemt, [2007] BCJ No. 980

Intercepting and recording telephone conversations.

The plaintiff, Arlene Watts, sued the defendant, Joerg Klaemt, her daughter's neighbour, for breaching section 1 of the (British Columbia) Privacy Act, interfering with her economic relations, and for invasion of privacy and negligence. The Plaintiff worked with the Ministry of Social Services.

Following several disputes between the plaintiff's son-in-law and the defendant, the defendant began to use a scanner and a tape recorder to monitor the conversations going on within the plaintiff's house on a cordless phone. When he intercepted a conversation where the plaintiff counseled her daughter and son-in-law on ways to avoid detection and prosecution for welfare fraud, the defendant reported the contents of the conversation to the plaintiff employer, and this resulted to her termination for breach of trust. At issue was whether the defendant's action constituted a breach of privacy.

The defendant argued that a conversation on a cordless telephone of the second generation was not a private communication because such telephones are not secure telephone lines and anyone with a scanner could listen to a person speaking to another on a cordless telephone. The defendant also argued that a cordless telephone conversation does not meet the definition of a private communication in section 183 of the Criminal Code, as had been held in some decided cases. He argued that his actions were excused under section 2(2) (b) of the Privacy Act as incidental to the exercise of a lawful right - his defence of his property from any further harm from the plaintiff's son-in-law. He argued that the plaintiff's son-in-law's past behaviour, which included physical and emotional threats, indecent exposure, damages to property and harassment, required him to use all possible means to protect himself including intercepting the plaintiff conversations which would give him advance notice of any plans to cause him further harm.

The plaintiff, on the other hand, posited that the defendant's conduct in deliberately listening to her telephone conversations, recording those conversations, and publishing them to her employer constituted an invasion of privacy at common law and a breach of section 1 of the Privacy Act. She argued that even if the cordless telephone conversation may not technically meet the definition of a

private communication in the Criminal Code, the standards of privacy in a civil context are based upon the reasonable expectations of the parties to the communication.

The court accepted the defendant's argument that the reception by a scanner was likely excluded from the definition of private communication found in section 183 of the Criminal Code, but pointed out that the criminal definition of private communication was not dispositive of the issue in the civil context. The court held that the defendant's behaviour went beyond what could be regarded as incidental to the exercise of a lawful right of the defense of property. The court also held that the defendant violated the section 1 of the Privacy Act when he intercepted the telephone conversations, listened to them without consent, made a permanent recording and published them to the Ministry of Social Services. The court observed that the defendant had committed the acts intentionally, knew or ought to have known that he violated the plaintiff's privacy, and that his eavesdropping continued for a year. The plaintiff was awarded $30,000 in damages based on the substantial degree of suffering she had experienced, her loss of enjoyment of life, the loss of her reputation and public humiliation and her misconduct as a contributing factor. She was granted $1,000 for out of pocket expenses and awarded 5,000 in punitive damages to reflect the society's abhorrence of the defendant's action and to serve as a deterrent.

PIPEDA Case Summary #2009-009
Published at: https://www.priv.gc.ca/en/opc-actions-and-decisions

Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com

An investigation by the Office of the Privacy Commissioner of Canada (OPC) has concluded that Accusearch, Inc.,[1] doing business as Abika.com, a Wyoming-based search services website, violated key provisions of Canadian privacy law in its collection, use and disclosure of the personal information of residents of Canada.

Abika.com provides a range of search services on individuals by engaging third-party researchers who search for and obtain personal information about individuals from a variety of public and private records and databanks. It also provides a service under which it compiles "psychological profiles" of the behavior and personal traits of specifically identified individuals.

The U.S. Federal Trade Commission (FTC) separately investigated the activities of Abika.com, successfully bringing suit before the District Court for the District of Wyoming to curtail the sale of confidential consumer information. The U.S. Tenth Circuit Court of Appeals recently affirmed the lower court ruling. The OPC filed an amicus curiae (friend of the court) brief in that appeal in support of the FTC position, arguing that the online trade in personal information across international borders threatens the privacy rights of Canadians and the reputations of Canadian businesses.

In its decision, the Tenth Circuit Court of Appeals affirmed that Abika.com was in the business of soliciting customer requests for confidential information and then paying researchers to obtain it. The court also affirmed that the company knew that its researchers were obtaining the information through fraud or illegality. In so doing, Abika.com "knowingly sought to transform virtually unknown information into a publicly available commodity." As a result of this important decision, Abika.com remains under an injunction prohibiting it from trading in confidential customer phone records, as well as other non-public "consumer personal information" without express written permission from the consumer.

This U.S. court decision clearly recognizes the harm to privacy resulting from unauthorized online trade in personal information and offers important new protection to citizens on both sides of the Canada-U.S. border.

Responding to a three-part complaint, the OPC conducted its own investigation of the information-handling practices of Abika.com.[2]

Based largely on information provided by the FTC, the investigation determined that the American company disclosed the personal information of Canadians, without their knowledge or consent, to third parties. The Assistant Privacy Commissioner concluded that such actions contravene the Personal Information Protection and Electronic Documents Act, which governs private-sector companies.

Moreover, the Assistant Commissioner found that Abika.com typically accepts and fulfils requests for personal information without considering whether the request is for an appropriate purpose. In some cases, in fact, the company knowingly turned over the personal information of Canadians for purposes that a reasonable person would consider highly inappropriate in almost any circumstances.

A third element of the complaint, relating to the accuracy of the personal information that was disclosed about the complainant in a prepared "psychological profile", was dismissed on the grounds of insufficient proof. The Assistant Commissioner did, however, underscore her suspicions that much of the psychological profile was highly questionable and inaccurate.

The Assistant Commissioner has recommended that Abika.com stop collecting, using and disclosing the personal information of people living in Canada without their knowledge and consent. The company did not provide a substantive response to the recommendations within the timelines set by the Assistant Commissioner. It was not considered reasonable in the circumstances to grant a request from American counsel representing Abika.com for a further time extension.

The Assistant Commissioner recognized and thanked the U.S. Federal Trade Commission for its invaluable assistance in this investigation. This is an important step in international co-operation and collaboration that will become increasingly necessary to adequately protect privacy rights on both sides of the border in years to come. The collaborative efforts of the OPC and the FTC in this case have enhanced and ensured consistency in approach between the two jurisdictions.

---

[1] *This American company has no relation to and should not be confused with Accu-Search Inc., an Edmonton-based company offering searches of legal documents related to private property and land titles, business and corporate registrations, court matters and vital statistics databases in Alberta.*

[2] *In February 2007 the Federal Court of Canada decided that the Personal Information Protection and Electronic Documents Act gives the Privacy Commissioner of Canada jurisdiction to investigate complaints relating to the trans-border flow of personal information. The court determined that the OPC had jurisdiction to investigate the complaint against Abika.com, even though the company was based in the U.S., and notwithstanding any difficulties there could be in carrying out an effective investigation.*

3.0 INTRODUCTION TO SURVEILLANCE

What is surveillance?

Surveillance is the systematic monitoring of human activity. As technology continues to improve, surveillance becomes easier, less expensive, and more common. Also, after the events of September 11, 2001, many people are much more aware of surveillance, its potential impact on our civil liberties and its potential uses for security purposes. Originally, surveillance was used to aid national security and the police, but now its use has spread to include the monitoring of stores, workplaces and public places, such as parking lots, hospitals, social media, and highways. There are many different forms of surveillance. These include visual surveillance, video-taping with cameras, using tracking devices, and/or recording conversations. Surveillance can involve monitoring one individual (personal surveillance) or monitoring large groups of people (mass surveillance).[405] Surveillance is commonly used to collect information about an individual's activities in order to catch unwanted actions or to prevent unwanted actions from happening. This chapter will look at the various kinds of surveillance commonly used in workplaces, in public places, by the government, by the Canadian Security Intelligence Service and by the police services. It also discusses how your privacy can be affected by surveillance.

3.1 SURVEILLANCE IN PUBLIC PLACES

What is a 'public place'?

The *Criminal Code* of Canada consistently defines the scope of a "public place" as including any place to which the public has access as of right or by invitation, express or implied.[406] By using the word "includes" the Criminal Code definition is listing some descriptions to help you identify a public place, but it also suggests that there may be more types of places that could be considered public places. For instance, a private road was legally treated as a public place even though it could not be seen from the highway it ran next to because it was repeatedly used by the public without objection from the land owner.[407] Since the landowner was aware of the public using the road and did not object to it, he had given an implied or unspoken invitation to everyone that this activity was

---

[405] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (Canberra: Xamax Consultancy Pty Ltd., 1998) Website http://www.rogerclarke.com/DV/Intro.html.

[406] *Criminal Code of Canada*, Revised Statutes of Canada 1985, Chapter C-46, (hereinafter *Criminal Code*), sections 150, 197(1), 319(7).

[407] *R v Lavoie*, [1968] 1 Canadian Criminal Cases 265 (NBSCAD).

allowed. Thus, how the public and the landowner treated the use of the private road made it eligible to be legally treated as a public place.

3.1.1 The Growing Trend of Monitoring Public Places

Am I being monitored in public places?

The general public has come to tolerate a certain degree of surveillance when in public places, both from government agents (such as the police) and private agents (such as an employer). This can be seen in our subtle daily interactions with closed circuit television monitoring cameras. Often when we drive vehicles in or out of underground parking lots, when we approach building entrances, or while we are walking through annexes between buildings, our movement are being taped by security monitors or cameras. We are also taped when we withdraw cash from ATM banking machines to buy milk and bread at the local convenience store, or other cash withdrawals and purchases. When this type of security monitoring first started, it was relatively easy to predict the placement of the black shoe-box sized television. Back then, if you objected to being taped, you could just avoid the relatively few and obviously monitored areas.[408]

Over time, the number of public places being monitored has grown greatly. This may not always be obvious because modern technology has made monitoring equipment smaller and much more difficult to detect. Improvements of features such as bullet proof casings, night vision, the capacity to operate only when something is moving, being able to pan and take pictures over a large area and improved picture quality have all helped to make the use of video surveillance cameras grow to an unprecedented level all over the world. The use of photo-radar to help catch vehicles speeding on roadways has expanded into the use of cameras at street corners to help catch traffic light or turning violations. The monitoring of convenience stores has grown into the monitoring of entire malls. The monitoring of more vulnerable public buildings—like city halls and post offices—has also grown into the monitoring of residential complexes and playgrounds.

Surveillance in public places collects personal information about people without their consent. As the scope, degree and quality of monitoring of public places continues to develop, there appears to be an expectation that our tolerance of being monitored will also grow. Some of us may be

[408] D. Banisar and S. Davies of Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. Report (October 7, 1998) Global Internet Liberty Campaign. website http://gilc.org/privacy/survey/intro.html (hereinafter *Privacy and Human Rights*).

mesmerized by the ever-increasing advances in technology. On the other hand, we may also feel defeated by evolving technology as we realize how all-encompassing it is. People may have mixed emotions about the monitoring of public places, and wonder if they should be concerned about its growing use.

3.1.2 Some of the Potential Benefits of Monitoring Public Places

There is no doubt that the monitoring of public places can be beneficial. More and more, video cameras are seen as a modern-day necessity at vulnerable places, such as banks, convenience stores and underground parking lots. Visual surveillance systems have become a "value-added" feature to be incorporated right into the original designs of modern urban centers and new housing sub-divisions.[409] People feel safer, when these "extra eyes" tape activities in an area and help prevent some crimes from happening or help catch those who commit crimes. Police routinely make use of images caught on video cameras to help identify and track down law breakers. Video camera images can be very good evidence in a court of law. Camera images are not as prone to fading or being distorted over time as a person's memories often are. Camera pictures are more exact reproductions of an event than a person's description of that same event when viewed through their feelings and retrieved from their many memories. The greatest perceived value of having video surveillance systems is that, when used properly, they are like having extra police officers or extra eye-witnesses to help find, prosecute and deter injustices.

3.1.3 Some of the Disadvantages of Monitoring Public Places

Because monitoring is believed to increase the security of public places, the idea of tape-recording the people visiting them may not seem too troubling at first. However, we need to ask whether the use of surveillance cameras really reduces the number of crimes or whether it only serves to displace or move crimes to areas that are not presently being monitored by cameras. Without scientific data about crime trends in Canada, it may be unwise to assume that more surveillance necessarily ensures an overall more secure society.[410]

We also should not assume that increasing surveillance will reduce security costs. Surveillance of public places costs money and the cost may not be proportional to the problem it is meant to fix. For instance, one surveillance camera that monitors traffic light infractions at one street intersection

[409] *Privacy and Human Rights*.
[410] B. Phillips, "Privacy in a 'Surveillance Society'" (1997) 46 University of New Brunswick Law Journal 127.

costs 100,000 taxpayer dollars.[411] There are other less expensive alternatives for dealing with such offences, which may not involve an invasion of our privacy. For example, putting more traffic police officers on patrol would be more cost effective when you consider that often there already are eye-witnesses to infractions, and that the use of cameras would require having someone review the recorded monitoring of the corners anyhow.

Finally, monitoring of the public may also have unintended legal repercussions for those who are taping and those who are taped. For example, business owners may open themselves up to increased responsibility for the safety of their patrons. It may be argued that using video cameras at certain shops is an indicator that you already have some safety concerns, and that there is a duty for you to address these concerns adequately. An example of private individuals monitoring people's activities in a busy place frequented by many people is "Bar Watch,"[412] a voluntary program throughout Calgary where bar owners commit to installing special surveillance cameras to improve safety at their establishments. Some cameras are left on continually as a precaution and to help deter more subtle crimes like theft, harassment, and drink tampering. With general monitoring, however, those who end up being filmed in the bar may also find themselves drawn into a divorce proceeding or a custody battle when the appropriateness of their whereabouts or the company they have been keeping is questioned.

Do business owners become liable for their patron's safety and injuries because they were aware of the potential for crime in or around their shops, as evidenced by surveillance camera use? Is setting up a video camera enough protection for customers or will the courts find that some of the shops ought also to have posted security guards to protect their patrons? Overall, the video monitoring of places frequented by the public may potentially create more legal problems than crimes it helps to solve.

3.1.4 Concerns about Surveillance in Public Places

There are many cameras watching us and not enough laws to regulate issues such as who can legally video tape us, who owns the images collected and what can be done with the video tapes. Wide-sweeping security cameras in residential complexes can take pictures of what is happening in our

[411] S. Craggs, "cameras Are Red Light Cameras a Cash Grab? Some Councillors Say Yes" *CBC News* (18 September 2014).
[412] Z. Nathoo, "Calgary Bars, Clubs Band Together to Keep Watch on Customers." *CBC News* (28 April 2009) (hereinafter Nathoo).

backyards or even in our homes if our curtains are open. Although the Calgary "Bar Watch" monitoring program is not sponsored by the police, the Calgary police applauded the move saying the footage can only be used as evidence in cases where there is criminal activity..[413] But even if police do not have free access to these tapes, other people associated with the bar operation can easily obtain the tapes. Sometimes, an individual's photo is taken and the image is used in a publication without the individual's consent.[414] When considering the benefits of a surveillance program, one should also keep in mind the hidden cost: an infringement of one's privacy. The point is not that we may have nothing to hide, but that citizens should be able to carry on with normal daily activities without being video-taped on a camera.

3.2 Government Surveillance

3.2.1 Government Surveillance in Public Places

Where does government surveillance occur?

Surveillance by video-taping or closed-circuit TV monitoring may occur in provincial government sites such as public libraries, schools, provincial government offices, municipal police departments and hospitals.[415] Some Canadian cities have installed or are considering installing video cameras in other public places as well.[416] It is argued that this public surveillance can help to reduce the incidents of undesirable acts like vandalism, bullying, and theft. The trouble with video surveillance, however, is that it is non-discriminatory. The cameras record all of the activities of all of the people who come into view of the cameras, whether or not they are under suspicion. There are concerns that people could be subjected to video surveillance and have their privacy invaded unduly.[417]

---

[413] Nathoo.
[414] *Aubry v Editions Vice-Versa*, [1998] 1 Supreme Court Reports 591 (S.C.C.) (hereinafter *Aubry v Editions Vice-Versa*).
[415] D. H. Flaherty, "Investigation Report: Investigation P98-012." (Presentation at FOIP '99: The major conference and training session on Freedom of Information and Protection of Privacy in Alberta. Edmonton June 7-8, 1999).
[416] For example, Sherbrooke, Quebec first installed video cameras in public areas in 1991. Other cities, such as Vancouver, Calgary and Edmonton have also considered doing this. See: Volume 35 No. 2 *The Democratic Commitment* "BCCLA opposes spy cameras" Kelowna, Sudbury and others have installed surveillance cameras in public areas. Hamilton police officers intend to bring video cameras with them on domestic abuse calls to tape witness statements. See: A. Aikins, "Cops with Cameras" Rabble.ca February 13, 2002. See also: J. Whiting, "Video Surveillance and Privacy Rights in Schools" (2000) 10 Education and Law Journal 229 at 237 (hereinafter Whiting); Privacy Commissioner, "Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna" News Release, October 4, 2001, Ottawa.
[417] D. Beyerstein, "Video Surveillance in Public Places" Position Paper. British Columbia Civil Liberties Association, 1999.

Are there any laws regulating government surveillance?

Government surveillance can result in the collection of personal information (for example, on a video tape). The Supreme Court of Canada has told us that under the *Charter*, a person has the right to be free from unauthorized secret electronic surveillance where that person has a reasonable expectation that agents of the state will not be watching or recording private activity.[418] As well, the provinces and the federal government have laws regulating the collection of personal information. For example, when personal information is collected by a provincial public body in Alberta, the public body must comply with the rules of personal information collection, use and management, which are listed in the Alberta *Freedom of Information and Protection of Privacy Act* (FOIPFOIP Act).[419] The information produced by monitoring programs, such as video recording or drug testing, falls under the definition of personal information in the FOIPFOIP Act.[420]

For information about the collection of personal information by the government, refer to Chapter 1.

Are there any Privacy Commissioner's findings on video surveillance?

In 2001, the former Privacy Commissioner of Canada, George Radwanski, following a complaint filed by the office of the Information and Privacy Commissioner of British Columbia, found that a video surveillance camera installed by the RCMP in the downtown core of Kelowna, British Columbia, which recorded activities of the general public for 24 hours a day seven days per week, was against the *Privacy Act.* Eleven signs were posted on the monitored area, and signed, "This area of the City of Kelowna may be monitored by video surveillance for law enforcement purposes" He said that privacy is a fundamental human right, which cannot be extinguished simply by telling people that their right is being violated. The Privacy Commissioner (as he then was) also noted that the *Privacy Act* did not outlaw continuous video surveillance *without* recording but hoped that the public would support his belief that this should be allowed only in very specific situations, such as location that are susceptible to a terrorist attack.[421] The RCMP did not remove the cameras.

---

[418] *R v Silva et al*. (1995), 26 Ontario Reports (3d) 554 (Ont Gen Div) (hereinafter *Silva*).
[419] *Freedom of Information and Protection of Privacy Act*, Revised Statutes of Alberta. 2000, chapter F-25 (hereinafter FOIP Act).
[420] FOIP Act, section 1(n).
[421] Canada, Office of the Privacy Commissioner, News Release: "Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna" (Ottawa: October 4, 2001).

The Privacy Commissioner felt so strongly about the public video surveillance in Kelowna that he launched a constitutional challenge in the British Columbia courts.[422]However, in 2003, the British Columbia Supreme Court found that the Privacy Commissioner had no capacity to commence a suit seeking a declaration that the Kelowna RCMP video camera surveillance violated the public's rights under the Canadian Charter of Rights and Freedoms.

What are the guidelines for using surveillance cameras in public places?

As a result of the current widespread use of surveillance videos by the police in public spaces, the Office of the Privacy Commissioner of Canada published a guideline in March 2006, which sets out the principles for evaluating the need to resort to video surveillance and ways of minimizing the impact of the surveillance on privacy. This guideline is reproduced below and was developed by a discussion group consisting of the Office of the Privacy Commissioner of Canada, the RCMP and other stakeholders established following the investigation of the Kelowna RCMP video camera surveillance use.

Excerpt from "OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities" – Guidelines are reproduced fully in the Appendix.

1. **Video surveillance should only be deployed to address a real, pressing and substantial problem.**
2. **Video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less privacy-invasive alternative.**
3. **The impact of the proposed video surveillance on privacy should be assessed before it is undertaken.**
4. **Public consultation should precede any decision to introduce video surveillance.**
5. **The video surveillance must be consistent with applicable laws.**
6. **The video surveillance system should be tailored to minimize the impact on privacy.**
7. **The public should be advised that they will be under surveillance.**
8. **Fair information practices should be respected in collection, use, disclosure, retention and destruction of personal information.**

[422] June 21, 2002. News release: Privacy Commissioner Launches Constitutional Challenge. See: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2002/02_05_b_020621/

9. **Excessive or unnecessary intrusions on privacy should be discouraged.**
10. **System operators should be privacy-sensitive.**
11. **Security of the equipment and images should be assured.**
12. **The right of individuals to have access to their personal information should be respected.**
13. **The video surveillance system should be subject to independent audit and evaluation.**
14. **The use of video surveillance should be governed by an explicit policy.**
15. **The public should have a right to know about the video surveillance system that has been adopted.**

Are there other guidelines for the use of video surveillance of public places?

In 2004, the Alberta's Information and Privacy Commissioner's office published guidelines for using surveillance cameras in public places.[423] The guidelines state:

- Surveillance cameras should only be used where conventional means for achieving the same objectives are substantially less effective than surveillance, and the benefits of surveillance substantially outweigh any reduction of privacy in the existence and use of the surveillance system;
- The use of the surveillance camera is justified on the basis of specific, verifiable reports of crime, safety concerns or other compelling circumstances;
- A Privacy Impact Assessment should be completed to assess the effects that the proposed surveillance system may have on privacy and the ways in which the impacts of any adverse effects can be reduced or eliminated;
- Stakeholders and the public may be consulted as to the necessity and acceptability of the proposed surveillance;
- Ensure that the proposed design and operation of the surveillance system creates no greater privacy intrusion than is absolutely necessary to achieve its goals;
- If a public body is going to use undercover surveillance for a purpose other than a specific law enforcement activity, it should conduct a Privacy Impact Assessment and provide it, together with reasons for the undercover surveillance, to the Information and Privacy Commissioner.

[423] *Guide to Using Surveillance Cameras in Public Places*, 2004. See: https://www.servicealberta.ca/foip/documents/SurveillanceGuide.pdf

The guidelines also provide guidance on how to develop a surveillance policy, installation of surveillance equipment, access, use, disclosure, retention and destruction of surveillance records.

In 1998, the Information and Privacy Commissioner for British Columbia, acting under British Columbia's *Freedom of Information and Protection of Privacy Act*[424] audited two public body sites in British Columbia: a public library and a public insurance provider. Some of the concerns that the Commissioner's office noted in the course of the investigation were[425]:

- hidden cameras, installed for the purposes of deterrence, were not an appropriate tool;
- the public should have adequate notice of the use of video surveillance before actually being under surveillance;
- video surveillance programs should always be accompanied by a written policy governing use of the video surveillance system to help ensure fair and consistent treatment of the collected information;
- there was a lack of investigation into other, less intrusive measures that could have been used and would have achieved the same goal (for example, security turnstiles, sign-in logs, etc.); and
- there was a failure to implement degrees of video surveillance on an escalating basis:
    - for example, start with using signs warning of video monitoring, but have no cameras;
    - if unsuccessful, increase surveillance to signs, and install obvious cameras, but do not run them;
    - if unsuccessful, use signs and run cameras but only for monitoring and not recording to tape;
    - if unsuccessful, increase surveillance to signs, and have the cameras on during high risk periods;
    - if unsuccessful, increase surveillance to signs, and have cameras monitoring/taping continually.

[424] Revised Statutes of British Columbia 1996, c. 165.
[425] B.C. Information and Privacy Commissioner *"Public Sector Surveillance Guidelines"*. (B.C. Privacy Commission: January, 2014) Website: https://www.oipc.bc.ca/guidance-documents/1601 .

Although the collection of personal information may be necessary in order for the various government public bodies to fulfill their services, the potential for information abuse requires close compliance with the privacy legislation pertaining to such public bodies, and the further development of the legislation to keep up with the expansion of surveillance technology. The FOIP Act in Alberta was designed to meet the balancing of public bodies requiring necessary information, with the necessity that the public have some assurance that their privacy is free from unnecessary intrusions or leaks of collected information.

Can you provide other examples of government surveillance?

Sometimes new technologies create concerns about government surveillance. For example, newer telephones come with many features such as:

- **Call Number Display (CND) or Caller ID**, which displays the telephone number of the calling party on a special type of screen;
- **Call Return**, which re-dials the last incoming call; and
- **Call Trace**, which allows customers to have details of the last incoming call recorded and forwarded to a law enforcement agency for investigation.

As telecommunications technology advances, government organizations want to improve their efficiency by incorporating telephone systems that have many features, such as voice mail and Caller ID. Government agents, however, must adhere to federal or provincial privacy laws, which may inadvertently be breached by some of the features of newer phone systems.[426] For example:

- there are circumstances when an institution does not need to know or should not know who is calling or from where—like when an institution provides confidential advice on such matters as sexual harassment, drug abuse, crisis counseling or pay equity;
- the displayed telephone number may not belong to the caller if the caller is borrowing a phone, so if a government agent relies on this phone number without confirming it, the recorded information could be wrong;
- records may be retrieved and displayed on a computer terminal at the same time as an employee picks up the receiver of her telephone, but if the caller is borrowing a phone the information automatically retrieved will not be related to the caller or if the information is not necessary to answer a caller's inquiry it will have been retrieved unnecessarily which

[426] T. Wright, Ontario Privacy Commissioner. "Caller ID Guidelines" Information and Privacy Commissioner: December 1992 website www.ipc.on.ca/english/pubpres/sum_pap/papers/callid-e.pdf

may also contravene provisions of privacy legislation governing the manner in which institutions may use personal information; and

- telephones with Caller ID or Call Return must be placed out of the view and use of the general public to ensure an incoming confidential call remains as such.

Government offices must be aware of their ongoing obligation to adhere to privacy legislation before subscribing to any communication services that may inadvertently breach this legislation and compromise their clients' privacy.

The monitoring of government sites by video surveillance programs and other government practices must adhere to the federal *Privacy Act*, or provincial privacy legislation, which are further discussed in Chapter 1.

What protections from surveillance do I have if the government is my employer?

Your rights as an employee, whether employed by the government or the private sector, are discussed under 3.3.6 Workplace Surveillance.

3.2.2 Canadian Security Intelligence Service and Surveillance

The name of this agency is usually shortened to "CSIS", which is pronounced 'see-sis.'

What is CSIS' purpose?

CSIS has been Canada's spy agency since 1984. It is primarily responsible for helping ensure Canada's national security.[427] Before that, the RCMP Security Service branch did this job.[428] Unlike the RCMP, CSIS is not a police force. CSIS agents do not have the power to arrest or detain people. They do not carry weapons and do not enforce the laws like police officers do. CSIS agents protect Canada's national security by collecting and analyzing information about possible threats to Canada's security and then passing this information on to the government and various law enforcement agencies for them to follow up on. CSIS agents get their powers to investigate such matters from the *Canadian Security Intelligence Service Act (*"the CSIS Act"*)*.[429]

---

[427] For more information on CSIS visit website www.rcmp-grc.gc.ca/html. See also E. Shaw, J. Westwood and R. Wodell, *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How To Protect Them* (Vancouver: B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association, 1994) (hereinafter Shaw, Westwood and Wodell).

[428] I. Leigh, "Secret Proceedings in Canada" (1996) 34(1) Osgoode Hall Law Journal 113 (hereinafter Leigh).

[429] *Canadian Security Intelligence Service Act*, Revised Statutes of Canada 1985, c.C-23.

How do CSIS investigations work?

CSIS does some of its investigations openly and some secretly. Open investigations include having interviews with people whom CSIS agents believe may have valuable information for their investigations. Secret surveillance techniques used by CSIS include tape-recording telephone conversations, eavesdropping on conversations with the use of microphones, searching for documents, checking mail, and video-taping. Before CSIS agents can do any of these types of surveillance, they must first obtain approval from the Federal Court of Canada in the form of a written document called a "warrant". Under the CSIS Act, they do not have to obtain court permission to use covert (undercover) informants. In 1990, however, the Supreme Court of Canada ruled that the RCMP required a warrant to do this type of monitoring for their criminal investigations.[430] CSIS assumed that this court direction would also apply to their security investigations so it became CSIS' policy to get warrants for this type of monitoring as well.[431] In addition to getting court permission to monitor people, CSIS can also make use of its existing agreements with various federal and provincial government departments for automatic access to certain types of information like Revenue Canada's Customs and Excise records and Canada Employment and Immigration records.

How does CSIS get surveillance warrants?

In order for CSIS to get a surveillance warrant from the court, they must first show that the information they hope to gather is "strictly necessary" to their investigation of threats to the security of Canada. [432] They must also swear that other methods of investigation have either failed, would be unlikely to succeed, or would take too much time to get in an emergency situation. In their application, CSIS must name the specific person or persons they want to target for surveillance, the places that will be involved, and the type of information they believe this surveillance will help them collect. If information outside of these listed areas is collected and CSIS just forgot to or missed listing them, the extra information gathered cannot be used. If some of the information collected was unexpected, but is useful to their investigation, CSIS will usually be allowed to use it.

---

[430] *R v Duarte*, [1990] 1 Supreme Court Reports 30 (SCC).
[431] Leigh.
[432] Leigh.

Before applying to the court for a warrant, CSIS' warrant application papers first go through about 34 review steps within the CSIS organization. This is done to help ensure that there are no inaccurate or misleading details, no unsupported opinions or conclusions in the application.

There are only a few judges who have expertise in this particular area of surveillance warrants and who are designated to review and question CSIS' warrant applications. Between 1993 to 2003 CSIS filed warrant applications at a rate of 200 to 300 a year, amounting to a total of approximately 2,544 applications. Out of all of the applications only 18 were rejected by the Federal Courts. This means that 99.3% of the time CSIS succeeded at having their warrant applications approved.[433] In applying to get each warrant renewed, CSIS had to show one of the designated judges what information the original warrant had produced so far and why an extension of the warrant was necessary.

What surveillance powers can a judge grant to CSIS?

The judge can grant many different types of surveillance powers to CSIS. These powers are granted when certain phrases or "clauses" are included in the written warrant. For example, CSIS can apply to be permitted to intercept the communications of a specific person both at a place named in the warrant and also at places to which the person is believed to have gone or will go. This type of surveillance power comes from a warrant having in it a phrase which is commonly called the "resort to clause." CSIS can also apply to be allowed to intercept communications of unknown persons who go to certain places specified in a warrant. Here the surveillance power attaches to a place, and those people who come in contact with it are automatically under legal surveillance. This type of surveillance power comes from a warrant having in it what is commonly called a "basket clause."

In 1997, CSIS made application for a warrant that included a "visitor clause."[434] This type of clause would have given CSIS investigators a warrant for surveillance of a class of persons merely described by CSIS investigators as:

- being of a specific nationality;
- those admitted to Canada as a visitor;
- those identified in CSIS data banks as being known intelligence officers or a member of X group; or

[433] C. Freeze, "CSIS Has Easy Time Getting Warrants," *The Globe and Mail* (21 April 2018).
[434] *Re Canadian Security Intelligence Service Act,* [1997] Federal Court Judgments No. 1228, (QL) [1998] 1 Federal Court Reports 420 (FCTD).

- those for whom there were reasonable grounds to believe they would engage in espionage or other threat related activity while they were in Canada.

In this case, the judge denied the application for a "visitor clause" in a surveillance warrant. The judge held that the law requires a valid surveillance warrant to be initially authorized by a judicial act. This means that the evidence supporting the need for a warrant gets examined by an objective third party who then determines whether the use of such intrusive powers against a person can be justified. It was held that if a "visitor clause" was allowed in a warrant, a judge would be giving CSIS the power to basically issue its own surveillance warrants on any people who fit a certain general description. Thus, while judges will consider approving warrants that include "resort to" or "basket clauses," (described above) they will not authorize a "visitor clause."

Can I challenge the validity of a CSIS surveillance warrant?

Because CSIS warrants are usually applied for *ex parte*, meaning without the person named in the requested warrant being present, you usually do not know that there is a surveillance warrant for you or for the places that you frequently visit. If, however, you are aware of such a warrant, you can make an application to the court to have the warrant rescinded or withdrawn.[435] To do this, you will have to argue that the judge who issued the warrant in the first place made an error in doing so because CSIS did not have enough evidence to support the application for the warrant. The affidavit (sworn statement) listing the evidence CSIS used to support getting the warrant in the first place should be made available for you to look over so you can see what evidence the judge based his decision on to issue the warrant. If the supporting evidence includes the identity or information leading to the identity of any confidential sources or person involved in covert CSIS activities, it may be edited out by the reviewing judge, since the CSIS Act requires that these persons' identities not be disclosed. With the remaining information you have the opportunity to persuade the reviewing judge that there was not enough evidence to support getting a warrant in the first place.

3.2.3 Police Agencies

Can the police "bug," tape, or eavesdrop on my private conversations?

Yes, if they have a warrant to do so. Legally, "communications" are or involve the passing of thoughts, ideas, words or information from one person to another, and "conversations" are generally made up of a series of "communications." Under the *Criminal Code* it is illegal for anyone,

[435] *Atwal v Canada*, [1988] 1 Federal Court Reports 154 (T.D.), appeal allowed (1988), 79 National Reports 91 (FCA).

including the police, to intercept private communications using any device which includes wiretaps, room bugs or recording body packs hidden on a person's body, without a warrant.[436] Even if undercover police agents or other agents of the state, like police informants, are a party to the conversations being wiretapped, they must still have a warrant to record the communications or conversations.[437]

The *Criminal Code* also allows the police to intercept private communications without a warrant when:

- one party has consented to the interception;
- the police have a reasonably grounded belief that there is an immediate risk of bodily harm to the consenting party; or
- the purpose of the interception is to prevent the bodily harm.[438]

If nothing in the private communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur, then the agent of the state who intercepts the private communication is to destroy any recording or transcript of the private communication as soon as possible.[439]

Why would the police want to use wiretaps?

Wiretapping is the interception of a telephone transmission by accessing the telephone signal. It is a convenient shortcut for investigators in that they can more easily gather information from conversations made between two parties who do not know a third, unwelcome party is listening. Wiretaps also produce a foolproof informer. Unlike many other investigative techniques, like informants, wiretaps may be preserved indefinitely and remain as credible as the day they were recorded.

What sorts of reasons would the police have to support getting a warrant for wiretaps?

To get a warrant to carry out electronic surveillance, the police must satisfy a judge that:

- other investigative methods have or would be likely to fail;[440]

---

[436] *Criminal Code*, section 184.
[437] *R v Duarte* (1990), 65 Dominion Law Reports (4th) 240 (SCC).
[438] Section 184.1(1)(c).
[439] Section 184.1(3).
[440] According to the Supreme Court of Canada, this means that a wiretap should only be used if there are no other reasonable alternative methods of investigation under the circumstances. See: *R v Araujo*, [2000] 2 Supreme Court Reports 992.

- granting such a warrant is in the best interest of justice;
- there are reasonable and probable grounds to believe that an offence has been or is being committed; and
- the surveillance will help gather evidence of that offence.[441]

The courts use these same factors when reviewing whether or not the police should have used a wiretap.

What sorts of offences can the police investigate using wiretaps?

The *Criminal Code* sets out a long list of *Criminal Code* and other federal offences that may be lawfully investigated by intercepting private communications.[442] Included in these offences are murder, sexual assault, aggravated assault, uttering threats, and drug trafficking. Should the communications being legally wiretapped turn up information of other crimes that are not listed, the evidence (also called "windfall evidence") could also be used to prosecute the additional offences.[443]

Will wiretap warrants automatically be reviewed by the court when the offence they were used to detect is heard?

Not necessarily. A study conducted by the Solicitor General's office showed that the average conviction rate over five years for cases where wiretap evidence was introduced was only 34%. On the other hand, in cases where the wiretap evidence was not used, the average conviction rate dropped ten per cent to23%.[444] Since it appears that the police actually have a better chance of getting a conviction by introducing the wiretap evidence at trial, it is not surprising that the police use wiretaps as both an investigative tool and for gathering the actual evidence that will be used in court. If it is only used as an investigative tool and not as a means of collecting evidence, the defense would have no way of challenging the legality of the wiretap or even knowing of its existence.[445]

---

[441] *Criminal Code*, section 186 as discussed in Shaw, Westwood and Wodell at 36.
[442] Section 183.
[443] M. V. Fortune-Stone, in J. E. Pink and D. C. Perrier, eds., *Electronic Surveillance—From Crime to Punishment* (3d ed.), (Scarborough: Carswell, 1997) 215 at 218.
[444] Canada, Solicitor General, *Annual Report on the Use of Electronic Surveillance*, 2016 (Ottawa: Public Safety Canada, 2016) Table 11 and 12 at 13(hereinafter *Annual Report*).
[445] *Annual Report*, at 16.

Why should an ordinary citizen worry about police using wiretaps?

The authority for a wiretap cannot specify the precise item being sought so it must permit a much broader search than other types of searches. When a telephone line is tapped, the privacy of the persons at both ends of the line is compromised. If you call someone or someone's home or office that is subject to wiretap, you may be overheard without your knowledge even if your conversation is proper, confidential and not related to the offence being investigated. There is a danger that private information about innocent third parties may be recorded. In this sense, wiretaps can be more intrusive than a physical search because people know they are being searched. Another concern with wiretaps is that the application used in support of getting the warrant is placed in a sealed package.[446] It will not be opened where no charges are laid and there is no evidence of fraud. An individual who was under surveillance, therefore, has no means of knowing if there was police misconduct in placing surveillance on him or her. Wiretapping abuses, sometimes involving thousands of illegal taps, have been detected in many countries.[447] Among these abuses, wiretapping has been targeted at people thought to be political opponents, student leaders and human rights workers.

Does the Charter *help protect against electronic surveillance by the police?*

Yes. Any electronic surveillance by agents of the government, like the police, is a search.[448] The *Charter,* which guarantees our right to be free from unreasonable search and seizure, applies to the government and its agents. This means that the rules developed by the courts for other kinds of searches also apply to electronic surveillance.

For more information on the rules and tests for excluding evidence that has been gathered through the breach of a *Charter* right, please see Chapter 4: Searches.

Section 7 of the *Charter* can be used to support the argument that a defendant should have access to the sealed packet containing the application used to get the surveillance warrant in order to make full answer and defense. Before this information is disclosed, a prosecutor may request and the judge may order the editing of its contents to remove such sensitive information as:

---

[446] *Criminal Code*, section 187.
[447] *U.S. Department of State Singapore County Report on Human Rights Practices for 1997, January 30, 1998* as cited in *Privacy and Human Rights*.
[448] *R v Garofoli*, [1990] 2 Supreme Court Reports 1421 (SCC) (hereinafter *Garofoli*).

- the name of confidential informant;
- anything that might prejudice the interests of innocent persons; or
- anything that might compromise the nature and extent of ongoing investigations.[449]

Can the police use other types of electronic surveillance techniques?

There are other types of electronic surveillance. These include:

- **Video surveillance:** if a person has a reasonable expectation of privacy, then any unauthorized secret video surveillance is considered a search that breaches section 8 of the *Charter* even if the person under surveillance is doing an illegal act.[450] The police, however, can apply for a warrant under the *Criminal Code* to use video surveillance.[451]
- **Tracking devices:** which have been installed to monitor movement are an invasion of one's reasonable expectation of privacy.[452] It is possible, however, for the police to apply for a warrant allowing them to use this technique.[453]
- **Dial or digital recorders:** record the date, time, and length of telephone calls. The telephone number being called from and the number being called are also being recorded. Although the courts have found that the recording of such information does not require special authorization,[454] Parliament has added a section to the *Criminal Code* which requires that the police obtain a warrant for this type of surveillance if there is a reasonable expectation of privacy.[455]
- **Cellular phones:** these transmit messages via radio waves. Messages can be intercepted by scanners. Interception of these calls by the police requires either reasonable grounds to believe that the situation was urgent, necessary, and that the caller or receiver is likely to cause harm or a warrant..[456]

---

[449] *Criminal Code*, section 187. See also: *R v Parmar* (1987), 34 Canadian Criminal Cases (3d) 260 (ONHC), acquittal affirmed (1990), 53 Canadian Criminal Cases (3d) 489 (ONCA) and *R v Garofoli* as discussed Leigh, at 127.
[450] *R v Wong*, [1990] 3 Supreme Court Reports 36 (SCC) (hereinafter *Wong*).
[451] *Criminal Code*, section 487.01.
[452] *R v Wise*, [1992] 1 Supreme Court Reports 527 (SCC).
[453] *Criminal Code*, section 492.1.
[454] *R v Fegan* (1993), 80 Canadian Criminal Cases (3d) 356 (ONCA).
[455] *Criminal Code*, section 492.2.
[456] *Criminal Code*, section 184.5 and 184.6.

Can the police search my cellphone without a warrant?

In certain circumstance the police do not require a warrant to search an individual's phone. The courts have determined that while conducting an investigation police can search a suspects phone if the individual was lawfully arrested, the search directly relates to the person's arrest and if there is an objectively reasonable reason for the search. Additionally, police must take detailed notes of what was examined on the device and how the phone was searched. .[457]

How can I find out if I am under police surveillance?

There is no formal process that allows you access to your file because it is exempted from being disclosed. The only way you can find out if you are currently under electronic surveillance is to hire a private investigator to do an electronic "sweep" of your home or office. Some electronic surveillance equipment, however, is so sophisticated that it is virtually impossible to detect. If you have been under police surveillance in the past, you will eventually receive notification of this, for within 90 days after the surveillance warrant has expired the government must notify you in writing that you were the subject of an electronic surveillance.[458] However, you do not have a right to know why the police had you under surveillance, how long you were under surveillance or what they found out.[459] This notification could be delayed up to three years if the party who applied for the warrant shows how it is the interests of justice to do so and a judge grants such an extension.[460]

3.2.4 Surveillance in Public Schools

My school is thinking about putting up surveillance cameras. Can it do this?

There are a growing number of concerns about the safety of students and teachers in Canada's schools. While it is difficult to conclude that schools are more dangerous, highly publicized events such as school shootings give the impression that they are. One solution considered by schools is to install video surveillance cameras.

Those in favour of installing surveillance cameras in schools argue that they help to ensure a safe learning environment. They also argue that the videotapes created are a reliable source of information about events that occur in schools. Those opposed to installing surveillance cameras argue that students and teachers would be reluctant to participate freely in discussions because they

[457] *R v Fearon,* 2014 SCC 77, 2014 CSC 77.
[458] *Criminal Code,* section 196.
[459] Shaw, Westwood and Woddell, and *Zaduk v R* (1979), 46 Canadian Criminal Cases (2d) 327 (ONCA).
[460] *Criminal Code*, section 196(3).

are being watched. Also, the tapes provide a permanent record of student activities, which could be subject to misuse.[461]

Would surveillance cameras in schools violate my Charter *rights?*

The Supreme Court of Canada suggest that hidden or secret school surveillance would be considered a "search" under *Charter* section 8.[462] Since schools are subject to the *Charter*, any such search must be "reasonable". Whether or not a search is reasonable will probably depend upon whether or not students had a reasonable expectation of privacy in the circumstances. For example, a student walking down a crowded hallway will have a lower expectation of privacy than one using the washroom.[463]

What if the cameras are out in the open? The Supreme Court of Canada has also indicated that students have a significantly reduced reasonable expectation of privacy in schools.[464] One author believes that school surveillance programs that are not secret, and the use of the videos for school discipline and police purposes, would be found to be constitutional under *Charter* section 8.[465] Some jurisdictions there have seen arbitration cases which discuss whether video surveillance within schools is an invasion of students and staff members privacy. It has been found that for video surveillance within schools to be permissible it must either be authorized by statute, used for purposes of law enforcement, or necessary to proper administration of lawfully authorized activity.[466] Necessity is established when the surveillance is more than a mere helpful tool used to enhance the safety of students and staff.[467] The Ontario Privacy Commission has developed a set of Guidelines which can be used by school boards when deciding if surveillance cameras are necessary.[468] The Alberta Privacy Commission have also developed video surveillance guidelines for both public and private organizations. Further, various school boards within Alberta have created regulations for the implementation of video cameras within their schools.

---

[461] Whiting, at 240-1.
[462] See, for example, *Wong*.
[463] Whiting, at 248.
[464] *R v M (MR)*, [1998] 3 Supreme Court Reports 393.
[465] Whiting, at 249.
[466] *Re Halton Catholic District School Board* (2015), 2015 CarswellOnt 11491, Ontario Information and Privacy Commissioner (Hereinafter *Halton*).
[467] *Halton*.
[468] A. Cavoukian, Ontario Privacy Commissioner, "Guidelines for Using Video Surveillance Cameras in Schools", Information and Privacy Commissioner of Ontario: July 2009.

For more information on schools, searches and students' privacy, please see Chapter 4: Searches.

Would school surveillance programs be permitted under provincial privacy legislation?

Several provinces have passed privacy legislation that applies to schools. A videotape from a school surveillance camera would probably be considered a "record" in the control of a public body. So, schools and school boards would need to have policies that ensure that the guidelines laid out in the provincial privacy laws were followed. These guidelines usually deal with information collection, use and disclosure.

For more information on provincial privacy legislation, see Chapter 1.

3.2.5 Government Surveillance and New Technologies

Introduction

Spying on the enemy has been a war tactic since there has been war. When large groups of people began to organize into nation-states, spying expanded to include surveillance of other countries. Huge technological advances have pushed spying up to a whole new level. Computer technology and satellites enable governments to spy on individuals or organizations within the country as well as to combat terrorism, drug-trafficking and other crimes. However, a big concern is whether innocent people's privacy is invaded by blanket technologies like Carnivore and Echelon.

What is the Downstream and Upstream program?

'Downstream' and 'Upstream' are the names of special eavesdropping hardware used by the National Security Agency (NSA) in the United States. Together the software's work to collect private online communication of foreigners outside of America who are believed to possess foreign intelligence information. Downstream works by collecting user data from major internet services such as Gmail, Facebook, Microsoft, and Apple. The Upstream program has the NSA partnering directly with internet service providers such as AT&T so that they can tap into fiber optic cables which carry internet traffic and create a copy of all the live data. The software's are supposed to filter out "wholly domestic" communications between Americans within America, but still collect information between Americans and individuals located abroad. The remaining data is then search by the NSA for any communications to or from specified individuals. Any relevant communications

found is then stored for future searches which do not require a warrant.[469] In 2013 the Snowden leak revealed Canada's knowledge of these programs due to the intelligence sharing pact between America, the United Kingdom, Canada, Australia, and New Zealand. This agreement, more commonly referred to as the Five Eyes Alliance, has resulted in the sharing of intelligence operations between the countries since 1956.[470] These technologies and agreements are not new and have been used in tangent with other surveillance tools for decades. However, the government use of the programs to spy on citizens causes concern for many.

What are the limits to Carnivore?

The Upstream and Downstream program allows the American government to collect data and perform searches without the use of a warrant, as authorized under section 702 of the Foreign Intelligence Surveillance Act.[471] This conduct results in the collection and storing of billions of communications between American citizens and foreign individuals from around the world. Although the collection is large the NSA can only search the data for specific targets who pose a threat to national security. At the beginning of 2017 the American Congress renewed section 702.[472]

What is Echelon?

For years there was a controversy over whether a system called Echelon even existed. But in February 2000 Mike Frost, a former Canadian spy, confirmed its existence. Reports describe it as an automated global interception and relay system that is operated by intelligence agencies of the United States, the United Kingdom, Canada, Australia and New Zealand.[473] The technology works by spying on satellite communications worldwide. The National Security Agency of the United States is reported to be the leader of the group and others contribute.

---

[469] "Upstream vs. PRISM", Electronic Frontier Foundation. Website: https://www.eff.org/pages/upstream-prism (hereinafter Upstream).

[470] S. Kim et al, Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements (Lawfare, 2018), online: <https://www.lawfareblog.com>.

[471] *Foreign Intelligence Surveillance Act*, FIS § 702 (2018).

[472] "How Congress's Extension of Section 702 May Expand the NAS's Warrantless Surveillance Authority", Electronic Frontier Foundation. Website: https://www.eff.org/deeplinks/2018/02/

[473] L. Matney, "Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching you your Entire Life", *Tech Crunch* (August 3, 2015) online: Tech Crunch <https://techcrunch.com/> (hereinafter Uncovering ECHELON).

The United States allows other governments access through international treaties. The first such treaty that set the foundation for the sharing of intelligence information dates back to after World War II, and the first Echelon system is said to have existed in 1971.[474]

What does Echelon do?

According to reports, Echelon is capable of intercepting billions of communications every day—such as phone calls, e-mails, Internet downloads and other satellite transmissions. Data is collected using various means, including ground radio antennae, satellites and sniffer devices on key Internet junctions. There have also been suggestions that underwater phone cables have been tapped with special devices. Like Carnivore, the information is collected at random and then sorted using artificial intelligence programs. One such program is called DICTIONARY; this is actually a special system of computers that searches for key words.

Why haven't I heard of these technologies before if they are so powerful?

In order for an intelligence-gathering technology to be effective, the information recovered must be fairly reliable. In other words, many argue that it is to the advantage of those who use the technology for the subjects of surveillance to be ignorant of the fact that they are being spied upon. This allows spies to get more unguarded statements. There has been no clear, public statement that Echelon exists by governments, although some departments in Australia and New Zealand that are involved in the project have admitted it exists. However, the United States denies that any such system exists.

Why should I be concerned with these kind of programs?

Spying on military targets and enemies of a country is generally accepted as a necessary evil if not a desired use of technology to protect that country. However, powerful technologies such as Downstream/Upstream and Echelon also target, either directly or indirectly, civilians. This means that people going about their everyday business may be caught by government eyes whether this examination is justified or not. Democracies are based on the idea that civilians control and empower government and that civilian freedom should be as unrestricted as possible. If a search warrant based on a reasonable suspicion of wrongdoing is needed before police can enter your home, how can blanket surveillance of people's personal communications or business transactions be permitted? There does not seem to be a good reason for this violation of privacy.

[474] Uncovering ECHELON.

Often the explanation for using these tools is the prevention of crime, especially drug trafficking and terrorism. It is argued that the government needs to use this technology to prevent the harm that criminal activity does to society. These are worthy goals; however, a balance must be struck between security and privacy. It has not yet been proven that the stated goals are worth the cost to our privacy. If the goal of the government is to protect a democratic society, we must look at whether in the pursuit of this goal, the values of a democracy, such as freedom of speech and human dignity, are actually damaged. As well, these technologies may be used as a means of political control. For example, groups like Amnesty International may be targeted more than other groups.[475]

Another concern is that there does not seem to be adequate controls of or accountability for the use of these technologies. Because of the secrecy, it is difficult to know how powerful these surveillance technologies are or if they are abused. Also, more than one nation is involved, and this increases the range of the technologies. National security is a key concern, but invasions of privacy must be limited and justified when they are deemed necessary.

3.3 SURVEILLANCE AND THE PRIVATE SECTOR

3.3.1 Private Surveillance in Public Places

Are there any video surveillance guidelines for private sector organizations?

Yes. In March 2008, the Office of the Privacy Commissioner of Canada ("OPC"), in collaboration with the Information and Privacy Commissioners of Alberta and British Columbia released the *Guidelines for Overt Video Surveillance in the Private Sector*. These Guidelines set out the manner in which organizations should evaluate the use of video surveillance to respect privacy rights and comply with the law and was aimed at businesses subject to the PIPEDA or the Provincial Information Protection Acts of Alberta and British Columbia. These Guidelines *do not* apply to covert video surveillance, like surveillance by private investigators on behalf of people or insurance companies, nor do they apply to the surveillance of employees. Video surveillance is said to be covert when the individual is not made aware of being watched. In 2009 the OPC released the *Guidance on Covert Video Surveillance in the Private Sector*.

What do these guidelines require organizations to do?

[475] Uncovering ECHELON.

The Guidelines require organizations to *follow these ten steps when considering, planning and using video surveillance*

1. Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.
2. Establish the business reason for conducting video surveillance and use video surveillance only for that reason.
3. Develop a policy on the use of video surveillance.
4. Limit the use and viewing range of cameras as much as possible.
5. Inform the public that video surveillance is taking place.
6. Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.
7. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.
8. Give individuals access to information about themselves. This includes video images.
9. Educate camera operators on the obligation to protect the privacy of individuals.
10. Periodically evaluate the need for video surveillance.

What can I do if I think I am a victim of surveillance in a public place?

People who think they have been illegally watched usually first think about approaching the police to lay criminal charges. While it is illegal under the *Criminal Code* to intercept and tape private conversations, it is not a criminal offence to photograph or videotape someone in a public place if there are no voice recordings.[476] Presently, there does not appear to be an appropriate and adequate legal way under the *Criminal Code* to stop a private individual in advance from using a picture taken of you in a public place. Thus, while Canadian law has placed some limitations on government surveillance, there are only a few limits upon surveillance of private individuals by the general public.

Can I be monitored in a public place?

Whether or not you can expect to be monitored in a public place depends on whether or not you have a "reasonable expectation of privacy" while being in that particular place. For example, the courts have decided that although a public washroom is a public place, you have a reasonable expectation of privacy when you are in a cubicle or stall within the washroom.[477] But one can reduce or eliminate what would otherwise be someone's reasonable expectation of privacy in a store fitting room by posting notices that the particular area is being monitored.

---

[476] S. Alter, N. Holmes and W. Young, *Privacy Rights and New Technologies: Consultation Package* (Ottawa: Library of Parliament Research Branch, 1997) (hereinafter Alter, Holmes and Young).
[477] *Silva*.

Even if you could show that you had a reasonable expectation of privacy in the place you had been photographed in, such as a washroom cubicle, the person would not be charged for taking your picture but could possibly be charged by the police for a related offence, such as mischief. To prove mischief, however, one must show that the person destroyed, damaged, rendered useless or interfered with the lawful use, enjoyment or operation of property or data,[478] which does not necessarily come from having your picture taken and used without your consent.[479]

If I choose not to go to the police, what other alternatives do I have for unwanted surveillance?

You might attempt to get an "after-the-fact" remedy for having your picture used by suing for invasion of privacy in civil court. In order to get compensation for the use of your picture without your permission, however, you would have to prove and quantify actual damages generated by the use of the picture.[480] To get an injunction—a court order to stop the use of the picture—will be very difficult because you will have to show that "special damages" will occur from the use of the picture even before the picture is released. Special damages are effects above and beyond those that are inflicted on the general population and could be difficult to establish.

For more information on the right to privacy, see Chapter 1. For information on invasion of privacy, see Chapter 2.

3.3.2 Private Investigators and Surveillance

Are there any special privacy laws that deal with private investigators?

Other than rules under the *Criminal Code*, legislation and common law, which apply generally to everyone, there are currently very few special privacy laws applicable to private investigators. Thus, private investigators are generally not subject to more restrictions than any other person when it comes to privacy.

However, under the *Personal Information Protection and Electronic Documents Act*[481] the collection of evidence for civil litigation (e.g., for a divorce or lawsuit) by a private investigator may

[478] *Criminal Code*, section 430.
[479] See L. Potvin, "Protection Against the Use of One's Likeness in Quebec Civil Law, Canadian Common Law and Constitutional Law (Part I)" (August, 1997) 11 Intellectual Property Journal 203 for overview of law.
[480] *Aubry v Editions Vice-Versa*.
[481] Statutes of Canada 2000, Chapter 5 (hereinafter "PIPEDA").

be illegal. This legislation makes it illegal to secretly collect information about a person without his or her consent, unless the investigator is working for free. There is an exception from requiring consent if there is a contract at issue (for example, in an employer-employee situation). In this case, the private investigator will be able to secretly gather information about the person. However, the legislation does not currently permit that investigator to disclose or share the information he or she has gathered.[482]

For more information about the PIPEDA, see Chapter 2.

If you are a private investigator or an organization planning to hire a private investigator for covert surveillance, what steps should you take to ensure your surveillance is legal?

It is the responsibilities of both a hiring organization and the private investigator it intends to hire for covert surveillance to ensure that all collection, use and disclosure of personal information is done in accordance with privacy legislation. By way of guidance, the OPC, in its Guidance on Covert Video Surveillance in the Private Sector, released in May 2009, recommends that covert video surveillance must be considered only in the most limited cases. In those cases, the OPC recommends that both a hiring organization and the private investigator consider and incorporate the following into their agreement:

- confirmation that the private investigation firm constitutes an "investigative body" as described in PIPEDA "Regulations Specifying Investigative Bodies";
- an acknowledgement by the hiring organization that it has authority under PIPEDA to collect from and disclose to the private investigation firm the personal information of the individual under investigation;
- a clear description of the purpose of the surveillance and the type of personal information the hiring organization is requesting;
- the requirement that the collection of personal information be limited to the purpose of the surveillance;

[482] L. Cohen, "Private Investigators and Forensic Services" (July 2001) 25(7) Canadian Lawyer 46 at 46-7.

- the requirement that the collection of third party information be avoided unless the collection of information about the third party is relevant to the purpose for collecting information about the subject;
- a statement that any unnecessary personal information of third parties collected during the surveillance should not be used or disclosed and that it should be deleted or depersonalized as soon as is practicable;
- confirmation by the private investigation firm that it will collect personal information in a manner consistent with all applicable legislation, including PIPEDA;
- confirmation that the private investigation firm provides adequate training to its investigators on the obligation to protect individuals' privacy rights and the appropriate use of the technical equipment used in surveillance;
- the requirement that the personal information collected through surveillance is appropriately safeguarded by both the hiring organization and the private investigation firm;
- the requirement that all instructions from the hiring company be documented;
- a provision prohibiting the use of a subcontractor unless previously agreed to in writing, and unless the subcontractor agrees to all service agreement requirements;
- a designated retention period and secure destruction instructions for the personal information;
- a provision allowing the hiring company to conduct an audit.

3.3.3 Telephones and Privacy

I called around for prices on a new vehicle without giving anyone my name, but now the dealers are calling me regularly with a "new deal." How did they find out it was me who called?

Many of the new features discussed earlier in this chapter allow people to obtain your information. Caller ID allows for the called party to display and collect the telephone numbers of the incoming calls without the knowledge or consent of the callers even if the callers have an older phone system. Some systems even display the name of the telephone subscriber as well as their telephone number. This feature is useful in that anonymous or nuisance calls could more easily be traced and stopped or, if used like a peephole on a door, left unanswered. But some businesses are using Caller ID to create telemarketing databases. Using "reverse directories," which give a person's name and address from a telephone number, mailing lists can also be created. If you made your price inquiries from

your home telephone without using any "caller blocking" and the business had a Caller ID screen or Call Return feature they would know where the interest in their product originated from and may feel it is part of their service to keep customers who once showed an interest in their product updated on price changes or sales. In most provinces, you can have your telephone number and name "blocked" from being displayed on a Caller ID. If you are calling from a place that has a switchboard system you may need to go through the operator to access this feature. "Call Blocking" is often available for calls made from both regular phones and cell phones.

Is it legal for someone to intercept my cell phone conversations?

No. Even though a person's reasonable expectation of privacy when using a cell phone is low, it is a *Criminal Code* offence to purposely intercept cellular telephone communications,[483] and police cannot intercept and record cell phone conversations without first obtaining proper authorization to do so. [484]

What can I do if I think my phone is tapped?

Even though you do not hear noises on the phone line such as clicks, pops, static or voices, your phone could still be tapped. Most wiretapping devices do not give off any sounds that can be heard by ear alone. If you hear other people talking on your phone you may be experiencing something called "crosstalk," which is a common phone problem and should be reported to the phone company to clear up. If the phone company does find an authorized wiretap, they will not inform you of this. If, however, they find an unauthorized wiretap the phone company will alert you, notify the appropriate law enforcement agency, and remove the wiretap. If someone has intentionally intercepted your private phone conversation you can consult the local law enforcement officials about identifying and charging the individuals under the *Criminal Code* and may consult a lawyer about the possibility of recovering compensation for other types of damages, such as emotional upset.[485]

---

[483] *Criminal Code*, sections 184.5 and 193.1.

[484] *R v Solomon* (1996), 110 Canadian Criminal Cases (3d) 354 (Que CA), affirmed [1997] 3 Supreme Court Reports 696. For a discussion of the lower court decision, see H. L. Rasky, "Can An Employer Search The contents of Its Employees' E-Mail?" (1998) 20 Advocates Quarterly 221 at 226. See also: *R v Cheung* (1995), 100 Canadian Criminal Cases (3d) 441 (BCSC).

3.3.4 Workplace Surveillance - The Employer's Perspective

Why do employers want to use surveillance?

Surveillance of employees by employers always generates heated debates, especially if the surveillance is electronic and constant.[486] Employers often claim that employee surveillance is necessary in order to help:

- promote greater productivity in the workplace;
- conserve resources by curtailing employee misuse or theft of workplace property;
- ensure protection of their workers from harassment and violence;
- prevent employees from violating copyright laws by downloading items;
- prevent employees from smuggling trade secrets and other important information out of the company; and/or
- protect itself from negative publicity associated with embarrassing employee behaviour.[487]

Employers are also quick to add that an employee's actions during working hours are not private actions, and that electronic surveillance is just another and more efficient form of older supervision techniques.[488] From an employer's perspective, in order for a workplace to run successfully and effectively, employees must accept that they have to give up some privacy and autonomy in favour of the employer having control over the workplace and the work done there.[489]

What gives employers the authority to use surveillance?

For authority to use surveillance, employers rely on their "Residual Management Rights," which gives management the right to manage those areas that have not been addressed in an employment contract or an agreement between the workers and the employer (such as a collective agreement).

3.3.5 Workplace Surveillance - The Employee's Perspective

What concerns do employees have about workplace surveillance?

Employees generally accept the idea of residual management rights (defined above), but they have concerns about management using these rights to put in place any rule that it wishes, especially if

---

[486] L. Bevan and A. Staniusz, "Search and Surveillance in the Workplace: The Employer's Perspective" (1992) Labour Arbitration Yearbook 165 (hereinafter Bevan and Staniusz).
[487] A. Conry-Murray, "Special Report—The Pros and Cons of Employee Surveillance" Volume 12 No. 2 Network Magazine pp. 62-66.(hereinafter Conry-Murray).
[488] *FMC Corp*., 46 Labour Arbitration Reports 335 (Mittenthal, 1996) as discussed in Bevan and Staniusz.
[489] B. Bilson, "Search and Surveillance in the Workplace: An Arbitrator's Perspective" (1992) Labour Arbitration Yearbook 143 (hereinafter Bilson).

the rule is arbitrary and discriminatory.[490] Individual workers invest a large part of their lives in their work. They therefore have a great interest in the maintenance of environmental conditions, which help add to their job satisfaction.[491] Surveillance may create job stress and more frequent complaints of stress-related illnesses such as chest pain, digestive problems, headaches and depression. Monitoring may also have a negative effect upon an employee's sense of dignity and overall self-esteem, which in turn may have a negative impact on workplace morale.[492] Even the Supreme Court of Canada recognizes that privacy is essential for the well-being of an individual and is worthy of constitutional protection.[493] Most employees view electronic surveillance as an unnecessary embarrassment, and argue that such a practice should be reviewed to help ensure that:

- it is reasonable;
- it is related to a valid employer goal; and
- the impact that it has on the employees is taken into account.

3.3.6 Workplace Surveillance - The General Rule

What is the general rule about surveillance in the workplace?

One's expectation of privacy in the workplace may not be the same or as great as it is elsewhere, but it does not totally disappear. An employer is entitled to gather information that is related to a legitimate business requirement. Employee monitoring and surveillance are methods that ensure employee productivity.[494] Intrusive and unnecessary information gathering about an employee's private life is not acceptable. What is a fair or reasonable balance between employee privacy and surveillance can be affected by such factors as:

- whether the workplace is *federally or provincially regulated*, which in turn will determine which level of government legislation will impact it;
- whether the employer is from the *private* or *public sector*; and
- whether the employees are *unionized* or *non-unionized*, because if the employment contract for a position is regulated by a contract that a union has

[490] A. Barss, "Search and Surveillance in the Workplace: The Employee's Perspective," (1992) Labour Arbitration Yearbook 181 (hereinafter Barss).
[491] Bilson.
[492] J. West and D. Sanderson. "Monitoring Employee Communications Can Be a Risky Move" (April, 1998) 3 The Lawyers Weekly.
[493] *R v Dyment*, [1988] 2 Supreme Court Reports 417 at 427-28. See also Bilson, at 153.
[494] Conry-Murray.

negotiated, this comprehensive agreement will impact upon both parties' expectations and actions.

My boss has started monitoring us at work with a surveillance camera. Although we do not like it, he will not stop. Can he legally continue to monitor us like this?

Whether an employer's surveillance of an employee in a given workplace is appropriate depends on the particular employment agreement between the employer and the employee, and who the employer is. Generally, if the workplace is ***non-unionized*** or without a formal or comprehensive agreement of employment conditions, a boss in a ***private sector*** workplace is able to introduce this type of surveillance into the workplace since there was no agreement that he would not change the working conditions in the future. This though is still dependent on whether the employee has a reasonable expectation of privacy. In Canada, employees have a general right to privacy in the workplace, however if an employer has a legitimate concern, such as theft, surveillance in a particular area would typically be permitted. The boss though, should give the employees reasonable notice that he will be starting to use this type of surveillance, so that the employees can decide if they want to continue to work there under these new job conditions or to start looking for other work and quit the job when the surveillance actually starts.[495]

If the workplace is ***non-unionized*** and your employer is a ***government*** body, then the employer must comply with the corresponding level of privacy legislation. The federal *Privacy Act* governs the fair practices of the collection and use of personal information and applies to federally regulated work sites like Canada Post and federal government departments. Video-taped records are considered personal information under this Act.

If your employer is a provincial government body, your employer will have to comply with government privacy legislation when gathering and using personal information collected by video surveillance.

The rules and duties imposed under provincial and federal laws are discussed in Chapter 1.

[495] Barss.

If a complaint about surveillance arises in a ***unionized*** workplace where there is a collective agreement—a work contract that a union has negotiated for the employees—then the matter is usually sent to an arbitrator to decide. Arbitrators making decisions do not follow one particular public policy on whether employee monitoring surveillance is appropriate. Each conflict is dealt with as a unique, private problem between the two parties in a particular workplace that have agreed to a specific working agreement. However, the arbitrators do have a set of steps they routinely go through to help ensure they have fully considered all sides of the conflict.

1. First, arbitrators will check to see if surveillance was directly mentioned or indirectly implied in the existing collective work agreement, or if the employer is complying with a legal requirement such as Occupational Health and Safety legislation.
2. Second, if surveillance is not mentioned in the contract, then an arbitrator will determine if it falls within Management's Reserve Rights to introduce a surveillance program by balancing employee privacy with an employer's need to continue to run the enterprise effectively.
3. Third, if the arbitrator finds that management has the authority to implement surveillance, he or she will review the new surveillance program to determine if it is reasonable.[496] If this is a federally or provincially run workplace, the employer will have to follow the rules and duties imposed by the corresponding level of privacy legislation.

What if it is not clear in the collective agreement whether the employer can use surveillance?

To help interpret any unclear language in the agreement, arbitrators may look to other laws to help determine what it means. For instance, if the agreement is between the government or a government-controlled agent and a union, then the rights, freedoms, and other values expressed in the *Charter* may have direct application.[497] In some cases, the *Charter* or other legislation may also be an aid in interpreting collective agreements in the private sector. The Supreme Court of Canada has stated that an arbitration board always has the authority and the duty to apply a statute that is relevant to issues arising under collective agreement.[498] Other information like employee handbooks, company policies, and past practices of the company may also be helpful in understanding the collective agreement. Because collective agreements are often changed or renewed after ongoing

[496] C. Wedge, "Limitations on Alcohol and Drug Testing in Collective Bargaining Relationships" (1994) 2 Canadian Labour Law Journal 461.
[497] *Douglas College v Douglas/Dwantlen Faculty Association*, [1990] 3 Supreme Court Reports 570 (SCC).
[498] *McLeod v Egan*, [1975] 1 Supreme Court Reports 517 (SCC).

negotiations, the ability to use surveillance at a workplace may change over time. At one point in time an employer may have the right to install video cameras, however, at another time this right may have been bargained away.[499]

What is "reasonable" or "fair" for a new surveillance program in the workplace?

Arbitrators have been discouraged from developing a general theory of fairness in interpreting management rights over the years, so arbitrators decide this on a case-by-case basis.[500] In coming to their decision, some of the things an arbitrator may look at are: [501]

- whether this type of surveillance is inconsistent with the existing employment agreement;
- whether this type of surveillance relates to matters that go directly towards the employment relationship;
- whether there is a connection between the new surveillance policy and the orderly and efficient operation of the workplace;
- whether the method of surveillance intrudes as little as possible while still being effective;
- whether the change in surveillance policy was effectively brought to the employees' attention;
- whether the new workplace policy is in harmony with privacy legislation and human rights legislation; and
- whether this workplace surveillance conforms with the values in the *Charter*.

Thus, although the personal or private concerns of employees are not the starting point in reviewing an employer's power to start a surveillance program, employees are entitled to notice about the program and to fairness. Generally, arbitrators do not accept an employer's argument that the surveillance of employees by modern electronic technology is no different than ordinary supervision. If there is no well-founded reason to put in surveillance, arbitrators appear less likely to agree with employers doing what they thought they had the right to do. There is, however, the

---

[499] See generally: *Lenworth Metal Products Ltd. v United Steelworkers of America, Local 3950,* [2000] Ontario Judgments Number 4352, (ONDC), where the court held that it was not patently unreasonable for the arbitrator to conclude that the installation of surveillance cameras was a "rule" in order to determine whether the use of cameras was reasonable under the circumstances. But see: *Re Hercules Moulded Products Inc. and U.F.C.W., Loc. 1993 (Reaume)* (2001), 94 Labour Arbitration Cases (4th) 176, where the arbitrator said that by introducing surveillance cameras to the workplace the employer had not made or changed a "rule" (hereinafter Hercules).

[500] Bilson.

[501] Barss, at 182.

opportunity for an employer to collect and present evidence to show that the least intrusive and minimal surveillance will be used, or that any other form of surveillance will not work in order to successfully support their using a mechanical surveillance system.

Can my employer have me under surveillance outside the workplace?

In today's competitive market, employers are faced with increasing pressures to control costs. An employer may want to investigate an employee's behavior outside of the workplace to confirm that an employee is entitled to a private or public worker's benefit or to "catch" the employee doing something that is inconsistent with his or her benefit claim.[502] When determining if an employer's video tape surveillance of an employee's activities off of the work site during a claimed absence—like taking a "sick day" or "sick leave"—is justified or not, the arbitrator will weigh the employee's right to privacy against the company's right to investigate a possible abuse of benefits. In doing this, an arbitrator may consider:

- whether it was reasonable to initially request surveillance; and
- whether the surveillance was conducted in a reasonable manner.[503]

In other words, there has to be sufficient evidence from the beginning to justify surveillance of an employee outside the workplace. Also, employers must monitor employees only to the extent necessary to protect their interests. If the arbitrator decides that the surveillance or surveillance method invaded the employee's privacy without the employer having a reasonable basis for doing so, the evidence collected by it cannot be used.

Can an employer legally monitor my use of the computer equipment at the office?

Yes, usually.[504] A survey conducted by the American Management Association found that nearly 75 percent of the United States companies surveyed said that they recorded and reviewed their employees' communications activities on the job, and 25 of the companies indicated that they had fired employees for misusing equipment, such as the Internet and e-mail.[505]

Although employees can often assume that their use of company e-mail may be monitored, employees have a reasonable expectation of privacy when using workplace computers. However,

---

[502] *Doman Forest Products Ltd. et al.* (1990), 13 Labour Arbitration Cases (4th) 275 (Arb. Bd.) (hereinafter *Doman Forest*).
[503] Hercules.
[504] A. M. Gahtan, "Monitoring Employee Communications" (1998) 2(2) Information & Technology Law 29.
[505] D. Moulton, "Workplace e-mail raises liability, privacy concerns" Volume 20 Number 39 *The Lawyers Weekly* February 23, 2001 at 11.

employers do retain the right to delve into employee's computers so long as it is reasonably justified.[506]

As modern technology has developed the tools used to monitor employees have also expanded. For example, employers can track what you searched for on the internet or replaying back-up copies of "deleted" phone or e-mail messages. Surveillance of the use of these systems has developed partly because these tools are open to abuse by employees who may use them for personal—possibly illegal—purposes that might be attributed to the employer. For example, if an employee uses his employer's tools to download copyrighted intellectual property or to send hate literature, these acts will probably be attributed to the employer who owns, and is supposed to control, the tools. Employers may also want to monitor keystrokes on computers as a way of determining an employee's production.[507] Employers also do not want their internet resources wasted on such activities as personal or inappropriate site "surfing."

Although a company owns the tools to monitor its employees, this does not automatically give an employer the unrestricted right to monitor an employee's use of equipment. The important key in determining whether or not an employer's monitoring activities constitute a violation of the criminal law or of an employee's privacy rights is whether the users of the tools had a reasonable expectation that their messages would not be intercepted by any other person.[508] The presence of user identification codes and passwords creates an impression in many employees that their e-mail messages are private messages, yet private messages can provide information about an employee's personal life that employers may use later in promotion or layoff decisions. Also, although it is an offence under the *Criminal Code* to "intercept a private communication,"[509]the review of items such as previously sent e-mail is not the "interception" of a "communication." Only intercepting or reading an e-mail while it is originally being sent is illegal—not reading it at another time.[510]

---

[506] *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34.
[507] *Privacy and Human Rights*.
[508] C. Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill Law Journal 849 at 849 (hereinafter Morgan).
[509] *Criminal Code*, section 184.
[510] *R v Weir*, [1998] Alberta Judgments 154. (QL).

Thus, whether an employee has a reasonable expectation of privacy depends on the totality of the circumstances which is determined by analyzing:

- the nature of the material being searched;
- whether the employee had a subjective expectation of privacy with regards to the searched material;
- whether the employee had a direct interest in the material being searched; and
- an assessment as to whether the subjective expectation was objectively reasonable.

3.4 CONCLUSION

Surveillance can be used to help ensure our safety, but it can also be a threat to our personal privacy. While it is illegal for someone to intercept private conversations (wiretapping or bugging) without court permission, it is not illegal for people to take our photographs or videotape us without our permission.[511] Modern technology has developed cameras that are able to zoom in on objects as small as the writing on a cigarette package up to 300 meters away and can take good pictures in what appears to be total darkness. Technology has also developed a camera that can scan a crowd of twenty faces in a second and then match these faces to pictures of faces already collected and held on another file.[512] One can only imagine the invasion of privacy that would be generated if this type of surveillance system was used with a closed-circuit television system monitoring busy public places. Once all the latest surveillance technology is in place, the door to our privacy cannot remain closed. Strong legislation will be required for striking a fair balance between privacy and the need to know.

[511] Alter, Holmes and Young.
[512] Alter, Holmes and Young.

3.5 CASE STUDIES

3.5.1 Surveillance During Employment

Colwell v Cornerstone Properties Inc., [2008] OJ No. 5092

The use of a secret video camera in an office environment.

An employee who had been with a company for seven years, and had been promoted to a commercial manager, left her job after discovering that a secret video was installed in her office by her immediate boss. The employee asked for an explanation and questioned why she was not advised of the camera since she was the person directly responsible for the maintenance of staff. When her immediate boss could not provide a satisfactory answer, the employee considered the incident as a breach of her employment contract amounting to constructive dismissal. Amongst the issues for determination were, whether there was a constructive dismissal, whether the employee failed to mitigate her damages, and whether she was entitled to aggravated and /punitive damages. On the issues of constructive dismissal, the court held that installing a secret camera in a trusted manager's office without her knowledge, although acceptable employer conduct, when coupled with the totally implausible explanation of the immediate boss, was an unacceptable action. The court also ruled that the cost to human dignity caused by the surveillance along with the unbelievable explanation of the immediate boss left the employee in a position of being unable to rely on his honesty and trustworthiness. This amounted to more than mere bad faith and unfair dealing, hence not only her privacy was violated but also her contract of employment, because all her trust evaporated. The court found that the employees' contract of employment contained an implied term that each party would treat the other in good faith and fairly throughout the employment, and that she was justified in leaving a poisoned atmosphere and was thus constructively dismissed. On the issue of mitigating her damages the court ruled that the employee was not obligated to return to the defendant in order to mitigate her damages as she had made every effort to find alternative employment. The employee was awarded $15,279 based on her salary of $37,500 and her proper period of notice, which was seven months. The court found that the employer's actions were not sufficiently egregious to warrant punitive damages.

Re Alberta Wheat Pool and Grain Workers' Union, (Williams, 1995) [513]

A case emphasizing that employee surveillance outside the workplace is a last resort.
In this case a worker had accumulated a long history of absences from work due to illness. For example, at one point the worker had taken two 78 week long absences from work, having worked only 20 days in-between the two absences. When the employer heard rumors that the employee was building a house in the Okanagan and realized that the employee had returned to work just as his benefits were to run out and stayed only long enough to qualify for long-term disability benefits, the employer hired private detectives to videotape this employee's activities to determine if the employee was doing activities that were inconsistent with his claimed illness. When the case went before an arbitrator, however, the arbitrator decided that the employer could not use the videotape evidence because, even though an employer has the right to investigate the reasons for an employee's absence when there are suspicious circumstances, the employer must first consider less intrusive alternative methods to get this information, like questioning the employee more carefully or questioning his doctors.

[513] *Re Alberta Wheat Pool and Grain Workers' Union, Local 333* (1995), 48 Labour Arbitration Cases (4th) 332 (Arb. Bd.).

Re Puretex Knitting Co., (Ellis, 1979) [514] Employee privacy in the workplace is not to be eroded because of a minor company concern.

The president of a company that manufactures sweaters and other garments had concerns about in-plant theft of his stock, so the workplace had a practice of regularly inspecting the handbags of the women employees as they left the plant. In a 20 year period there where a maximum of 10 occasions where some form of theft was discovered or suspected. However, following a major theft incident, in which a woman had removed $100,000 to $150,000 worth of merchandise over a period of years using a "booster bag" with a false bottom, management installed nine closed-circuit television cameras in the plant for the purpose of deterring theft. These cameras rotated with the speed of a second hand on a watch, did not tape-record, and did not have zoom capabilities for more detailed inspections. The cameras were obvious, but were installed without notice to the workplace union or employees. The union persisted in its attempts to have the cameras removed, but the collective agreement did not disallow the use of cameras and the employer refused to remove them. The case eventually went to an arbitrator and, although the arbitrator could not be persuaded that the cameras were a source of psychological stress on the employees because they were only there to deter theft and not to assess worker performance, the arbitrator did order the removal of the cameras in the production area. In coming to this decision, the arbitrator pointed out that the only possible justification of this type of surveillance was the one serious "booster bag" theft incident, that aside from this one incident there was not a theft problem of serious enough proportions to warrant use of this form of surveillance, and that this type of slow rotating surveillance was unlikely to deter this type or mode of theft anyway.

[514] *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union*, (1979) 23 Labour Arbitration Cases (2d) 14 (Arb. Bd.).

3.5.2 Surveillance of Public Places

Heckert v 5470 Investment Ltd., [2008] BCJ No. 1854

Invasion of privacy by a landlord.

Heckert brought an action for damages against the defendant for invasion of her privacy and breach of her right to quiet enjoyment. She was a tenant in an apartment building consisting of 12 floors and 49 suites and owned by the defendant. A surveillance camera was installed on the 12th floor where Heckert lived, and at the time, was the only camera in the building. From the way the camera was installed, any person watching the video images was able to see very close –up and detailed images of anyone entering and exiting Heckert's suite. Heckert and the building manager did not get along and the manager had made several attempts to evict her. In one of the disputes, Heckert refused to show identification and to sign for new keys and the manager denied her ready access to the building for 28 days. Heckert considered this interference to her right of quiet enjoyment. She argued that the video surveillance camera invaded her privacy and caused her stress. The defendant, on the other hand, argued that Heckert had no right of privacy in and about the 12th floor hallway and that her right to quiet enjoyment was not interfered with. The court ruled that the defendant violated Heckert's right to privacy and that the violation was willful. Although the court found that the 12th floor was a public place, it determined that Heckert was nonetheless entitled to be free from the scrutiny of a surveillance camera upon entering and exiting her apartment suite because she enjoyed a reasonable expectation of privacy in the hallway. In reaching its decision, the court considered that the positioning of the camera was disturbingly intrusive, was of little utility as a means of assisting police in identifying trespassers and only showed people in detail when in close proximity to Heckert's suite. Heckert was awarded $3500 for the breach of her privacy. The court rejected Heckert's claim for breach of quiet enjoyment because it should have been pursued by way of judicial review.

Regina v Sloan, 1994 (Ontario Court of Appeal) [515]

The possible treatment of motor vehicles as private and public places.

In this case the driver of a motor vehicle was suspected of being about to engage in criminal activity. The police followed the motor vehicle from a city's Main Street area to the far, tree-covered corner of an almost deserted parking lot two miles away. Upon sneaking up to within one and a half feet of the driver's side car window, a police officer noticed an illegal act being performed in the car. The people in the car were charged with doing an illegal act in a public place. The court, however, ruled that a motor vehicle is in itself a private place. (Even an undercover police officer's vehicle is a private place)[516]*The court also ruled that a motor vehicle does not automatically stop being a private place merely because it is parked in a place that the public has lawful access to. However, if the illegal act in the vehicle was being done within the sight of more than one person, like above the dashboard or by a heavily traveled area, the act would be taking place in a public place. The police's surveillance, purposely going up to the car to look into it, did not change a private place into a public place, and the charges were denied.*

[515] *R v Sloan*, [1994] 18 Ontario Reports (3d) 143 (ONCA).
[516] *R v Hutt*, [1978] 2 Supreme Court Reports 476 (SCC).
[110] *R v Wong*, [1990] 3 Supreme Court Reports 36 (SCC).

3.5.3 Police Agencies

R v Wong, 1990 Supreme Court of Canada[110]

A case establishing that unauthorized video surveillance by police violates one's right to be free from unreasonable search and seizure.

Police suspected that a particular hotel was repeatedly being used as a "floating" gaming house by people of Asian descent. Since the identity of the Asian police officers was well known in the community, it seemed virtually impossible to infiltrate the gambling sessions. The police concluded that only video surveillance would enable them to further their investigation. The Metro Police Intelligence Branch and a Crown Counsel did not believe that under the present law it was possible to obtain judicial authorization to specifically conduct video surveillance. There was no law prohibiting video surveillance, so the investigators decided to proceed without special video surveillance authorization and installed a video camera in the drapery valance of the room that was registered to a person suspected of gambling. After monitoring the activities in the rooms on five separate occasions, the police had no doubt that illegal gambling sessions were being held in the hotel suite. The suite was raided and several occupants were charged with the offence of keeping a common gaming house. At trial, the judge dismissed the charges holding that the video surveillance of the accused was a violation of section 8 of the Charter and excluded the evidence collected by it. The higher Court of Appeal, however, stated that there was no Charter violation because the accused could not have a reasonable expectation of privacy when doing something illegal. The case was appealed all the way up to the Supreme Court of Canada where it was determined that:

- *whether a person has a reasonable expectation of privacy or not cannot be based on whether or not that person is engaged in an illegal activity,*
- *video surveillance is an invasion of a reasonable expectation of privacy and thus violates section 8 of the Charter,*
- *there was no warrant available for video surveillance that the police could have applied for, and*
- *despite the Charter breach, the resulting evidence should not be excluded due to a reasonable good faith misunderstanding by the police officers and the lack of a strong argument showing how its use would have brought the administration of justice into disrepute (Section 24(2) of the*

Charter provides that evidence that is obtained in a manner that infringes the Charter shall be excluded if its admission will bring the administration of justice into disrepute.)

It is important to note that the police cannot do something even if it is not illegal, if the activity involves a Charter violation. After this case, a specific section of the Criminal Code was added to deal with the procedures for getting authorization for video surveillance warrants.

4.0 INTRODUCTION TO SEARCHES

This chapter looks at searches in several different situations, such as searches by police, in workplaces, at border crossings and at schools. The law that applies to each of these areas varies depending on whether the search is done by the government or occurs in the private sector.

4.1 SEARCHES BY GOVERNMENT

Section 8 of the Canadian *Charter of Rights and Freedoms*[517] provides that everyone has the right to be "secure against," or in other words, "free from," unreasonable search or seizure. Generally, we think of a search as looking for something, and a seizure as the taking of a thing from a person without that person's consent. Since the *Charter* applies to governments, we are protected from unreasonable search or seizure by the government. In order to take advantage of the protection in section 8 in a particular situation, one must establish three things:

- FIRST: that a search or seizure involving government action occurred;
- SECOND: that the search or seizure was unreasonable; and
- THIRD: that the evidence turned up in the search or seizure should not be used in court.

However, our *Charter* rights are not absolute; their importance in a particular situation must be balanced with the state's concern for the good of society as a whole. Thus, there are situations where even though the government has violated *Charter* section 8, the search or seizure will be found to be constitutional. **For further information about how the *Charter of Rights and Freedoms* works in Canada, refer to Chapter 1.**

4.1.1 POLICE SEARCHES

The *Charter* applies to police officers who are conducting searches because they are considered to be acting for the government or state. Over the past decades, no area of the criminal law has changed as much as the area of search and seizure.[518] Because the law of search and seizure is constantly and quickly evolving, it is difficult to state what exactly the rules are in this area at any one point in time. In determining whether or not the police can do a search or use the evidence from a particular search in court, the court applies many different layers of tests that continue to be more narrowly defined.

---

[517] *Canadian Charter of Rights and Freedoms* Part I of the *Constitution Act*, 1982, being Schedule B of the *Canada Act 1982* (U.K.), 1982, c.11 (hereinafter *Charter*).

[518] F. P. Hoskins, "Search and Seizure" in J.E. Pink and D. C. Perrier, eds. *From Crime to Punishment* (Carswell: Scarborough: Carswell, 1997) 303 at 303 (hereinafter Hoskins).

This section is not meant to be an exhaustive review of the law of search and seizure, but rather a general overview of the general principles behind the evolving laws.

Is it a search or seizure?

In the criminal law, some things that are searches or seizures are obvious to one's common sense, but others are not. For example, searches include:

- having someone strip,
- rummaging through someone's pockets, or
- looking through a person's desk.

While taking scrapings of the debris from under one's fingernails is a search and seizure, taking someone's fingerprints off of something is not. The taking of blood or urine for tests is intrusive and each type of sample stores a great deal of information on a person; taking either sample is a search. Taking a sample of a person's breath for a Breathalyzer test is considered to be similar to taking a blood sample and is also a search. Collecting a sample of a person's voice, handwriting or picture of one's physical appearance are not searches because we often freely show these things to the public.

What is and what is not considered to be a search or seizure for the purpose of the criminal law is based on what the court calls a person's "reasonable expectation of privacy". The degree of privacy that a person might reasonably expect varies depending on the type of activity or situation that brings her into contact with the state.[519] The courts tell us that what a person's reasonable expectation of privacy is must be determined by taking into account all of the circumstances in any particular situation, some of which are:

- whether or not the person was present at the time of the search;
- if the person had possession or control of the property or place;
- if the person owned the property or place;
- the historical use of the property;
- the person's ability to regulate access, including the right to admit or exclude others from the place;
- if the person thought they had an expectation of privacy; and

[519] B. Hovius, S.J. Usprich and R. M. Solomon, "Employee Drug Testing and the Charter" (1994) 2 Canadian Labour Law Journal 345 at 364 (hereinafter Hovius, Usprich and Solomon).

- if it appeared to others that the person had a reasonable expectation of privacy.[520]

If an accused person cannot establish that she had a reasonable expectation of privacy, then she cannot rely on the protection of the *Charter* guarantee that one is to be free from unreasonable search or seizure. However, if an accused person does establish that she had a reasonable expectation of privacy at the time the police search or seizure was done, then the search must be reviewed as to whether or not it was reasonable or unreasonable.

Was the search unreasonable?

Many searches are done after getting the written authority to do so in a document called a search warrant. A valid search warrant requires that a neutral and impartial person, who is capable of balancing the interests of the government against those of the individual, like a judge or a justice of the peace, is satisfied that:

- the person who wants the warrant swears that he has reasonable grounds to believe that an offence has been committed;
- the pieces of evidence which are listed in the warrant, and authorized to be seized, are those which are strictly relevant to the offence under investigation; and
- evidence of the particular offence under investigation will be recovered in the search.[521]

Generally, a search done without a search warrant is unreasonable.[522] There are some exceptions to this, such as a search done after a person is arrested or the taking of a breath sample for alcohol content analysis. With or without a valid search warrant, the search process still needs to be examined to see if it is reasonable. The general test is that a search or seizure will be reasonable if:[523]

A) it is authorized by law;

B) the law authorizing the search or seizure is a reasonable law that is constitutional; and

C) the manner in which the actual search or seizure was carried out is reasonable.

---

[520] Hoskins, at 305.
[521] Hovius, Usprich and Solomon, at 367.
[522] *R v Hunter* (1987), 59 Ontario Reports (2d) 364, (ONCA).
[523] *R v Collins* (1987), 33 Canadian Criminal Cases (3d) 1 (SCC) at 14 (hereinafter *Collins*).

A) Whether or not the search is authorized by law

In Canada there are only two possible sources of legal authority for a search or seizure: the common law and statutory law.

Common Law:

Presently there is common law (also called "case law") to show that there is authorization for at least the following nine types of searches and seizures:

1) Search Incident to Arrest ("SIA"): A peace officer or a citizen automatically has the authority to search a person at the time of a lawful arrest[524] for the protection of the person making the arrest or for just a general search for evidence. This is sometimes referred to as a "pat down" search. Generally, a SIA does not have to be done at the exact same time as the arrest. There may be circumstances that force a delay in the SIA, such as waiting for a police officer of the same sex to arrive and conduct the search.[525] The Supreme Court of Canada, however, has stated that the exercise of this SIA power is not unlimited.[526] In particular, the court said:

a. The SIA power is a discretionary power; the police officer does not have to use it. When a police officer is satisfied that the law can be effectively and safely applied without a SIA, he may not need to do one.

b. If a SIA is done, it must be done to support a valid reason connected to the arrest, such as discovering an object that may be a threat to safety, help one escape, or act as evidence against the accused. A SIA is not to be done just to intimidate, ridicule or pressure the accused to into making admissions.

c. A SIA must not be done in an abusive fashion, and any restraint used should be in proportion to the purpose and the other circumstances of the situation.

A search incident to arrest that does not meet the above goals could be characterized as unreasonable, unjustified at common law, and therefore a breach of section 8 of the *Charter*.[527]

2) Search With Consent: A peace officer is allowed to conduct a warrantless search or seizure of a person, place or thing where the person has consented to it.[528] In court, however, the prosecution must show that the consent was valid by showing that the person giving consent:

---

[524] *Cloutier v Langlois* (1990), 53 Canadian Criminal Cases (3d) 257 (SCC) (hereinafter *Cloutier v Langlois*).
[525] *R v Simmons* [1988] 2 Supreme Court Reports 495, (SCC) (hereinafter *Simmons*) as discussed in Hoskins.
[526] *Cloutier v Langlois*, at p.278.
[527] Hoskins, at 307.
[528] *R v Dyment*, [1988] 2 Supreme Court Reports 417 (SCC) as discussed in Hoskins, at 309.

- said or implied that she consented through words or conduct;
- had the authority to give the consent in question;
- voluntarily gave the consent and was not coerced by the police or by other conduct;
- was aware of the nature of the police conduct to which she was being asked to consent;
- was aware of his or her right to refuse to permit the police action; and
- was aware of the potential consequences of her giving consent.

3) Search of Cars: A car can be searched as part of a SIA if the accused was in the car or had just gotten out of it. A car may also be searched when:[529]

- the vehicle is stopped, or the occupants are detained, lawfully;
- the officer doing the search has reasonable and probable grounds to believe that an offence has been, is being, or is about to be committed and that the search will turn up evidence relevant to that offence;
- there are exigent circumstances (such as the possible removal or destruction of evidence) that do not make it practical to get a warrant; and
- the scope of the search is within reasonable relationship to the offence suspected and the evidence sought.

The courts have determined that when a police officer requires a driver to produce her driver's license and the vehicle's insurance, it is not a search for the purpose of *Charter* section 8.[530] This particular request does not intrude on a person's reasonable expectation of privacy because the driver of a motor vehicle has to produce a license and other documents to show that she is complying with the legal requirements attached to the privilege of driving a vehicle on public property.

4) Search of that which is in "Plain View": If a peace officer sees an object in her plain view, then she has the right to seize it without a warrant, if:[531]

- the officer's "initial intrusion", or position from which she saw it, was lawful;

[529] *R v D(ID)* (1987), 38 Canadian Criminal Cases (3d) 289 (Sask CA) as discussed in Hoskins, at 308.
[530] *R v Hufsky*, [1988] 1 Supreme Court Reports 621 (SCC) as discussed in Hovius, Usprich and Solomon, at 361.
[531] *R v Ruiz* (1974), 8 New Brunswick Reports (2d) 46 (NBCA).

- the officer accidentally discovered the evidence and did not know in advance that it was there and decided to seize it by purposely relying on the "plain view" authority;[532] and
- it was immediately clear to the officer that the items seen may be evidence of a crime, were contraband (illegal) or were otherwise subject to seizure. (One cannot seize something just because it is in plain view.)

5) Search of Garbage: Garbage can reveal a lot of intimate facts about our lives: our sex practices, our medical conditions, our personal relationships, our political affiliations, our eating, reading and recreational habits and the like. When we put out our trash, we expect it to be collected, combined with the trash of others, and then taken to a dump. We do not expect it to be inspected. Yet, how can we expect that which we deliberately throw away to remain private? The courts have decided that, where the householder shows that he is abandoning the garbage by putting it off of his property in such a way as to indicate his intention to abandon possession of it to others, he no longer has a reasonable expectation of privacy in it and makes it open to everyone, including police officers.[533] The court, however, has determined that although a person has a lower expectation of privacy after being arrested, it is not so low as to allow the automatic seizure of his garbage because he no longer has control of how or to whom he discards it.[534] The position will be different in a situation where an accused has already abandoned his garbage before it was seized by the police during his arrest. By abandoning his garbage an accused would objectively have no subsisting privacy interest on the garbage. See *R. v Patrick* below under **Case Studies**.

6) Strip Search: Although a strip search is highly intrusive, and may include such actions as bending over to expose the rectal area, it is authorized if there are reasonable and probable grounds to believe it is necessary. For example, if a person arrested has a criminal record for concealing drugs or weapons on the body, it would be reasonable to check for these things.[535] The Supreme Court of Canada has indicated that strip searches are only constitutionally valid if they are conducted as part of a lawful arrest in order to discover weapons, in order to ensure the

[532] *R v Law* [2002] Supreme Court Judgments Number 10. In this case the police recovered a stolen safe and took photocopies of the contents. The court said that this was not a "plain view" search because the officer took the documents and photocopied them to discover evidence of tax fraud. It was not something that could be seen from plain view.
[533] *R v John Krist* (1995), 100 Canadian Criminal Cases (3d) 58 (BCCA).
[534] *R v Stillman*, [1997] 1 Supreme Court Reports 607 (SCC) (hereinafter *Stillman*).
[535] *R v Flintoff* (1998), 126 Canadian Criminal Cases (3d) 321 (ONCA).

safety of the detained person, the police or others or in order to discover, preserve or prevent the disposal of evidence. The strip search must be conducted in a way that does not infringe the detained person's *Charter* rights. Generally, strip searches should only be conducted at the police station, except where there are difficult circumstances.[536] See *R v Golden* below under **Case Studies**.

7) Search of Lower Body Cavity: This is another highly intrusive search where a sigmoid, or curved tube, may be inserted up to six or eight inches into an arrested person's lower body cavity to search for evidence.[537] See *Reynen v Antonenko* below under **Case Studies**.

8) Search of the Mouth: Because items such as packets containing drugs can be concealed in the mouth and quickly swallowed when a person is detained, case law authorizes that in certain circumstances a police officer may grab a person by the throat to prevent him from swallowing and then inspect the inside of the person's mouth.[538] Although this is both alarming and painful, it may be the only way to prevent a suspect from swallowing evidence.

9) Search Incident to Duty: Just because police officers have a duty to do something does not always mean that they are automatically given all the tools or powers to complete their duties. Common law from the Supreme Court of Canada, however, shows that if a police officer's conduct falls within the general scope of her duty and if the conduct involved a justifiable use of power associated with the duty, then the officer's conduct is justified.[539] For example, there is no written law that says you can stop a vehicle to talk to the driver to see if he is impaired, but because it is part of a police officer's duty to preserve peace—prevent crime or protect life and property—and because impaired driving is a serious problem that needs detection and deterrence, the court has determined that police officers have common law authority to randomly stop vehicles to implement programs such as "Check Stop" or "Alert" to help them combat impaired driving.

Legislation:

[536] *R v Golden*, [2001] Supreme Court Judgments No. 81.
[537] *Reynen v Antonenko et al* (1975), 20 Canadian Criminal Cases (2d) 342 (hereinafter *Reynen v Antonenko*).
[538] *Stillman.*
[539] Waterfield test from *R v Dedman*, [1985] 2 Supreme Court Reports 2 (SCC).

Aside from the common law (judge made law), another source of authority for searches is legislation (written laws passed by the government). Legislation can protect people from unfair invasions of privacy because legislation requires a neutral and impartial judge to weigh out the competing interests between the person and the government before authorizing a search or seizure.[540] Many provincial laws give police the power to search and seize in certain circumstances, and usually each piece of legislation is worded very specifically so as to cover only a particular area. While the individual search and seizure provisions can vary from one provincial Act to another,[541] section 487 of the *Criminal Code* authorizes the issuing of a search warrant for all federal Acts.[542]

Some of the searches and seizures authorized by the legislation in the Canadian *Criminal Code* are:

1) Collection of Forensic DNA Samples: The police can get a warrant that authorizes them to take samples of bodily substances for the purpose of forensic DNA analysis.[543] For a discussion of this process see **Chapter 6 Genetic Testing**.

2) Video Taping and Wiretaps: For a discussion on these two types of authorized surveillance/searches see **Chapter 3 Surveillance.**

3) Searches or Seizures in Dwellings: Since 1997 the *Criminal Code* has given a police officer the authority to do a search of a dwelling or arrest a person in a dwelling with or, in some special circumstances, without a warrant.[544] In some situations, the police may not even be required to announce themselves before entering the dwelling. For more information about the circumstances that helped the government decide that the police needed this power in some situations see *R v Feeney* under **Case Studies**.

4) General Investigative Search Warrants: The *Criminal Code* allows a police officer to use any investigative technique, device or procedure (including video surveillance) which would otherwise be an unreasonable search or seizure if he can show a judge that:[545]

---

[540] Hoskins, at 310.
[541] Hoskins at 310.
[542] Hoskins at 311.
[543] *Criminal Code* Revised Statutes of Canada 1985, chapter C-46, section 487.05, (hereinafter *Criminal Code*).
[544] *Criminal Code*, section 495(1).
[545] *Criminal Code*, section 487.01 as discussed in Hoskins, at 319.

- there are reasonable and probable grounds to believe that a federal offence has been or will be committed;
- information concerning the offence will be obtained through the use of the technique;
- it is in the best interest of the administration of justice to issue this technique; and
- there are no other provisions in the *Criminal Code* or any other federal law that would provide a warrant or order permitting this technique, procedure or device to be used.

If it turns out that there is authorization for the search, then one must continue to these questions:
B) if the law authorizing the search or seizure is a reasonable, constitutional law; and
C) if the manner in which the actual search or seizure was carried out is reasonable.

B) Is the law authorizing the search or seizure reasonable?

Laws that were once authority for search and seizures may themselves be found to be unreasonable over time, either through constitutional challenges or developing case law. If the law authorizing the search is itself unreasonable or unconstitutional, then the search flowing from it will be unreasonable.[546]

C) Is the manner of the search or seizure reasonable?

Just because there is good solid authority for a search or seizure does not automatically mean that a search or seizure was done reasonably. The actual conduct during the particular search must also be looked at. For example:

- Is a female police officer strip-searching a male suspect a reasonable manner of searching? It may be reasonable if an immediate strip search is necessary and there are no male police officers nearby available to help. However, it will probably be unreasonable if the delay in getting someone of the same sex as the suspect will not endanger anyone or permit evidence to be lost.
- Is using a pair of steel handcuffs to pry a person's mouth open during a mouth search a reasonable manner of searching? It may be reasonable if the suspect is snapping her jaw shut in a motion that threatens to bite the officer's finger. However, it will not be reasonable if the suspect is cooperative or showing no such signs of aggressive behavior.

[546] *R v Rao* (1984), 12 Canadian Criminal Cases (3d) 97 (ONCA); leave to appeal to SCC refused, [1984] 2 SCR ix (hereinafter *Rao*); *R v Kokesch*, [1990] 3 Supreme Court Reports 3 (SCC).

If the search or seizure process has passed **A - C**, (search authorized by good law and done in a reasonable manner) then the search is considered to be reasonable, meaning that there is no section 8 *Charter* violation and the evidence can be used in court.

However, even if the search or seizure process has not passed **A - C**, it is still possible that the evidence obtained from the illegal search and seizure might be used in court because the *Charter* may allow it to be used.

Can the evidence from an unreasonable search/seizure be used?

The *Charter of Rights* gives judges the authority to admit evidence obtained from an unreasonable search and seizure under subsection 24(2). Three factors must be taken into account in determining whether or not it would be appropriate to admit the evidence that was obtained from an unreasonable search or seizure into court. They are:[547]

1) Seriousness of the Charter-Infringing State Conduct;
2) Impact on the Charter-Protected Interests of the Accused; and
3) Society's Interest in an Adjudication on the Merits.

How these factors are considered is:[548]

Step 1—Seriousness of the Charter-Infringing State Conduct: The first inquiry requires a court to assess whether the admission of the evidence would bring the administration of justice into disrepute by sending a message to the public that the courts condone state deviation from the rule of law. This inquiry requires an evaluation of the seriousness of the state conduct that led to the breach.

This inquiry does not seek to punish the police or to deter *Charter* breaches. Even though deterrence will be a happy consequence, the main concern here is the preservation of public confidence in the rule of law and its processes.[549]The keys notes under this step are that:

---

[547] *Collins*. See also: *R v Grant*, [2009], Supreme Court Judgments Number 32, where the Supreme Court of Canada determined that despite the measure of certainty brought by the previous three exclusionary steps, the general rule of inadmissibility of all non-discoverable conscriptive evidence was inconsistent with the requirement that the court considers "all the circumstances" in determining admissibility.

[548] See *R v Grant*, 2009 SCC 32, 2009 CarswellOnt 4104.

[549] *R v Grant*, at paragraph 73.

- The court on a s. 24(2) application must consider the seriousness of the violation, or the gravity of the offending conduct by state authorities whom the rule of law requires to maintain the rights guaranteed by the *Charter*.

- The more severe or deliberate the state conduct that led to the *Charter* violation, the greater the need for the courts to dissociate themselves from that conduct, by excluding evidence linked to that conduct, in order to preserve public confidence in and ensure state adherence to the rule of law.

- State conduct which violates *Charter* rights vary in seriousness. On one end of the spectrum, admission of evidence obtained through unintentional or minor violations of the *Charter* may minimally undermine public confidence in the rule of law. On the other end of the spectrum, admitting evidence collected through intentional or reckless disregard of *Charter* rights will most likely have a negative effect on the public confidence in the rule of law, and risk bringing the administration of justice into disrepute.

Step 2—Impact on the Charter-Protected Interests of the Accused: The second inquiry focuses on the seriousness of the impact of the *Charter* breach on the protected interests of the accused. This step inquires into the extent to which the breach actually undermined the interests protected and whether the breach is fleeting, technical or profoundly intrusive.

Step 3— Society's Interest in an Adjudication on the Merits: This step consideration the reliability and importance of the evidence to the proper adjudication of the case. The question under this step is whether the truth-seeking function of the criminal trial process would be better served by admitting the evidence, or by excluding it. This inquiry is said to reflect the society's "collective interest in ensuring that those who transgress the law are brought to trial and dealt with according to the law."[550]

[550] *See also:R v Askov*, [1990] 2 S.C.R. 1199 (SCC), at pp 1219-20.

What are some overall concerns regarding police searches?

There is a concern that, in deciding whether or not evidence from an unreasonable search and seizure should be excluded, the court places far too much weight on the fact that the police could have discovered the evidence without breaching the *Charter* as a means of justifying the use of the evidence. Some argue that if the police are able to show that the evidence was discoverable without a *Charter* breach, then the breach was much more serious and should result in the automatic exclusion of the evidence.[551] Others argue one step further—if the evidence was obtained through the breach of *anyone's Charter* right, not just the *accused's*, then it should be excluded.[552] They argue that failing to look at all of the police's conduct in an investigation ignores the fundamental purposes of the *Charter* itself, which is to set up a line that the state cannot cross.[553] Ignoring breaches of the *Charter* by the police during an investigation leads to the predictable conclusion that such conduct is permissible.[554]

Another concern with police searches is the court's gradual shifting of the *Charter* protection against unreasonable search and seizure from protecting people[555] to protecting those people who have property.[556] This concern is supported by the criteria that the court uses to assess whether or not a person has a reasonable protection of privacy. For example, the following factors:

- possession or control of the property or place;
- ownership of the property or place;
- historical use of the property; and
- ability to regulate access,

point to the actual ownership of property. Applying these factors, the court has determined that a person who owns a car or is driving a car has a greater reasonable expectation of privacy than does someone who is merely a passenger.[557] There may be several unintended consequences in using these criteria to establish a reasonable expectation of privacy. For example, children who live in their

[551] D. Stuart, "Stillman: Limiting Search Incident to Arrest, Consent Searches and Refining the Section 24(2) Test" (1997) 5 Criminal Reports (5th) 99 at 108 (hereinafter Stuart).
[552] U. Hendel and P. Sankoff. "R. v. Edwards: When Two Wrongs Might Just Make A Right" (1996) 45 Criminal Reports (4th) 330 at 340 (hereinafter Hendel and Sankoff).
[553] Hendel and Sankoff, at 344.
[554] Hendel and Sankoff, at 340.
[555] *R v Edwards,* [1996] 1 Supreme Court Reports 8 (SCC) at 145 (hereinafter *Edwards*).
[556] D. J. Schwartz, "Edwards and Belnavis: Front and Rear Door Exceptions to the Right to be Secure From Unreasonable Search and Seizure" (1997) 10 Criminal Reports (5th) 100 at 102 (hereinafter Schwartz).
[557] *R v Telus Communications Co*, 2013 SCC 16, 2013 CarswellOnt 3216.

parents' home do not own the house, do not have the ability to regulate access to it and cannot claim either a superior historical use or control of the place.[558] Likewise, guests or visitors cannot establish a reasonable expectation of privacy. Homeless persons, sharing dormitory-style accommodations in a shelter, have less personal privacy than individuals who rent their own apartments, but they should have no less right to be free from warrant-less state searches and seizures.[559] Rather than applying to all equally, the present criteria appear to give more section 8 *Charter* protection to those who own property.

Can the police legally intercept my emails or text messages?

In order to obtain text messages or emails the police must be granted a judicial wiretap authorization.[560] The requirement for this special warrant offers increased protection since the authorization standards are much higher. Police must demonstrate that they have tried other investigative procedures or that other tools are likely to fail and that the urgency of the case makes other tools impractical. If a special wiretap warrant is given the interception is time-limited.

Police and Search Warrants

How are the police supposed to carry out a search warrant?

Search warrants given under a provincial Act may have specific directions on how they are to be carried out either listed in the warrant or in the specific Act under which they were issued. A search or seizure under a federal warrant must be carried out by the rules set out in the Canadian *Criminal Code*.[561] Generally, search warrants must be carried out during the day, which is 6 a.m. to 9 p.m., unless whoever issued the warrant specifically authorizes it to be carried out during the night.[562] Federal warrants may be executed on any day of the week, including Sunday or a statutory holiday. The person doing the search should identify herself as a police officer and state the reason why she is demanding entry into the place. She is not required to do this if unannounced entry is necessary to prevent the destruction of evidence. If it is practical to do so, the person carrying out the search warrant should have it with her so the owner or occupant of the place has a reasonable opportunity to examine the document.

---

[558] Schwartz, at 105.
[559] Schwartz, at 106.
[560] *R v Weir*, [1998] Alberta Judgments Number 155 (Q.B.), affirmed (2001), 156 Canadian Criminal Cases (3d) 188 (ABCA).
[561] Hoskins, at 315 – 317. *Criminal Code*, section 487.
[562] *Criminal Code*, section 488.

If the person in charge of the place refuses to allow the officer to enter to carry out her warrant, then the officer is entitled to use reasonable force to get inside.[563] If, however, the place being searched is a dwelling, then, generally speaking, the police officer is not entitled to forcibly enter unless urgent circumstances exist. The person carrying out the search warrant has no legal authority to search anyone whom she finds in a dwelling during the search. The right to search someone has only been recognized as an incident of arrest (SIA). A police officer is, however, entitled to control the premises if she has reason to believe that such a detention is a necessary part of the authorized search, like to help ensure the safety of the persons carrying out the warrant or to prevent the possible destruction of evidence.[564] If the dwelling house is not occupied at the time of the search, then the police officer who carried out the search warrant should leave a copy of it in a noticeable place inside the dwelling.

As a general rule,[565] the warrant should list the articles to be seized with sufficient description so that the police officer will know exactly what to look for and not go on what is commonly called a "fishing expedition." "Fishing" is just "snooping" or collecting things that might turn out to be useful evidence later but which are not suspected of being illegal or evidence of a crime at the moment they were seized. The person executing the warrant is not, however, limited to seizing only those articles described in the warrant. He may also seize anything that he believes on reasonable and probable grounds has been obtained by or has been used in the commission of an offence.[566] Although only the person to whom the warrant is directed is authorized to make the search and seize the named articles, there does not appear to be anything prohibiting other people, like the owners of stolen property or experts who are more qualified in identifying the articles sought, from accompanying the police officer who is doing the search.

Can someone come right into my house, arrest and search me?

Yes.[567] A police officer can get a specific arrest warrant to enter a private dwelling to carry out a lawful arrest if he persuades a judge or justice that:

---

[563] *Criminal Code*, section 25(1).
[564] *Levitz v Ryan* (1972), 9 Canadian Criminal Cases (2d) 182 (ONCA).
[565] James A. Fontana, *The Law of Search and Seizure in Canada* (Toronto: Butterworths, 1997).
[566] *Criminal Code*, section 489.
[567] Hoskins, at 307 - 308; and Department of Justice, News Release "Minister of Justice Tables Response to Feeney Case" (October 30, 1997) as per the new law.

- there are probable grounds to believe that the person who is inside the dwelling is a person for whom there is an outstanding warrant; or
- that there are reasonable and probable grounds to believe that the person has committed a criminal offence.

If there are urgent circumstances that do not make it practical to obtain an arrest warrant, a police officer can also forcibly enter a dwelling to make an arrest without a warrant to:

- prevent the commission of an offence that would cause immediate and serious injury to any person;
- prevent destruction of evidence; or
- arrest someone he is in hot/fresh pursuit of.

Depending on the urgency of the situation, it may not even be necessary for the officer to announce who she is before entering. The fact that in some circumstances police officers can make forced, unannounced, warrantless entry into a dwelling to arrest a person is very significant, because after making a lawful arrest, a peace officer is permitted to extend a SIA search to the immediate surroundings in which the arrest was made and which are under the control of the person arrested.[568] If, however, the officers arrested a person inside a dwelling house after getting a warrant to do so, they would not automatically have the power to also search the whole premises without a warrant, for when the police got an arrest warrant, they could have also gotten a search warrant.

If I stay with my friend, do I have a reasonable expectation of privacy in his place while I am there?

Probably not, but whether there exists a reasonable expectation of privacy is depends upon the situation. Past cases[569] show that some of the circumstances the court will consider in determining this are:[570]

- whether or not the person was present at the time of the search;
- if the person had possession or control of the property or place;
- if the person owned the property or place;
- the historical use of the property;

[568] *Rao*.
[569] *Edwards*.
[570] *Edwards*.

- the person's ability to regulate access, including the right to admit or exclude others from the place;
- if the person themselves thought they had an expectation of privacy; and
- if it appeared to others that the person had a reasonable expectation of privacy.

In the Canadian case that first listed these factors, the court held that even though a male had a key to his girlfriend's place, was a frequent visitor who sometimes spent the night and who kept some of his things there, he still did not have a reasonable expectation of privacy in her place. The court found that he did not contribute to the rent or household expenses except to help his girlfriend buy a couch. He had keys to the apartment, but he lacked the authority to regulate access to the premises as, anyone he wished to admit, his girlfriend could exclude and, anyone he wished to exclude, his girlfriend could admit. Overall, the court found that he was only an especially privileged guest who did not have a reasonable expectation of privacy in his girlfriend's place.

Who can see the information the police used to get a search warrant?

In order to get a search warrant, the police officer must first tell a judge or justice what information leads her to believe that she has reasonable and probable grounds to support getting a search warrant. The application for the warrant and the warrant itself may contain sensitive information that could negatively affect the person investigated under the warrant, or it may reveal any informants or surveillance techniques that provided information to get the warrant. The *Criminal Code*[571] says that there must be no newspaper publication or broadcast of the location of:

- the place that was either searched or to be searched, or
- the identity of any person who is or appears to occupy/possess/control that place, or who is suspected of being involved in any offence in relation to what the warrant was issued for without the consent of every person referred to.

This "ban," however, does not apply if a charge has been laid for any offence in relation to that for which the search warrant was issued.

[571] *Criminal Code*, section 487.2(1).

The *Criminal Code* also states that an application can be made to a judge or justice asking that they make an order "sealing" or denying access to any information relating to the warrant. This type of application must show that:[572]

1) justice would be undermined by the disclosure because:
    - it would compromise the identity of a confidential informant;
    - it would compromise the nature and extent of an ongoing investigation;
    - it would endanger a person engaged in a form of undercover work or that type of work;
    - it would prejudice the interest of an innocent person; or
    - any other sufficient reason; and

2) the importance of the reason to seal the warrant information outweighs the importance of access to this information.

If a warrant was "sealed," even the accused must show a judge how the accused's need to see it for his right to make a full answer and defense is greater than the right for which it was sealed. If the warrant file is opened, past case law suggest that, although a policy of openness is favoured, public access may be restricted if nothing was discovered in the search.[573]

If I know an arrest is wrong, should I still let the police arrest and search me anyway?[574]

Yes. Most would say that it is not advisable to interfere with a police officer carrying out her duties. If you resist any arrest, (even an arrest made of the wrong person) you may still be charged and found guilty of resisting arrest or assaulting a police officer even if the police do not follow-though on the charges on which you were originally arrested.[575] This will mean that you have a criminal record. Just because a search incident to an arrest (SIA) does not turn up anything to support the officer's suspicion for making the initial SIA, does not automatically mean that it was an illegal search. While you should not physically resist an arrest and SIA, you may, however, raise your objections to the officer and call it to the attention of any nearby witnesses. Later, you can complain to police headquarters or consult

[572] *Criminal Code*, section 487.3.
[573] *MacIntyre v Nova Scotia (Attorney General)* (1982), 65 Canadian Criminal Cases (2d) 129 (SCC) at 141.
[574] E. Shaw, J. Westwood and R. Wodell. *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How to Protect Them* (Vancouver: B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association , 1994) at 28-33 (hereinafter Shaw, Westwood and Wodell).
[575] *R v JMG* (1986), 29 Canadian Criminal Cases (3d) 455; leave to appeal to Supreme Court of Canada dismissed 59 Ontario Reports (2d) 286; 29 Canadian Criminal Cases (3d) 455 (ONCA) (hereinafter *JMG*).

a lawyer on whether the police officer's treatment of you was unreasonable or illegal, and if so, how you might proceed.

4.1.2 SEARCHES BY CUSTOMS

Canada shares a long and unprotected border with the United States. There are many points of entry. The border encourages not only legitimate commerce between the nations but also illegal activities such as the smuggling of liquor, narcotics, weapons or other contraband. Countries have the right to control both who and what enters their boundaries. To help protect her borders, Canada passed the *Customs Act*.[576] This Act gives customs officers wide powers to search persons, vehicles and goods, and also allows the taking of samples, seizures and forfeitures based on only a reasonable suspicion that a breach of the Act might be taking place.[577] The Act recognizes that persons, vehicles and goods can arrive in Canada by a variety of means and through one of many unstaffed ports of entry. Thus, persons, vehicles and goods that have not formally cleared customs can still be subject to the Act even though they are already well inside Canada.[578]

This need to protect what flows in and out of Canada greatly reduces one's "reasonable expectation of privacy" when going through customs or a border crossing. Travelers arriving in Canada or crossing international borders expect to be subject to a screening process.[579] This process usually requires the traveler to produce proper identification, travel documentation, and involves a search process beginning with the completion of a declaration of all goods being brought into the country. Searches of a person's luggage and of the person are accepted aspects of the search process where there are grounds for suspecting that a person has made a false declaration and is transporting prohibited goods.

Customs officers have extremely wide powers to search (even wider than the police). Also, both Parliament and the courts have recognized that the public interest in preventing prohibited goods from entering Canada and attaching duties to imported goods justifies searches without the usual requirement for a warrant or an arrest. Customs searches, however, must still pass the scrutiny of

[576] *Customs Act*, Revised Statutes of Canada 1985, c.1 (2nd Supp.) [Unofficial Chapter No. C-52.6] (hereinafter *Customs Act*) as discussed in Scharbach at 44.
[577] C*ustoms Act*.
[578] *R v Jacques* (1996), 95 Canadian Criminal Cases (3d) 238 (NBCA affirmed (1996), 110 Canadian Criminal Cases (3d) 1 (SCC).
[579] *R v Simmons* (1984), 11 Canadian Criminal Cases (3d) 193 (ONCA); affirmed (1988), 45 Canadian Criminal Cases (3d) 296 (SCC) (hereinafter *Simmons*).

being reasonable and done in a reasonable manner. If a customs search is found to be authorized but still unreasonable, then it must be determined if the evidence gathered in the search can be used in court using the same test as discussed above under **Police Searches.**

Are customs officers authorized to do strip searches?

Yes. The *Customs Act*[580] states that an officer may search any person who

- has arrived in Canada;
- is about to leave Canada; or
- who has had access to an area designated for use by persons about to leave Canada and who leaves the area but does not leave Canada,

if the officer suspects on reasonable grounds that the person has hidden on or about her body anything that would be evidence of a breach of the Act. The law requires that the search of a person be done in a private search room and by someone of the same sex. If there is no officer of the same sex at the place at which the search is to take place, an officer may authorize any "suitable" person of the same sex to perform the search.[581] Before you submit to a Customs search of your person, you can ask to be taken before a senior officer at the place where the search is to take place. If the senior officer sees no reasonable grounds for searching you, you will not be searched.

While the *Customs Act* itself does not specify the extent of the personal search, past court cases have shown that there are multiple types of border searches:

1) routine questioning which every traveler undergoes at a port of entry, accompanied in some cases by a search of baggage and perhaps a pat down or frisk search of outer clothing;
2) the strip or skin search;
3) cellphone, table, and laptop searches;
4) full body scan; and
5) a body cavity search in which customs officers have access to medical doctors, x-rays and other highly invasive means.

[580] *Customs Act*, section 98.
[581] *Customs Act*, section 98(4). Compare with section 104 of the Act.

The *Customs Act* makes it an offence to obstruct or resist any authorized personal search, but before a strip, skin or body cavity search you are considered detained for the purpose of your *Charter* rights and must be informed of your right to get a lawyer.[582]

Are customs officers authorized to open my out of country mail?

The *Customs Act*[583] states that an officer may examine any mail that has been imported, and open or cause to be opened any such mail that she suspects on reasonable grounds may contain any goods that may be in breach of the Act. She may also take a reasonably sized sample of anything contained in the mail.[584] However, to open imported mail that weighs thirty grams or less (letters), the custom's officer must either have the consent of the person to whom the letter is addressed, or the person who sent it must have signed and attached a postal label giving authorization to open it.

4.1.3 SEARCHES IN PRISONS

Is an inmate entitled to access section 8 Charter protection: that is, be free from unreasonable search or seizure?

In theory, yes. The Supreme Court of Canada has determined that a person confined in a prison retains all of his civil rights other than those expressly or impliedly taken away by law.[585] In practice, however, an inmate attempting to use the *Charter's* protection against unreasonable search and seizure is faced with the difficulty of first showing that he had a reasonable expectation of privacy. The Supreme Court of Canada notes that there is a substantially reduced level of privacy in prisons as occupants of prison cells expect to be exposed and observed. Therefore, a prisoner cannot hold a reasonable expectation of privacy with respect to practices such as frisk searches, routine head counts and random, unannounced surveillance patrols known as "winds."[586]

The three most common types of searches in prisons are:

- **Frisk Searches:** which is a hand search of a clothed inmate from head to foot, down the front and rear of the body, around the legs and inside clothing folds, pockets and footwear and

[582] *Greffe v R* (1988), 41 Canadian Criminal Cases (3d) 257; reversed in (1990), 55 Canadian Criminal Cases (3d) 161 (SCC).
[583] *Customs Act*.
[584] *Customs Act*, section 99(b).
[585] *Canada v Solosky*, [1980] 1 Supreme Court Reports 821 at 839 (SCC).
[586] *Weatherall v Canada (Attorney General),* [1988] 1 Federal Court Reports 369 (Fed. T.D.); varied [1989] 1 Federal Court Reports 18 (Fed CA); reversed [1991] 1 Federal Court Reports 85 (Fed. C.A.); affirmed [1993] 2 Supreme Court Reports 872 (SCC) (hereinafter *Weatherall)*.

can include searching by use of hand-held scanning devices. Touching of the genital area, although not specifically precluded, is avoided.

- **"Counts":** which are regularly scheduled cell patrols. The guard announces the beginning of the count at the top of the particular range to be counted to let inmates know that the count is starting and then walks down the range looking into each cell for two to three seconds in order to ensure that the inmate is accounted for and is alive and well.
- **"Winds":** which are unannounced patrols conducted at random times each hour. "Winds" help verify that inmates are not engaged in any activities detrimental to the good order and security of the institution.

Is being searched by a member of the opposite sex while in prison reasonable?

In 1993, the Supreme Court of Canada had the opportunity to specifically review whether the three types of searches done by female guards on male inmates were unreasonable searches for the purpose of section 8 of the *Charter*.[587] The court found that all of these types of searches are necessary in a prison for the security of the institution, the public and the prisoners themselves, and that inmates cannot hold a reasonable expectation of privacy with respect to these types of searches. Any possible inappropriate effects of these practices are minimized by providing guards with special training to ensure the searches are professionally executed with due regard for the dignity of the inmate. The court did comment, however, that it is unreasonable for male guards to do these types of searches on female inmates.

Is it not unfair that female guards can search male inmates, but male guards cannot search female inmates?

Female inmates represent only a small minority of the total federal prison population. Thus, for women to have significant opportunities for employment as custodial staff in federal prisons it was considered necessary that women be able to work on an essentially equal basis with men in prisons for males.[588] Such affirmative action programs, where to establish equality sometimes requires that people be treated unequally, may be called for in certain cases to promote equality and are in accordance with the *Charter*.[589]

The Supreme Court of Canada also noted that, biologically, a frisk search or surveillance of a male's chest by a female guard does not raise the same concerns as the same practice conducted by a male

[587] *Weatherall*.
[588] *Weatherall*.
[589] *Weatherall*.

guard on a female inmate. Moreover, the court recognized that women generally occupy a disadvantaged position in relation to men. Viewed from this perspective, it becomes clear that the effect of cross-gender searches are different and more threatening when done on women than on men.

4.1.4 SEARCHES OF STUDENTS IN SCHOOL

Why is searching school students a special issue?

In Alberta, children between the ages of 6 and 16 must go to school. They can go to a public school, a separate school, a private school, a charter school or they may be schooled at home. Every child who:

- is at least 6 years old at September 1st, but younger than 19 years of age, and
- is a Canadian citizen, a permanent resident, the child of a Canadian citizen or the child of a permanent or temporary resident

has the right to access an education program.[590]

Under the *School Act*, children must attend school up to the age of 16. [591] Children who are under 6 years old may be admitted to a pre-grade one program, which is called kindergarten or Early Childhood Services.

The *School Act* is one of the Acts that contain laws regarding schools, students, teachers and the rules for attending school.[592] Many people are concerned with behavioural problems in school, such as drug use, theft, harassment, vandalism and violent crimes against other students and teachers. Others are alarmed by news items indicating that around inner-city schools, "Johns" (people who are trying to obtain the services of prostitutes), prostitutes and impaired people often bother students who are on their way to school.[593] At one time students felt safe once they got into a school building, but that is not always the case now. Two high school students in Edmonton had this to say about their school: "I don't feel safe at all, you look at some kids the wrong way and they'll say, 'I'll kill you'." "Too

[590] Alberta Civil Liberties Research Centre. *Rights and Responsibilities in Canada: Navigating Through Alberta's Schools* (Calgary: Alberta Civil Liberties Research Centre, 1996) at 1 – 12 (hereinafter *Rights and Responsibilities*).
[591] *School Act*, Revised Statutes of Alberta 2000, chapter S-3, subsection 13(1)(c) (hereinafter *School Act*).
[592] *School Act*, section 13.
[593] V. Hall, "Schoolgirls Learning to Fight Back: McCauley Jr. High Students Dodge Johns, Drunks." *Edmonton Journal* (28 November 1998) 4.

many kids these days try to impress their peers by carrying or displaying weapons."[594] Parents have an obvious interest in teaching their children how to act in dangerous situations or avoid them altogether, but just what responsibility do they and school officials have when it comes to maintaining order on school property, and what powers do they have to meet these responsibilities?

At the beginning of the *School Act* it states that parents have a right and a responsibility to make decisions about the education of their children.[595] It also states that the best educational interests of the students are the most important consideration when using any authority under the Act. Under the Act teachers have a duty to:

- competently provide instruction to students;
- teach approved courses;
- promote goals and standards of providing education;
- encourage and foster learning in students;
- regularly evaluate students and report the results;
- maintain order and discipline in the school and on the school grounds while attending school and school activities; and
- carry out other duties assigned to them in their employment contracts.[596]

Under the Act a principal also has many duties. Some of the principal's duties are to:

- provide instructional leadership in the school;
- Provide a welcoming, caring, respectful, and safe learning environment;
- direct the management of the school;
- ensure the students have the opportunity to meet the standards of education set by the Minister;
- maintain order and discipline in the school, on the school grounds and during activities sponsored / approved by the school board; and
- any other duties assigned by the school board.[597]

[594] J. Farrell, "Most Students Back Weapon-Searches" *Edmonton Journal* (28 November 1998) 4.
[595] *School Act*, Preamble.
[596] *School Act*, section 18.
[597] *School Act*, section 20.

Does the School Act *give school officials the authority to search students?*

The Act does not expressly say that school officials can search students. But the power to do so, and do so quickly, appears to be a necessarily incidental part of their responsibility to keep drugs, weapons and other harmful substances out of the school environment.[598] Thus, on the one hand, school officials have a duty to teach students. This includes teaching them about the constitutional rights that members of society have. On the other hand, school officials must also be able to react quickly when faced with a threat to the school environment or the safety of students. This may mean that under certain circumstances some of the students' constitutional rights may appear to be violated by the very same people who are supposed to be fostering in the students a respect for such rights.[599]

Why would schools need to be able to search students or their lockers?

At the beginning of each school year, schools usually publish something like a student handbook, which includes information on such things as what is considered appropriate behavior and dress in the school and the rules in the school that one could be punished for breaking. Although the rules vary from school to school, the types of behaviors that are usually disciplined include:

- refusing to follow the school rules;
- poor attendance;
- use of profane language;
- a pattern of neglecting school assignments or other duties;
- intentionally destroying school or personal property;
- pushing, shoving or other aggressive behavior; or
- other gross misconduct, such as fighting, carrying a weapon, drug or alcohol use or sexual misconduct. [600]

The types of discipline used by schools also varies. Some of the main forms of discipline include detentions, removal of privileges, removal from the classroom for one class period, administrative student transfers, suspension from school, withdrawal from the school, and expulsion from the school. In many minor offences, a principal has discretion to either deal with the matter himself or consult with the child's parents. In some cases the crime might be so serious that the police must be contacted.

---

[598] S. Bindman, "Privacy rights weighed against school discipline" *Calgary Herald* (25 June 1998) 10 (hereinafter Bindman).
[599] G. Dickson, Q.C. "Students and the Charter" (April/May, 1999) LawNow 42 (hereinafter Dickson).
[600] *Rights and Responsibilities in Canada* at 15 – 22.

But the principal cannot exercise this discretion until he knows the nature and extent of the offence. To help confirm that a student suspected of breaking a school rule has in fact done so, school officials may first need to find proof of the breach to determine the appropriate level of punishment.

What is the general law around school searches?

The provincial Act governing schools in Nova Scotia is very similar to the provincial *School Act* governing schools in Alberta. In reviewing a search done in a Nova Scotia school[601] the Supreme Court of Canada said that although there is no express authority for physically searching students under the Nova Scotia Act, the power to do so could be inferred from the broad responsibilities school officials are given, such as maintaining proper order and discipline and administering and supervising the educational program of the school. The court also went on to say that, because public schools are a part of government, they too have to comply with the *Charter*,[602] and one of the *Charter*'s guarantees is that one is to be free from unreasonable search and seizures.[603] As discussed earlier in **Searches by the Police**, the court had already established the general search rule that searches without search warrants are unreasonable.[604] However, in this school search case, the court recognized that the relationship between a principal and student is not the same as the relationship between a police officer and an accused citizen. While the police and the accused citizen are adversaries, a principal has an interest not only in the welfare of the other students but in the accused student as well. The court also recognized that students are compelled to attend school where order must be maintained to protect the student body, and that this lowers a student's "reasonable expectation of privacy" while in a school. Because of this different and special relationship between school officials and students, the students' lowered expectation of privacy, and the need for someone to act swiftly to ensure the safety of a high concentration of students compelled to attend school, the court felt it was necessary to develop some school-specific tests or guidelines in determining what is a reasonable search in a school environment.

---

[601] *R v M (MR).,* [1998] 3 Supreme Court Reports 393 (SCC) (hereinafter *MRM*).
[602] *Charter*.
[603] *Charter*, section 8.
[604] *R v Hunter*, (1987), 34 Canadian Criminal Cases (3d) 14 (ONCA).

What will be considered a reasonable search in a school?

Often a Canadian court's review of school search cases[605] starts with the application of a two-step test borrowed from an American student search case.[606]

1. One must first consider whether the search was justified from the beginning. Under ordinary circumstances, a school official will be justified in starting a search when there are **reasonable grounds** for suspecting that a search will turn up evidence that the student has broken or is breaking either the specific rules of the school or the general law.
2. Second, one must determine whether the scope or extent of the actual search conducted was reasonable in relation to the circumstances which prompted and justified the search in the first place. When the search method used is reasonably related to the objective of the search and not too intrusive for the age and sex of the student nor the nature of the infraction, the extent of the search will be found to be reasonable.

In addition to the above test, the Supreme Court of Canada set out four rules when it comes to student searches in a school.[607] They are:[608]

1. It is not necessary for a school official to have a warrant before searching a student.
2. The school official must have **reasonable grounds** to believe that there has been a breach of school regulations and that a search of a student would reveal evidence of the breach. The information to create a school official's reasonable grounds may come from such sources as a teacher's or principal's own observations, one credible student or from more than one student.
3. Courts should recognize that school officials are in the best position to weigh the significance of the information given to them about the existing situation in their particular school, such as how credible a source of information is and how serious the suspected conduct is.
4. Factors that should be considered in determining whether a particular search by a school official in a school was reasonable include that:
    a) there should be some authority for the search in written laws;

---

[605] Such as *R v J.M.G.*

[606] *New Jersey v TLO*, 469 US 325, 105 S. Ct. 733, 1985 U.S. LEXIS 41 (1985) as discussed in E. Alderman and C. Kennedy*, The Right to Privacy* (New York: Alfred A. Knopp, 1995) (hereinafter Alderman and Kennedy).

[607] *MRM.*

[608] G. M. Dickinson, "Supreme Court Ruling Has Implications for School Locker Searches" (1995-96) 7 Education & Law Journal 281 (hereinafter Dickinson).

b) the search must be conducted in a sensitive manner and be minimally intrusive; and
c) all of the circumstances surrounding the search be considered.

Have there been any Canadian cases dealing with school searches?

Although there have been many cases in the United States that have dealt with school authorities searching lockers, there is very little Canadian case authority on this topic.[609] Generally, however, the courts have determined that locker searches have been minimally intrusive in cases where the school officials have had a reasonable belief that illegal drugs or weapons may be found in them.[610] Notwithstanding that there are locks on school lockers, it appears that students still have a lowered reasonable expectation of privacy in what they put or have in them.[611] A Supreme Court of Canada decision found that the contents of a student's backpack, which the student had left in the gymnasium, was specific and meaningful information intended to be private and thus the student had an expectation of privacy.[612] A suspicion that a student may be concealing drugs or weapon on his body may be more likely to warrant a strip-search.[613] Overall, it appears that the courts will give school officials considerable latitude to enforce school safety policies in Alberta schools.[614] There may however be a problem, where no grounds of reasonable suspicion existed for a search or where the search was carried out in an unreasonable manner.

What rights do students have if they are being searched?

As already mentioned, schools must comply with the *Charter*. One of the *Charter*'s guarantees is that a person who is being detained or arrested has the right to be promptly informed of the reason why he is being detained.[615] The *Charter* also guarantees that, within a reasonable time,[616] this person be informed of his right to have a lawyer,[617] and also be provided with a reasonable opportunity to access a lawyer. Since a student is compelled to be in school and can usually be disciplined for disrespecting a school official or her orders, it is easy to understand that a student would not see herself as being free to leave when being questioned by a school official in her office or while being searched for

[609] Dickson
[610] Shaw, Westwood and Wodell.
[611] A. Wayne Mackay, "Don't Mind Me, I'm from the R.C.M.P.: R. *v* M.(M.R.) - Another Brick in the Wall Between Students and Their Rights" (1997) 7(5) Criminal Reports 24 (hereinafter Mackay).
[612] *R v M (A),* 2008 SCC 19.
[613] Dickson.
[614] Dickson.
[615] *Charter*, section 10(a).
[616] *Feeney*.
[617] *Charter*, section 10(b).

illegal drugs.[618] One would expect, therefore, that a student so detained must be informed of her right to get a lawyer and be given an opportunity to act on this *Charter* guarantee.

In reviewing a case where a principal searched a student,[619] the Ontario Court of Appeal said that one's *Charter* right to get a lawyer must be interpreted in a way that is consistent with why it was included in the *Charter*. The court went on to say that the purpose of this right was to enable an accused person to get advice on what his rights are in certain circumstances and to get help in exercising those rights. This purpose did not extend to situations such as physical searches for narcotics because the suspect is ultimately obliged to submit; no amount of legal advice or assistance from a lawyer will deter this type of search.[620] The court also said that the circumstances surrounding a student search do not amount to a detention within the meaning of the *Charter* as a student is already under a kind of detention though his compulsory attendance at school. In school, a student is subject to the discipline of the school and is required to undergo any reasonable investigative procedure, and the court determined that a search is an extension of this. The court was willing to admit that there may come a time when significant legal consequences are inevitable and school officials become agents of the police in detecting crimes. While in these situations the school officials would have to follow the police standards that are higher, this is not automatically the case at the start of every school official's search of a student.

What are some criticisms of the current law on school searches?

The Supreme Court of Canada noted that an individual's "reasonable expectation of privacy" will vary according to the context or situation in which that person is.[621] In determining what is a reasonable expectation in each situation, all of the surrounding circumstances must be considered, including:[622]

- who exercises possession or control over the property or place to be searched;
- who owns the property to be searched;
- the historical use of the property or place to be searched;
- the ability to regulate access to the property or place; (including the right to admit or exclude others)

[618] Mackay at 31.
[619] *J.M.G.*
[620] *J.M.G.*
[621] *R v Hunter,* (1987), 34 Canadian Criminal Cases (3d) 14 (ONCA).
[622] *Edwards*.

- the subjective expectation of one's privacy; and
- the objective reasonableness of the expectation of privacy.

A student who brings his own lock to school and puts it on his locker has expressed the desire to exclude others from his locker. Even if the school provides locks on students' lockers, the purpose of a locker is to store and secure your personal items or items in your care so that others cannot have access to them. Both of these situations suggest that the student using the locker believes he has a reasonable expectation of privacy or the locker would be nothing more than just another open shelf in the school. A student's schoolbook bag, gym bag, purse or pocket are items controlled, and often owned, by the student who has brought them into the school. None of these items are routinely searched in a school, so the students also have a historical sense of a reasonable expectation of privacy in these things while at school. Also, a personal search of a student's body is in direct conflict with the school's role of helping to foster self-esteem in children so they have a sense of control and expectation of respect for themselves not only by themselves but from others. The fact that students are required to attend school should not also mean that they have no more expectation of privacy than that of a prison inmate or be treated as second-class citizens.[623]

Lower Standard for Searches and the Dual Role of School Administrators

As already shown, school officials can search students without a warrant if they have only as little as a "reasonable suspicion" that the search will turn up evidence of a violation of a school rule or the law. This is a much lower standard than police officers must have to legally search someone without a warrant.[624] This lower standard may be appropriate in situations where the school official is doing a search to enforce "in-house" school rules and keeping order within the school. However, it becomes quite another matter when the student's actions can also lead to criminal charges.[625] While school officials should not necessarily have to read students their rights every time they detain them, there is a difference between enforcing "in-house" school rules and enforcing the criminal law.[626] It is impossible to see how a school official who is enforcing an "in-house" school rule but also dealing with a breach of the criminal law can be anything other than an agent of the police.[627] However, even in cases where a police officer has been present during a principal's search of a student, the Supreme

[623] Dickinson, at 287.
[624] Bindman.
[625] Mackay at 25.
[626] Mackay at 31.
[627] Mackay at 29.

Court of Canada has determined that this does not necessarily make the principal an agent of the police.[628] Yet, how can one ignore not only the intimidating presence of a police officer at a student search, but also the police officer's inter-relationship with the principal at that moment, even if the police officer is not actually directing the search?[629]

While some courts recognize the dual legal role of school officials[630] it is not easy to decide how or when the shift from educator to police agent occurs. It seems to be largely dependent on the principal's intentions going into the search. Perhaps under so-called "zero tolerance" school board policies, a school official would be moving closer to being a police agent.[631] When that "special" school official--student relationship becomes confused by the shifting of the school official's roles, without an appropriate corresponding adjustment in the school official's procedures, a student's *Charter* rights are often set aside.[632]

Being Detained Inside a School

Students must attend school. Requiring that youth get an education is good for the student and for society as a whole. However, this positive aspect to compulsory school attendance also has the effect of reducing a student's reasonable expectation of privacy in general and especially during questioning or searches. Ultimately, a substantially lower standard is created when initiating a search, and students are not given a right to counsel even if criminal charges could be laid. These are some of the reasons why some say it appears that a student could virtually never be legally detained in a school,[633] and that this is an inappropriate way to view and treat growing children and young adults.

School officials have the difficult and important job of educating our children and keeping them safe at school. The searches school officials do may not only be justified but may be required in order that they fulfill their statutory responsibilities to provide a learning environment.[634] To help them fulfill this "positive statutory duty" school officials have been given a more flexible standard to initiate a

[628] *M.R.M.*
[629] Mackay at 28.
[630] *J.M.G.*
[631] Greg M. Dickinson, "Principals and Criminal Investigations of Students: Recent Developments" (1989) 14 Canadian Journal of Education 203 at 216-217, in Dickinson, at 285.
[632] Mackay at 25.
[633] Mackay at 31.
[634] *M.R.M.*

search.[635] However, a clear distinction must be made between a school official enforcing in-house school rules and a school official enforcing the criminal law. The sensationalism of a search taking place in a school somehow deflects attention away from what should be the main focus: the rights of a student accused of violating a criminal law.[636] Regardless of who is doing the search, a student's *Charter* rights ought to be called into play in circumstances where the student could face a criminal charge or penalty.[637] It is cause for concern when a school official's position of trust can be used to support searching students more easily for things that may turn out to be the basis for a criminal charge against the student.

Can a teacher or principal search suspicious persons who are on school property even if they are not students?

In 1987 the Nova Scotia Court of Appeal had to review such an incident.[638] Two men who were not students were found in one of the high school's washrooms. When questioned by the principal, they told him they were looking for a jacket that one of the students had. The student, however, denied having the jacket and wanted nothing to do with either of these two men. At this point the police were called in and they asked the men to empty their pockets. One of the men looked very nervous so the police officer checked his pockets and found two pieces of hashish, which the police seized. Because the police handled this search, their actions were reviewed in accordance to the higher standards that the police are required to use. Although the police's search was premature (it had been made based on "suspicion" not on "reasonable and probable grounds"), there was not a good enough argument made to show that using the evidence from the search would have brought the administration of justice into more disrepute than if the evidence was not used. The evidence, therefore, was not excluded and was used to help convict the man who had it.

Although the issue has not been directly addressed by the courts, one could argue that school officials do not have the same special relationship with non-students visiting a school as the court says they have with school students. If this is the case, then it would follow that a school official's lower standard for initiating a search would not apply to non-students. On the other hand, however, if the courts will give greater weight to the importance of the school official's duty to keep the school environment safe for the students who are compelled to be there, the court may find that it is

[635] Mackay at 32.
[636] Mackay at 32.
[637] Mackay at 32.
[638] *R v Bent* (1987), 79 Nova Scotia Reports (2d) 169 (NSCA).

reasonable that a school official be allowed to keep control of the school and be allowed to also conduct searches on non-students visiting school grounds based on her suspicions. Since the police have much training, experience and equipment for dealing with these matters and what might follow, the local police are contacted for advice before proceeding in a situation involving non-students or are contacted in advance to establish a policy of when to alert the local authorities of such suspicious activities taking place on school grounds.

Under what standards does our school liaison police officer operate when on the school campus?

In 1995, the Nova Scotia Youth Court reviewed a student search made by a police officer who, as part of a liaison program between the police and the school, was in the high school.[639] In this case, the principal had been informed by two students that they had seen a student (A.B.S.) hand 10 dollars to and receive a package from another student who they believed was a drug dealer. The principal gave this information to the police officer at the school. The police officer recognized A.B.S.'s name and believed him to be a person who used drugs and was suspected of drug trafficking. Since A.B.S. saw the police officer talking with the principal, the police officer feared the student would dispose of the drugs and so had A.B.S. immediately brought to the school office where the police officer told him he was going to search him for narcotics. When the officer found four small packages of marijuana on A.B.S, the officer arrested him and read him his *Charter* rights.

In reviewing this case the court found that, overall, the search was reasonable. The court said that the police officer had to meet the standard set out in the (then) *Narcotic Control Act*[640] since that was the authority he was using to make the search. Having information from two eye-witnesses and his suspicions that A.B.S. was involved in drug-dealing activity gave the officer the "reasonable and probable" grounds that he needed to meet this Act's standard. The court suggested that the officer also could have first took both the seller and the buyer into custody, interviewed the two eye witnesses himself, and then made any searches he felt were justified. As the officer's presence on campus was routine, the court did not see the pressing urgency of the search, but nonetheless still found it was reasonable. The court found that the police officer should have informed A.B.S. about his right to get a lawyer immediately when he was detained rather than after he was searched. However, in this

[639] *R v ABS,* [1995] NSJ No. 535 (QL) (NS Yth Ct)
[640] *Narcotic Control Act*, Revised Statutes of Canada 1985, c. N-1, Repealed: Statutes of Canada. 1996, c19, s 94, effective May 14, 1997 (SI/97-47).

particular case the court found that the breach was minor and that the officer believed in good faith that telling A.B.S. about the right was not necessary until after the search. The breach was not serious enough that the marijuana found during the search would be excluded from court. If other courts follow similar reasoning that was used in this case, then it appears that, even though a police officer may be a routine part of a program on a school campus, because they get their authority from Acts other than the *School Act*, they have to meet the search and right to counsel standards set for police authorities and not the lower ones that school officials can use.

4.1.5 SEARCHES UNDER ADMINISTRATIVE AUTHORITY

Does an inspector reviewing my place or papers have to have a search warrant?

Probably not. The courts and society recognize a difference between:

- searches made for the purposes of **criminal investigations**, and
- searches made for **regulatory purposes**, such as inspections and auditing.

Serious legal consequences and stigma can flow from searches made for criminal investigations. A warrant is usually required for these types of criminal offence investigation searches to help protect the innocent from the police's possible overzealous or reckless use of their search and seizure powers. Searches made for regulatory purposes, however, are usually conducted in highly regulated areas (such as restaurants, land developments and employment) and those involved in these industries know that they are subject to inspection to ensure they are complying with public health, safety or other regulations. Knowing the regulatory scheme they must meet, such businesses' reasonable expectation of privacy is low. Due to the important purpose of regulatory legislation, the need for powers of inspection, and the lower expectations of privacy,[641] it is likely reasonable that many highly regulated industries should expect to be checked unannounced and possibly without a warrant.

Some of the officials who have administrative search and inspection powers under various federal and provincial laws and municipal by-laws are:

- health inspectors;
- fire marshals;

[641] *143471 Canada Inc. et al v Minister of Revenue of Quebec*, [1994] Quebec Judgments No. 410 (QL) (QBCA) 90 Canadian Criminal Cases (3d) 1 (SCC).

- Employment Standards Branch officials;
- municipal by-law officers; and
- fish and wildlife officers.[642]

Each specific Act or set of Regulations under which these regulatory officials are appointed will list the requirements or on what cause (warrant or just their reasonable suspicion) they can conduct a search or inspection. The Supreme Court of Canada notes that the powers of inspection presuppose a visit to the premises and the inspector does not need to have a warrant; be acting on a complaint nor need the inspection to be based on reasonable and probable grounds that there is a breach. [643] The Court also recognizes the need to allow searches and seizures for regulatory purposes to occur on a routine or random basis without even a requirement that there be reasonable grounds for believing there has been non-compliance.[644] In most circumstances, a person does not have the right to deny these types of officials entry. If they are refused entry, the officials can contact the police for assistance who may have the power to enforce the entry.[645]

Who do I complain to about what I feel is an improperly done inspection?

If you have a concern about an inspection by a municipal (city) official, you should contact the City Clerk's office. If you have a concern about an inspection by a provincial official, contact the Ombudsman of Alberta. If your concern relates to an inspection by someone acting under a federal law, you could contact your Member of Parliament's constituency office, or the nearest office of the federal department or agency responsible for administering that area of law.

4.2 PRIVATE SECTOR SEARCHES

4.2.1 Security Guards and Private Agencies

Does the **Charter** *apply to searches by security guards?*

As already discussed, the fundamental things to be determined when looking to the *Charter* for help to exclude evidence that was gathered in an unreasonable search or seizure are:

FIRST: that a search or seizure involving government action occurred,

[642] Shaw, Westwood and Wodell at 67.
[643] *Potash Comite Paritaire de l'Industrie de lat Chemise et al. v Selection Milton* (1992), 75 Canadian Criminal Cases (3d) 367 (QBCA) reversed [1994] 2 Supreme Court Reports 406 (SCC) (hereinafter *Potash*).
[644] *Potash.*
[645] Shaw, Westwood and Wodell at 68.

SECOND: that the search or seizure was unreasonable, and
THIRD: that the evidence turned up in the search or seizure should not be used in court.

Since it is fundamental to first establish that the *Charter* applies by showing that the person gathering the evidence was acting as an agent of the state or performing a government function, purely private investigations are often not subject to *Charter* review.[646]

Usually, certain *Charter* rights are prompted (**told to the person; the person is informed of them**) when someone is arrested or detained.[647] However, the courts have determined that private citizens or private, non-governmental security officers do not make "detentions" within the meaning of the *Charter* even though these same actions done by the police or other state or government agent would be a detention. If a person is not detained within the meaning of the *Charter*, then he does not have to be informed of his right to silence and right to get a lawyer. Any statement he makes does not violate the *Charter* and generally can be used in court.

What if a security guard makes a citizen's arrest and wants to do a search incident to that arrest?

The authority for someone to make a citizen's arrest comes from either governmental legislation like the *Criminal Code* or the common law.[648] The courts have determined that the arrest of a citizen is a governmental function whether the person making the arrest is a peace officer or a private citizen or whether the officer is acting under specific legislation or the common law. Citizen's arrests and any associated searches must, therefore, comply with the *Charter*. Although a private security officer does not derive her authority to arrest a person from the same citizen's arrest powers as a private citizen does, she gets her powers from a section of the *Criminal Code* that states that anyone who is a person authorized by the owner or someone in lawful possession of property can arrest someone without warrant if that person is found committing a criminal offence on or in relation to that property.[649] Thus, while the *Charter* does not apply to purely private actions, it does apply to actions taken under the laws made by Parliament, and if a security officer's or citizen's power to arrest comes from a part of the *Criminal Code,* their actions are governed by the *Charter*.

---

[646] T. Scharbach, "Private Law Enforcement - Dodging the Charter" (1995) 1 Appeal: Review of Current Law and Law Reform 42 at 42 (hereinafter Scharbach).
[647] *R v Shafie* (1989), 47 Canadian Criminal Cases (3d) 27 (Ont. C.A.) (hereinafter *Shafie*).
[648] *R. v Lerke* (1984), 13 Canadian Criminal Cases (3d) 515, affirmed (1986), 24 Canadian Criminal Cases (3d) 129 (ABCA) (hereinafter *Lerke*).
[649] *Criminal Code*, section 494(2).

Police officers, private security officers and even citizens all have the right to do a search incident to an arrest ("SIA") when arresting someone, provided that it is a reasonable search. While a citizen's right to search a person he arrested can be essential and reasonable to disarm the person arrested, a search to seize or preserve property connected to the offence is another matter. In reviewing a citizen's SIA for evidence the courts have found that:

> 1) there has to be a strong connection between the search for evidence and the offence for which the person is being arrested. For example, there is no connection between arresting a person for trespassing and then doing a SIA for drugs in their pockets; and
>
> 2) because it is expected that the offender will be turned over to persons in authority without delay, it is rare that the citizen making the arrest will need to search for evidence. For example, if you have apprehended someone you know the police are also chasing and they are only minutes away it would not be reasonable to search the arrested person for evidence.

The court recognizes that just as with a police officer's SIA, a citizen's right to do a SIA is not automatic. Everyone who is arrested does not have to be submitted to the degradation of a search. The courts, however, recognize that a citizen may have a greater need of a right to search than does the police officer. Citizen's arrests frequently occur when the police are neither present nor available. Often, they result from a chase or circumstances where violent reactions can be expected. The citizen has no side-arm, uniform, badge or other signs of authority which help a police officer to avoid violence. The right to search during a citizen's arrest, or at least to disarm the person being arrested, has been found to be essential. If the extent of the search is found to be unreasonable, then the evidence from the search must be reviewed to determine whether or not it should be excluded from being used in court. The test for determining whether or not evidence collected during a *Charter* violation is the same in these situations as was discussed in the previous section **Searches by the police**.

Can evidence from an unreasonable search/seizure by a private citizen be used?

In reviewing searches by a private citizen, other than SIA's,[650] the courts have declared that generally the *Charter* does not apply. However, if the search by the private individual was done for the purpose of discovering evidence in order to press charges or was being carried out with police or other government agencies initiation or involvement, the private search would then be converted into a government act and subject to *Charter* scrutiny (remember that the *Charter* applies to public or state agents not to private individuals).[651] But when private security personnel simply start their own criminal investigation, the court has determined that they are not state agents.[652] What must exist in order for the court to find that private agents were working with the police is hard to imagine, since in one case where the police were called in and accompanied the security personnel in a warrantless search, it was determined that the private and state security guards were not working together.[653] Since the *Charter* does not apply to the evidence turned up in these searches by private actors, the evidence can be used in court, even in a criminal prosecution, without the accused person having access to the test that determines if evidence collected through the violation of a *Charter* right should be excluded.

Do private detectives and security officers have the same powers as police officers?

No. Private detectives or private security personnel have no more authority to question you or to search you or your bags than an ordinary citizen.[654] If a private agent wants to search you without arresting you, you can refuse. If you refuse and are searched anyway you can bring the matter to the police's attention for possible criminal charges. If you do not refuse, however, you may be found to have consented to the search.

If it means that more criminals will be caught, why should we be concerned that private security individuals are not held up to the same standard as the police?

The courts have determined that, when a private person merely detains or searches another on her own initiative, the detainee or searched person is not protected by the *Charter*.[655] Many argue that a detention, which ultimately leads to an arrest, or any search in a criminal investigation, is as much a

[650] Scharbach, at 44.
[651] *R v Meyers*, (1987) 52 Alta. L.R. (2d) 156 (ABQB) as discussed in Scharbach at 44.
[652] *R v Fitch* (1994), 93 Canadian Criminal Cases (3d) 185 (BCCA) (hereinafter *Fitch*) as discussed in Scharbach at 44.
[653] *Fitch*, as discussed in Scharbach at 44.
[654] Shaw, Westwood and Wodell at 66.
[655] Scharbach 45.

government action as the making of a citizen's arrest or the police carrying out a criminal investigation. It is of concern that whether or not the *Charter* applies is based upon the initial purpose of the search or detention or who exactly does the search, rather than the ultimate use of the evidence or the arrest of the person.

Closing our eyes to the means (intrusions by private individuals rather than state agents) because we may agree with the ends (catching more criminals) means we only want protection from the intrusion of the government and not by private individuals as well. Allowing this private intrusion to go unchecked has the potential to create two separate systems of law enforcement within Canada:

> 1) a public system which is regulated by the *Charter* in which violations of rights may be remedied by excluding the evidence; and
>
> 2) a private system which is not regulated by the *Charter* and in which there is no possibility of having evidence excluded even if it was gathered through *Charter* violations for the express purpose of providing the police with evidence for use in a criminal prosecution. Such an unregulated, private system of enforcement would leave us vulnerable to precisely those abuses that the *Charter* is designed to prevent, including unreasonable search or seizures.

4.2.2 Searches by Employers

Why would employees commit serious theft from their employers (bite the hand that feeds them)?

Employees who commit serious crimes against their employers, like theft or fraud, can be influenced by three factors:

1. **Opportunity:** employees sometimes see a very tempting opportunity to get a benefit from very little effort—such as taking advantage of an accounting error or side-stepping the normal internal controls that prevent or detect thefts.
2. **Motivation:** the motivation for theft or fraudulent behavior is usually based on need, greed or ego. A disgruntled employee is more likely to commit crimes against her employer than a satisfied one. Other pressures like a spouse's loss of a job, stock market losses, or additional expenses like a substance dependency or a significantly increased health care cost may also provide the motivation for an employee to commit a crime against her employer.
3. **Rationalization:** the easier it is for an employee to rationalize his inappropriate behavior *("Everybody's doing it," "The Company can afford it,"* "*No one is being hurt*," *or "I'm*

just borrowing the money"), the more likely it is that he will act against his employer to benefit himself.[656]

Can an employer search an employee?

When reviewing whether or not an employer can search an employee, decision makers draw a distinction between:

- searches of an employee's **person and their personal effects**, (which are seen as an outward extension of the employee), and
- searches of **company property** that an employee may have access to or the use of, like an employee's locker.

In either type of search, the court reviewing it will look at two things:

- **First**: whether the employer had the **right to conduct a search**, and
- **Second**: if the search was conducted **in a reasonable manner** or if there was a less intrusive measure open to the employer by which it could have also protected its interests.

The general rule is that an employer has no right to search his employee's **person or his personal effects** except where:

- the right to search was clearly laid out in an employment contract, collective agreement or employee handbook;
- there is an implied right to do so because it was the employer's past practice to do so;[657] or
- there exists a real apprehension of danger to the company's property and employees.[658]

In the case of an employer searching **company property,** the right to conduct such a search can even arise from a generally worded reserved management's right clause in a contract, which basically states that the employer/management has the right to decide and act on matters that are a part of running the

[656] D. Holmes and S. Ray, "Employee Fraud and How to Prevent It" (March-April, 1999) National 6 at 6.
[657] *RE United Automobile Workers Local 444, and Chrysler Corp. of Canada Ltd*. (1961), 11 Labour Arbitration Cases 152. (Ab. Bd.) (hereinafter *Chrysler Corp*.).
[658] *Re Inco Metals Company and United Steelworkers* (1978), 18 Labour Arbitration Cases (2d) 420. (Ab. Bd.) (hereinafter *Inco Metals*).

workplace business. Employers therefore have the right to search company property such as desks and files.[659]

The existence of a right to search does not automatically give the employer license to conduct a search in any manner. The manner must be reasonable. What is considered reasonable in either type of search is determined on a case-by-case basis and is based on a balancing of the interests of the employer to control theft in the workplace and the employee's privacy rights. To justify a search as reasonable, an employer must be able to show that there was a real and significant suspicion of an employee committing theft before he is searched, and that the employer used a method of searching that ensured that the employee being searched or affected by the search was not publicly singled out or embarrassed in front of other employees.[660] The searching of selected employees without just cause is unfair and unreasonable for it casts undue suspicion on them.[661]

The rules and guidelines for whether or not an employer can search an employee or an employee's workplace surroundings are very similar to those rules that determine whether or not an employer can use surveillance or drug testing on their employees. For more discussion/information on these areas please see Chapter 5: Drug Testing and Chapter 3: Surveillance.

Can my employer search my e-mail or computer at work?

Yes. The law supports that. Flowing from an employer's right to control the workplace, an employer has the right to read the files that are kept in a filing cabinet. Also, an employer has as great a right to review the information contained in work computers as examine the contents of filing cabinets or office desks. In particular, the law says that any e-mail once sent and received also forms an electronic file and that a computer is an electronic filing system. The courts have held that even computer disks are "documents."[662] Regardless of an employee's assumptions and usage of passwords, she generally cannot establish that she has a reasonable expectation of privacy on an employer's business computer. This in turn should help deter the exercise of the employer's right to search the employee's e-mail or

[659] H. L. Rasky, "Can An Employer Search The contents of Its Employees' E-Mail?" (1998) 20 Advocates Quarterly 221 at 223 (hereinafter Rasky).
[660] *Chrysler Corp*.
[661] A. Barss, "Search and Surveillance in the Workplace: The Employee's Perspective." (1992) Labour Arbitration Yearbook 181 at 184.
[662] Rasky, at 224.

computer/disk documents. It is an offence under the *Criminal Code,*[663] however, to intercept a communication between the original sender and its destination.

How can employers protect themselves if they cannot or should not search employees as a way of gathering evidence?

Although an employer is in a difficult position if they cannot use searches to gather proof that employees are stealing, police are also put in an equally difficult position every day when they gather evidence of criminal activity. The difficult challenges the police face have not justified overriding individual *Charter* rights, and likewise employees' rights should not be sacrificed for the purpose of securing a criminal conviction.[664] This type of private law enforcement would allow private employers to side step the *Charter*'s protections and leave employees exposed to abuses such as unreasonable searches or seizures.

If the theft of company property becomes an uncontrollable problem, well-publicized security procedures could be instituted which could protect the interest of the employer without having employees submit to embarrassing occasional spot checks which may cause other employees to believe that they are suspected of theft. In cases where theft is suspected and where there is no express provision permitting an employee search of private items, a company ought to be prepared to ask for the police's help if an employee will not consent to a search by the employer.[665]

4.3 CONCLUSION

The protection from unreasonable search and seizures, as offered by section 8 of the *Charter*, is fairly limited. Generally, it will apply in its full force only to searches and seizures that occur in a purely criminal context. The Supreme Court of Canada has emphasized that section 8 must be applied flexibly in regulatory circumstances; so it will offer little protection when a search or seizure occurs under regulatory legislation such as the federal *Income Tax Act*.[666] In other situations, because there can be a substantially reduced "reasonable expectation of privacy," one cannot be sure of the level of protection. Section 8 also will only apply when the government's act involving the individual's information amounts to a "search" or "seizure." Privacy cases that involve the misuse, transfer,

[663] *Criminal Code*, section 184.
[664] Scharbach, at 45.
[665] *Re Amalgamated Electric Corp. (Markham) and I.B.E.W., Local 1590 (Re)* (1974), 6 Labour Arbitration Cases (2d) 28 (Ab Bd) (hereinafter *Amalgamated Electric Corp*).
[666] *Baron v Canada*, [1993] 1 Supreme Court Reports 416 (SCC).

disclosure or improper retention of personal information will likely fall outside of the scope of the *Charter*'s protection.[667]

4.4 CASE STUDIES

4.4.1 Searches By the Police

R v Harrison, 2009 (Supreme Court of Canada)[668]

An example of the court's systematic review of whether particular pieces of evidence from an unreasonable search should be admitted into court.

The accused was stopped in Ontario because the rented motor vehicle he was driving did not have a front licence plate. The vehicle was registered in the province of Alberta, and did not require a front plate. The police officer had no reason to believe that any offence was being committed but went ahead to check the accused driver's licence. The officer discovered that the accused's licence was suspended and arrested the accused. The officer then searched the vehicle and discovered a large amount of cocaine.

The trial judge conducted a Charter section 24(2) analysis and found that the search of the vehicle was unreasonable and contrary to section 8 of the Charter, but determined that the cocaine was properly admitted in evidence because excluding the evidence would bring the administration of justice into disrepute. The accused was thus convicted of trafficking in cocaine. The accused applied to the Court of Appeal but his conviction was affirmed.

At the Supreme Court of Canada, the accused was acquitted. The court ruled that R v Grant (another Supreme Court of Canada case) had revised the section 24(2) analysis and held that courts must consider the seriousness of the breach of a protected Charter right, the impact of the breach on the accused's constitutional rights and the public interest in seeing the offence charged determined on its merits. The Supreme Court found that the scope of the breaches of the accused's right was serious, as only a bare suspicion existed for the stop, arrest and search. The court determined that the evidence seized represented proof of the commission of a major offence and that allowing the admission of the evidence from the search would undermine the broader reputation of the justice system. Given that the seized evidence was essential to the Crowns case, the court acquitted the accused rather than ordering a new trial.

[667] S. Onyshko, Informational Privacy and the Law in Canada (LL.M. Thesis, University of Toronto, 1995) at 290.
[668] *R v Harrison*, 2009 SCC 34.

***R v Patrick*,** [2009] SCJ No. 17

A case on the search of garbage already placed for collection

The police suspected that Patrick was operating an ecstasy lab in his home and seized bags of garbage he had paced for collection at the rear of his property, adjacent to a public alleyway. The police retrieved the bag by reaching through Patrick's airspace over the property line, to avoid stepping unto his property, and seized items from the garbage. The officers then used evidence of criminal activity retrieved from the bag to obtain a warrant to search Patrick's house and garage. The search turned up more evidence which was also seized.

Patrick argued at trial that the taking of his garbage bags by the police constituted a breach of his right to be free from unreasonable search and seizure guaranteed by s. 8 of the Charter of Rights and Freedoms. The trial judge ruled that Patrick had no reasonable expectation of privacy in the items taken from the bag and found that the seizure of the garbage bags, the search warrant and the search of Patrick's dwelling lawful. Patrick was thus convicted of unlawfully producing, processing and trafficking in a controlled substance. Patrick appealed to the Court of Appeal, but his conviction was upheld.

The Supreme Court of Canada ruled that neither the search of the contents of Patrick's garbage, nor the subsequent search of his dwelling breached section 8 of the Charter. Patrick abandoned his privacy interest in the garbage when he placed it for collection at the rear of his property where the garbage became accessible to any passing member of the public.

R v Grant, 2009 SCC 32

Police observed the accused *in an area that was being regularly patrolled because of its history of student assaults, robberies and drug offences during the lunch hour. Two plain-clothes police officers in an unmarked car drove past the accused and he looked at them in an unusually intense manner and "fidgeted" with his coat and pants in a way that aroused the officer's suspicions. A uniformed officer approached the accused and requested his name and address. The accused provided a provincial health card. The two plain-clothes officers approached the accused and identified themselves as police officers. The uniformed officer then asked the accused if he had anything in his possession that he should not have. The accused replied that he had marijuana and a firearm. The accused was arrested and searched and the marijuana and loaded revolver were seized. He was advised of his right to counsel and taken to the police station. He was charged with several firearms offences, including possession of a restricted firearm. The accused alleged violations of his right to freedom from unreasonable search and seizure under the Canadian Charter of Rights and Freedoms ("Charter"). At trial, the court ruled that there was no Charter breach, admitted the firearm in evidence and convicted the accused of five firearm offences. The trial court also ruled that the officer's inquiries did not amount to a search within the meaning of the Charter and that the accused was not detained prior to his arrest or that, if he was detained, he waived his rights by cooperating. On appeal, it was found that the accused was detained before he made his incriminating statements. The appellate court then ruled that, since the officers had no reasonable and probable grounds to detain him, the detention was arbitrary and a breach of the Charter. The appeal judge determined that the firearm was derivative evidence, but concluded that the admission of the firearm into evidence would not unduly undermine the fairness of the trial.*

On further appeal to the Supreme Court of Canada, the court ruled that, since the firearm was discovered as a result of statements taken in breach of the Charter, it was derivative evidence and the court had to consider whether the evidence was to be excluded. The court also ruled that, while the police were in error in detaining the accused, the mistake was understandable, was not done in bad faith, and was neither deliberate nor egregious. It found, therefore, that the effect of admitting the evidence would not greatly undermine public confidence in the rule of law. It further ruled that the gun was highly reliable evidence, was essential to a determination on the merits and should be admitted in evidence.

***R v Chehil*,** [2013] SCC 49

A case on the extent of Section 8 *Charter* right.

The Crown appealed to the Nova Scotia Court of Appeal against the trial judge's acquittal of Chehil, on a charge of possession of cocaine for the purpose of trafficking. The appeal was allowed, and a new trial was ordered which the accused appealed with leave to the Supreme Court. The court questioned whether the search and seizure of the narcotics were reasonable under section 8 of the Charter.

The police officers of the drug enforcement team at the Halifax Airport (Jetway team), examined the electronic passenger list of an overnight Westjet flight as part of a program designed to curtail drug trafficking. The officers were looking for circumstances that point to the presence of a drug courier on the flight. They had identified the characteristics of the drug couriers as- often travel alone on overnight flights, purchasing a last minute, walk-up ticket in cash, and checking a single bag.

Chehil was the last passenger on the flight. Identifying him as a possible courier, the officers had his luggage and that of some other passengers removed on a secured side of the airport. A police dog sniffed Chehil's luggage and identified it as containing narcotics. After Chehil retrieved his bag, from the carousel, one of the officers arrested him for possession of a controlled substance. Without Chehil's consent, the officer opened Chehil's suitcase and discovered a knapsack containing three kilograms of cocaine. At trial the judge held that the police violated Chehil's section 8 Charter right to be free from unreasonable search and seizures and that the information collected by Westjet was subject to the PIPEDA. The judge also ruled that the evidence was excluded under section 24(2) of the Charter and acquitted Mr. Chehil.

The Supreme Court found that the police had reasonable suspicion of Chehil's drug trafficking and as such the search was Charter complaint.. The court pointed out that balance must be maintained between respecting an individual's right to privacy and recognizing the necessity of interfering with rights in the legitimate interest of enforcing the law. The court also stated that reasonable suspicion requires an objective evidentiary foundation that is reviewable in the court and not equivalent to a "hunch'. The court reiterated that when determining whether the police had reasonable suspicion the totality of the circumstances must be assessed which includes examining exculpatory evidence. Further, police experience and training may be taken into account, but it alone does not entitle officers to deference. Taking all of the factors into account the court held the search was lawful.

***R v Anderson*, [2007] NJ No 31**
A case on a search warrant issued on the basis of a landlord's suspicion.

The accused entered into an agreement to rent to own a residential property. Following the accused's inability to keep up with the payment, the accused's landlord drove by the accused home accompanied by his father, to obtain the outstanding rent or evict the accused. The landlord and his father entered the residence via the basement door which was secured but not locked. They examined the lower portion of the property and went upstairs to examine the upper portion. The landlord and his father noticed a room with marihuana plants and the landlord called the police. The police obtained a warrant and searched the accused's residence on the same day, seizing marihuana plants in various stages of growth, two lights with timer and electrical wiring, and a Newfoundland and Labrador Lights and Power bill in the name of the accused.

The accused applied to court for the exclusion of the seized marijuana plants on the ground that the seizure breached section 8 of the Charter. *The accused argued that the search was invalid as the information used to obtain the search warrant was based solely on the information provided to the police by his landlord which the landlord obtained as a result of having entered his residence. The court ruled that the* Charter *did not apply to the landlord. The court also determined that the landlord acted as private citizen and did not breach the* Charter *by entering the accused residence. The court pointed out that not every illegal act constitutes a violation of the* Charter *and that only evidence obtained in violation of the* Charter *must be excluded.*

R v H (TT), 2006 ABPC 320

The accused was driving a motor vehicle quickly through an alleyway and across the streets to alleyways at about 3.00 am on the day in question. Two uniformed police officers followed the motor vehicle in a marked police car and stopped it. The accused could not produce insurance and said that he did not know the owner of the motor vehicle when asked. The officers decided to seize the motor vehicle and one of them started the paperwork for the seizure. While that was being done, a third uniformed officer who did not know of the decision to seize the motor vehicle arrived the scene. The third officer asked the accused whose motor vehicle it was and felt that the accused answered in a suspicious manner. He then proceeded to check if the motor vehicle's ignition was

damaged in any way and, in the process noticed a bag he suspected contained drugs. The bag contained drugs and he seized it. The officers then decided to arrest and charge the accused.

The court found that an individual driving a motor vehicle that is not his, for which he cannot identify the owner, nor produce valid documentation has no right to privacy with respect to that motor vehicle and cannot expect to prevent the authorities from searching it. The court also ruled that the search was reasonable and that individuals in a public street have a low right to privacy. The court further considered whether, if the accused had a right to privacy, the search was reasonable and ruled that a search without a warrant is, on its face, unreasonable but that there are exceptions. It found that it was unnecessary and unreasonable to search a vehicle that is in the process of being seized and ultimately searched. The search breached the accused right of freedom from unreasonable search and seizure as guaranteed under the Charter *but the court ruled that the breach is minor as the officer acted in good faith and the drug would have been found in any event.*

***R v Feeney*, 1997 (Supreme Court of Canada)[669]**

The case that helped develop the law regarding searches and arrests in private dwellings.

The police went to investigate the violent murder of an elderly man who was found in his home amongst a large amount of blood and with several blunt wounds to his head. His pick-up truck had been found in a ditch about one half kilometer from his home. By questioning the local residents, the police believed that another man, Mr. Feeney, had either been involved in or present at the accident involving the pick-up truck. Police were told Mr. Feeney had gotten home at 7:00 a.m. after a night of drinking and that he was asleep in the small trailer he lived in. Outside it the police yelled, "Police" but got no response. They forced their way into the trailer where they awakened Mr. Feeney who was asleep in his bed. They asked him to step into the light so they could examine his clothes. They saw lots of blood on Mr. Feeney's shirt, arrested him and searched his trailer. At trial Mr. Feeney was convicted of second degree murder.

In reviewing the case, however, the Supreme Court of Canada found that. Feeney's arrest was unlawful because at that time police could not enter a private dwelling without a warrant to make an arrest. In fact, when the police entered Mr. Feeney's trailer, they did not even have enough information to get an arrest warrant for Mr. Feeney, should he have come out of the dwelling, let alone go into a private dwelling after him. The court suggested that a new type of warrant should be legislated if Parliament wanted the police to have the power to arrest people in their homes. In part, because the arrest of Mr. Feeney was improper, the search of Mr. Feeney's trailer was also unreasonable and in violation of his Charter *right to be free from unreasonable search and seizure. The court, therefore, had to determine whether or not the evidence from the searches could be used in court. Mr. Feeney's fingerprints and statements, were determined to be* <u>not discoverable</u> *by other means. Allowing their use would have affected the fairness of Mr. Feeney's trial, so the court excluded them. The use of the remaining evidence (the bloody shirt, shoes, cigarettes and money) would not have affected the fairness of the trial. However, they were still excluded because the court found that the police obtained them in bad faith or through very serious* Charter *violations. In this case the police flagrantly disobeyed case law on making arrests in dwellings and reading a person his rights. The court found the police to be acting in a pattern of disregard for* Charter *rights without any urgent circumstances requiring them to do so. The court excluded the evidence not so much as to punish the*

[669] *Feeney*.

police's behavior but to help ensure that every person (innocent or presumed innocent) is entitled to full protection of the Charter.

The court's ruling in this case caused concerns that in certain situations public safety might be put at risk because of the delay created by the police always having to obtain a warrant to enter a dwelling. Changes were made to the law[670] *creating a special warrant to enter a private dwelling to arrest or apprehend a person, setting out clear procedures the police must follow before entering the private dwelling, and indicating the urgent circumstances in which a warrant from a judge would be impractical and not needed. The aim of the new legislation was to strike a reasonable balance between the police's powers to protect the public and the privacy rights of Canadians.*

***R v Golden*,** 2001 SCC 83

A case on strip searches.

A police officer set up an observation post in a building across from a sandwich shop to detect illegal drug activities. While watching the area through a telescope, an officer observed two people receiving a white substance from the accused and directed that the accused be arrested.

The accused was observed crushing alleged crack cocaine in between his fingers during the arrest but a frisk search of the accused found no weapon or narcotics. The officer then decided to search the accused's underwear and buttocks. At the landing at the top of the stairwell leading to the basement of the building, the officer undid the accused's pants and pulled back his underwear, to discover a plastic wrap containing a white substance protruding from the accused's buttocks. The officer attempted to retrieve this substance but was hip-checked by the accused. The officer took the accused back to the shop, and forcing the accused to bend over, continued the search. The officer pulled down the accused pants, exposing his genitalia and buttocks while trying to remove the package, but the accused repeatedly clenched his buttocks. Subsequently, with the accused held face down to relax, another officer retrieved the package from the accused buttocks with a pair of rubber gloves used for cleaning the washroom. The accused was then arrested and taken to the police station for more strip searching.

[670] Department of Justice Canada, News Release "Minister of Justice Tables Response to Feeney Case" (October 30, 1997).

At trial, the defence's application to exclude the evidence obtained from the second search was denied and the accused was found guilty of possessing a narcotic for the purpose of trafficking but was acquitted of assaulting a police officer. He was subsequently sentenced to 14 months imprisonment. The accused's appeal was dismissed at the Court of Appeal and he further appealed to the Supreme Court of Canada.

The Supreme Court found that searches of the person incident to arrest are the exception to the general rule that warrantless search are unreasonable under section 8 of the Charter. *The court however stated that for a strip search to be justified as an incident to arrest, the following conditions must be met: (1) the arrest must be lawful, (2) the search must be incident to the arrest and (3) the search must be conducted in a manner that does not interfere with the accused's* Charter *rights. The court ruled that strip searches should only be conducted at the police station except where the police could establish that they have reasonable and probable grounds to believe that it is necessary to conduct the search in the field rather than at the police station. Such situations were expressed as where there is a demonstrated necessity and urgency to search for weapon or objects that could be used to threaten the safety or the accused, the officers, or others. The Court determined that the chances of the accused disposing of the evidence on the way to the police station was low and that even if the accused disposed of the evidence, it would have been in the police cruiser and could have still been linked to the accused. The Court found that the decision to conduct the strip search was unreasonable as it was based on the officer's hunch. The Court found that the manner the search was conducted breached the accused's section 8 Charter rights. The accused's conviction was set aside and an acquittal entered.*

Reynen v Antonenko et al, 1975 (Alta. Supreme Court - Trial Division)[671]

An old case on the use of sigmoid scope in a lower body cavity search.

The police received information which led them to believe that Mr. Reynen would be traveling from Edmonton to Vancouver to buy drugs and then returning to Edmonton on the same day with the drugs hidden in his rectum. They saw Mr. Reynen board a plane headed for Vancouver under an assumed name. About four hours later he returned. Seeing the police approach, Mr. Reynen changed direction. When the police caught up with Mr. Reynen, they grabbed him by the throat to prevent him from swallowing any drugs he may have had hidden in his mouth, told him he was under arrest and handcuffed him. The police checked the inside of his mouth with a finger searching for drugs, but found none. Back at R.C.M.P. headquarters Mr. Reynen was asked to disrobe and his clothes were searched, but again no drugs were found. When Mr. Reynen was asked to bend over, the police noticed that the hair around his rectal area appeared to have been "greased." The police told Mr. Reynen to go to the bathroom and remove the drugs or he would be taken to the hospital to have them removed. Mr. Reynen chose to go to the hospital. At the hospital Dr. Antonenko told Mr. Reynen that he would have to do a rectal examination on him which would be uncomfortable. Following the Doctor's instructions, Mr. Reynen position himself on the examining table. Dr. Antonenko performed a rectal examination first by finger and then by using a sigmoid scope, which is like a hollow tube. When the sigmoid scope was inserted six inches into the anal canal, the doctor found and removed two red rubber condoms. Each condom was found to contain 25 capsules of heroin. Mr. Reynen later pled guilty to the narcotics charge laid against him.

Mr. Reynen sued the doctor and detectives for assault and battery, claiming the examination of his anal canal was done without his consent and there was no emergency requiring it to be done. An Alberta Court, however, found that the police had the statutory right and duty under the (then) Narcotics Control Act *to conduct a search and seizure of any drugs, and that the police are authorized to use such force as is reasonable, proper and necessary to carry out their duty provided no unnecessary violence is used. The court then reviewed the case to determine if the actions of the police were reasonable. The examination, conducted in a hospital by an eminently qualified medical practitioner, showed that the police took care to ensure Mr. Reynen was not subjected to any unreasonable force. The doctor testified that he would only do this type of examination with the suspect's cooperation in properly positioning himself as Mr. Reynen had done. Although the court*

[671] *Reynen v Antonenko*.

did not doubt that Mr. Reynen suffered some discomfort during the examination, he was not injured in any way by it. Overall the court found that the anal search was done in a reasonable and proper manner and without any unreasonable force or threat to Mr. Reynen's health and well-being. Mr. Reynen's lawsuit against the doctor and detectives was dismissed.

R** v **Godoy, 1998 (Supreme Court of Canada)[672]

A court reviews the scope of the police's powers in responding to emergency 911 calls.

A 911 emergency call from Mr. Godoy's apartment was received, but the line had been disconnected before the caller spoke. The call was traced and police officers were dispatched to the location to investigate the type of help needed. When the officers knocked at the apartment door, Mr. Godoy partially opened the door and said that there was no problem. The officers asked if they could enter to investigate, but Mr. Godoy tried to close the door. The officers stopped the closing of the door and entered the dwelling where they immediately heard a woman crying. In the bedroom they found Mr. Godoy's common-law wife crying in a curled fetal position. There was swelling above her left eye and one of the police officers said she had told him Mr. Godoy had hit her. Mr. Godoy was placed under arrest for assaulting his wife. In Mr. Godoy's struggle to resist the arrest a police officer's finger was broken, and Mr. Godoy was also charged with assaulting a police officer with the intent of resisting arrest.

The initial charge for assaulting his wife was dismissed after she testified in court that Mr. Godoy did not hit her. In reviewing the second assault/resist police officer charge, the trial judge determined that since the officers' entry into Mr. Godoy's apartment was unauthorized or without the proper reasonable and probable grounds necessary to violate the sanctity of a person's dwelling, all of the police's actions flowing from the event were illegal. The trial judge dismissed the assault/resist police officer charge. But the case was appealed to the Supreme Court of Canada where, in order to determine whether or not the police could forcibly enter dwelling houses in the course of the investigation of 911 calls, the court had to consider 1) if the police conduct fell within the general scope of their duty, and 2) if the conduct was a justifiable use of police powers associated with the duty. This two-step test is also known as the Waterfield test for evaluating the police's common law powers.

[672] *R v Godoy*, [1999] 1 Supreme Court Reports 311 (S.C.C.).

Canada's top court first found that 1) giving help to persons in distress is certainly part of the police's common law duty to preserve the peace, prevent crime and protect life and property. The court also determined that 2) the police's intrusion was minimal for they were in the apartment for only a short time and only because they had received an unsatisfactory answer at the door. Having stayed within the scope of their duties and limiting their intrusion, the court concluded that the police's actions were not illegal and the case was returned for a new trial on the charge of assault/resist police officer. On one hand, the court recognized the unquestionable privacy interest that one has in the sanctity of one's home. On the other hand, however, the court found that a 911 call is a person's call for help, and that due to such things like heart attacks, being held at gun point or domestic violence, the person may not be able to answer the door, but nonetheless still need help. While the court found that the extent of what the officers did in this particular situation was justified, it cautioned that responding to a 911 call would not give them the further authority to search the premises or otherwise further intrude on a person's privacy or property.

4.4.2 Searches By Customs

Regina v Monney, 1999 (Supreme Court of Canada)[673]

A case dealing with the authority of customs officers to detain and search travelers suspected of having swallowed narcotics.

Mr. Monney arrived at Pearson International Airport at approximately 4:00 p.m. after having swallowed 84 pellets, each containing about five grams of heroin, that had been wrapped in condoms. Mr. Monney claimed he was a taxi driver and had flown to Switzerland to visit a distant relative. The customs officers noticed that Mr. Monney appeared nervous, had no checked baggage, had not declared a bottle of alcohol in his possession, had bought an expensive airline ticket on a taxi driver's salary on the same day he flew, was born in Ghana (a country known as a source of narcotics) but denied ever having been there and was using two passports - one of which had a recent Ghana stamp on it. The customs officers decided they had sufficient grounds to detain Mr. Monney as a suspected drug courier and informed him of his right to a lawyer, whom Mr. Monney eventually consulted. He was taken to a "drug loo facility," which contains an apparatus similar to a toilet. This unit permits customs officers to process fecal matter and isolate any narcotics and associated material that passes through the digestive system of a suspected drug swallower. Although nothing was found during the strip search, a urine test showed positive signs of heroin. Written policy in the Customs Manual required that travelers suspected of swallowing narcotics are to be detained in the presence of qualified medical personnel, because of the dangerous health risk. Mr. Monney, however, said he felt fine and was instructed to tell the officers if he felt any stomach pains so that they could call a doctor. By 9:18 p.m. Mr. Monney began to excrete the pellets. By 1:50 a.m. 83 of the pellets had passed and he was transferred into the custody of the RCMP where he later passed the last heroin pellet. The court was asked to review whether the Customs Act[674] *authorizes this type of search .*

The Supreme Court of Canada found that in authorizing a search for that secreted "on or about his person," the Customs Act authorizes the detention of a traveler for such a period of time as necessary to confirm or discredit suspicion by means of a passive "bedpan vigil." The Act also requires that the search be done "within a reasonable time." The court determined that the delay of 30 minutes from the time Mr. Monney was detained until the search/bedpan vigil began was reasonable. There

[673] *R v Monney* (1997), 120 Canadian Criminal Cases (3d) 97 (Ont CA); reversed (1999), 133 Canadian Criminal Cases (3d) 129 (SCC).
[674] *Customs Act*.

was expert testimony that, given the dangerous health risk of having that much heroin inside a person, hospitalization would have been prudent while waiting for the pills to pass. But the court found the "port policy" used, the monitoring of Mr. Monney and his ability to advise of any change in his condition, also reasonable. Overall the court found that, although the compelled production of a urine sample or a bowel movement was an embarrassing process, in the context of a custom's setting this type of search did not violate the Charter *and was done in a reasonable manner. The court refused to comment on whether a more invasive form of collection, such as surgery or inducing a bowel movement, would also have been found to be reasonable.*

4.4.3 Searches of Students in School

R v M (A), 2008*,* (Supreme Court of Canada)[675]

The principal of a high school, which had a zero tolerance drug policy, gave a standing invitation to the police to bring sniffer dogs into the school to search for drugs. Police officers went to the school with a sniffer dog to conduct a random search. The officers had no information that drugs were present in the school and had no grounds to obtain a search warrant. They, however, obtained the permission of the school to conduct the search. The principal instructed the students to remain in their classrooms while the sniffer dog searched the gymnasium. The dog reacted to an unattended backpack. The police officers opened and searched the backpack without a warrant, and found some unlawful drugs. M, the student who owned the backpack was charged with possession of marijuana for the purpose of trafficking and the possession of psilocybin ("magic mushrooms").

The youth court judge ruled that both the sniffer dog search and the physical search of M's backpack were unreasonable as there was no basis for the search. The judge excluded the evidence on the ground that admitting it would bring the administration of justice into disrepute and acquitted M. The Crown's appeal to the Court of Appeal was dismissed. The Court of Appeal found that the youth court judge was correct to exclude the evidence as the search was a warrantless random search. The Crown further appealed to the Supreme Court of Canada.

[675] *R v M (A),* 2008 SCC 19, 55 C.R. (6th) 314; New Jersey *v* T.L.O., 469 U.S. 325, 105 S. Ct. 733, 1985 U.S. LEXIS 41 (1985) as discussed in Alderman and Kennedy.

The Supreme Court found that students are entitled to privacy even in a school environment. The court ruled that there was no authority for the sniffer dog search in either statute or common law and that the evidence was properly excluded under section 24(2) of the Charter. *The Crown's appeal was dismissed.*

***R v MRM*, 1998 (Supreme Court of Canada)[676]**

An example of a school official doing a search on a student in the presence of a police officer.

In the week before the search, the junior high school vice-principal was told by three or four students that a certain student was selling drugs on school property. On the day that a school party was to be held later that evening, the vice-principal was told that this same student "would be carrying tonight." When this 13 year old student arrived at the school party with a friend, the vice-principal escorted both of them into his office where, according to school policy, a plain clothes policeman was present during the vice-principal's search of the two teenagers. The search consisted of emptying pockets and pulling up one's pants. The particular student that the vice-principal received information on had a cellophane bag of marijuana hidden in his sock. The student carrying the marijuana was turned over to the plain clothes policeman who advised the student that he was under arrest for possession of a narcotic. The policeman read the student the police caution and his right to counsel. The police officer and arrested student went to the student's locker and searched it, but no drugs were found in it. The student was charged with the possession of a narcotic.

In the lower court the judge ruled that the student was detained for the search without having been informed of his legal rights, so the evidence from the search was excluded from the trial and the student was found not guilty. The higher Court of Appeal, however, found that the vice-principal's actions were reasonable and ordered a new trial. The Supreme Court of Canada agreed, saying that just because there was cooperation between the vice-principal and the police, and that a police officer was present during the search, this was not enough to show that the vice-principal was acting as an agent of the police or that the police officer was carrying out the search. The court said there was no reason to believe that the search would not have taken place if there had been no police involvement. It was, therefore, acceptable for the vice-principal to search the student based only on a reasonable suspicion that he was carrying drugs, rather than having to meet the higher standard of reasonable

[676] *R v MRM,* 1998 (Supreme Court of Canada).

and probable grounds that police must have before they do a search. The court found that because students know that school officials are responsible for providing a safe school environment and that this may sometimes require searches of students and their personal effects, students have a diminished reasonable expectation of privacy. The court also found that students in school are not detained in the same sense that the Charter *refers to when it provides that one must be advised of their right to counsel, so students being searched by school officials in school do not have to be notified of or given their right to have counsel.*

R** v **W (JJ), 1990 (Newfoundland Supreme Court - Trial Division)[677]

An example of the factors that a court took into account when reviewing a school locker search. *A principal knew that some of the students at his high school were using illegal drugs. In fact, he even kept a list of troubled students whose behavior might relate to illegal drug use. While questioning one student about some of the problems the student had in school, the student told the principal that what he himself was doing was minor compared to what he saw other students doing. With some encouragement from the principal, this student gave him the names of three students who were selling drugs in the school and had them in their lockers. Two of these names had come up before when the school staff and the principal were discussing students they believed were selling drugs in the school. With the additional information from this informant student, the principal had the three students mentioned open their lockers. Small quantities of drugs were found in two of the three lockers. The two students were charged for possessing drugs.*

The trial judge ruled that children in a school must have at least some minimum protection of their rights, and did not feel that the principal had enough evidence to justify the intrusion into these three students' lives. The drugs found during this search were not allowed to be entered into evidence and the students were acquitted. But a higher court, the Court of Appeal, found that the informant had not only provided the names of the students selling drugs that supported the principal's suspicions, but also mentioned the quantities they sold. The Court of Appeal determined that this was enough to meet the standard of "reasonable suspicion" which the principal needed to do the locker searches. There was no evidence to show that the actual search was excessively intrusive. The court found that in the face of the additional allegations from the informing student, the principal had to do something and what he did was reasonable. The higher court also reminded us that even if the trial Judge was right

[677] *R v W(JJ)* (1990), 83 Newfoundland and Prince Edward Island Reports 13 (NLSC).

in finding that an illegal search and seizure had taken place, it would not automatically mean that the evidence found during the search had to be excluded. There would have to be additional arguments made to show that it would be more likely that the administration of justice would be brought into disrepute if the evidence was admitted than if it were not admitted. A new trial was ordered at which the search and seizure of the drugs would be treated as legal and accepted into court as evidence.

4.4.4 Searches By Private Security Guards

***R v Buhay*, 2003** (Supreme Court Of Canada)[678]

A court's review of a search by both private security guards and police).

A short time after the accused rented a locker at the Greyhound bus depot in Winnipeg, a security guard at the bus depot detected a strong odour of marijuana from the locker. A Greyhound agent opened the locker and the security guards discovered a duffel bag containing some marijuana. The security guards placed the items back in the locker and called the police. The police officers smelled the marijuana and a Greyhound agent opened the locker for them. One of the officers seized the duffel bag containing the marijuana without a warrant. The accused came to retrieve the package the next day and was arrested. He was subsequently charged with the possession of marijuana for the purpose trafficking. At trial, one of the officers testified that he didn't consider getting a warrant while the other said he considered a warrant but felt he had insufficient grounds to obtain one. The officer also testified that he believed the accused had no reasonable expectation of privacy on the locker. The trial judge found that the police officers abused the accused's section 8 Charter *right and excluded the evidence under section 24(2) of the* Charter. *The Court of Appeal entered a conviction, and the accused appealed to the Supreme Court of Canada.*

The Supreme Court determined that the accused had a reasonable expectation of privacy in the content of the locker. The Court pointed out that while the expectation was not as high as the privacy afforded to one's own body, home or office, that a reasonable expectation of privacy existed in the locker sufficient to engage the accused's section 8 Charter *rights. The Court found that the accused had possession of the contents of the locker by the possession of the key and that the existence of a master key does no destroy the expectation of privacy. The fact that the signs on the lockers made no mention of the possibility that the locker might be opened and searched into was also considered.*

On the searches of the locker, the Supreme Court ruled that the search conducted by the security guards did not trigger any Charter *applications as the guards were not acting as agents of the state. The warrantless search and seizure by the police was however found to be an impermissible intrusion of the state on the*

[678] *R v Buhay*, 2003 SCC 30.

accused reasonable expectation of privacy, and a violation of his section 8 Charter right*. The Court deferred to the trial judge's decision to exclude the evidence under section 24(2) and restored the accused's acquittal.*

***R v Fitch*,** 1994 (British Columbia Court of Appeal.[679]*)*

An example of University Security Officers doing a room search.

On the evening of July 1st it was noticed that Mr. Fitch had not paid his rent for his room at the University of Victoria, where he was a student. In such circumstances it was normal procedure to send a campus security guard to knock on the door and if there was no answer to open the door and see if the person had vacated the room. When the security guard opened the door and entered the room he not only saw that the resident's possessions were still in it, but he also reported seeing some equipment on a desk that looked similar to some equipment that had been reported stolen two weeks previous. On the following day, based on this report, the Assistant Manager sent a second security officer to check on the room again. When this security officer entered the room he not only saw the previous items mentioned, but he opened a drawer under the bed and found nine camera lenses and two physics lasers that also appeared to be University property. Shortly afterwards three police officers attended, entered the room and were shown the various items of suspected stolen property. They returned to the police station to get a search warrant. Later in the evening the three police officers returned with a search warrant and conducted a detailed search of the room. On July 3rd, a police officer obtained a further search warrant after receiving information that the room had been entered into overnight. Once again the police seized a number of exhibits from the room.

In reviewing the search of the student's room, the court was not presented with proof that the security officers were state agents or were working in concert with the police. The court therefore determined that the University of Victoria Security was acting on its own in searching Mr. Fitch's room. The court determined that the first entry by the security officer was a minor intrusion for the legitimate purpose of seeing whether or not the room was abandoned. He had been performing a domestic function and had not entered on a criminal investigation. This did not amount to an unreasonable search. This security officer had seen enough to support getting a warrant and the proper thing for the security supervisor to have done was to call the police. Since the police could have gotten a warrant and done a search based on what was seen during the first entry alone, the court found that there was no Charter *violation by a state agent and the seized stolen property was admissible into court. The court, however, did mention that if it had been shown that the security officers were state*

[679] *Liquor Control Act*. Revised Statutes of Canada 1985 c N-1, s 12.

agents by being employed to provide security for a large, publicly funded institution, then the internal university security personnel would have been subject to the same standards as police officers.

***R v Brown*, 2008** (Supreme Court Of Canada)[680]
A case involving the use of sniffer dogs for searches

Three RCMP officers in plain clothes watched passengers disembark from an overnight bus from Vancouver, at the Calgary Greyhound bus terminal. The officers were part of the RCMP Jetway Program, a project which monitors travellers and identifies drug couriers. One of the officers became suspicious of the accused's behaviour while he was disembarking from a bus and proceeded to talk to him about the purpose of his travel. The officer warned the accused that he was not in any sort of trouble and was free to go at any time. The officer asked to see the contents of the accused's bag, and the accused obliged. Before the officer could touch the bag however, the accused angrily exclaimed, "What are you doing?" and pulled the bag back. The officer signalled to another police officer who came along with a dog trained to identify odours and controlled substance. The dog indicated the presence of drugs in the bag and the accused was arrested for possession of controlled substances for the purpose of trafficking.

The accused applied for the exclusion of the evidence at trial, on the basis that the search was unreasonable. The trial judge ruled that the dog's sniff of the accused's bag did not constitute a search within the meaning of section 8 of the Charter *as the accused had no reasonable expectation of privacy in the contents of the bag nor on the odour emanating from his bag. The trial judge convicted the accused of possession of cocaine and heroin for the purpose of trafficking. The accused's appeal was dismissed by the Court of Appeal, and he further appealed to the Supreme Court of Canada.*

The Supreme Court ruled that the use of sniffer dogs constituted a search within the meaning of section 8 of the Charter and a violation of the accused's section 8 Charter *right. The court found that the common law did not authorize the police to conduct a search in the fulfilment of their general duty investigate crimes. The Court cautioned that the exercise of the police powers should not be lowered to one of reasonable suspicion to avoid impairing the safeguards found in section 8 of the* Charter *against unjustified state intrusion. The Court allowed the appeal by the accused and set aside his conviction.*

[680] *R v Brown*, 2008 SCC 18.

4.4.5 Searches of Employees

A series of cases discussing whether or not certain employer searches of employees were conducted in a reasonable manner.

R v March, [2006] (Ontario Justice)[681]

Search of a Federal Jail Employee.

Glenn March, a corrections officer employed at the Stratford Jail, was charged with the offence of unlawful possession of cannabis. Chief Downing of the Stratford Jail received a tip that Mr. March was going to smuggle contraband tobacco into the Stratford Jail for an inmate. He commenced surveillance in the vicinity of the Stratford Jail with inspector Farkas. On the stated day, Chief Downing walked to the area described in the tip and found a Tim Horton's coffee cup with $150.00 cash and some contraband tobacco. He later observed Mr. March walk over the location of the contraband, stand facing the road while smoking a cigarette, look both ways and bend over the area in which the contraband was hidden, before going into the staff entrance of the Jail. Chief Downing could not see what Mr. March did when he bent over, but confirmed that the coffee cups and their content had been removed.

Chief Downing and Inspector Farkas met the Jail Superintendent on how to confront Mr. March, following which the Superintendent gave Chief Downing a written authorization to search Mr. March or any of his property located around the correction institution.
Mr. March co-operated with the inspectors and handed over 2 bales of tobacco and rolling papers, but a further search uncovered 14 grams of cannabis. Consequent to the search, Mr. March challenged the constitutionality of the section 22 of the Ministry of Correctional Services Act (the "Act") *that authorized the employee search. Mr. March submitted that he was an employee, not an inmate and that he had an expectation of privacy over his belongings and that the warrantless search violated his section 8* Charter *rights against unreasonable search or seizure.*
The court referred to a previous decision that determined that a search will be reasonable if it is authorized by law, if the law itself is reasonable and if the manner in which the search was carried out is reasonable and .ruled that the Inspectors were engaged in a valid and necessary administrative investigation within their mandate under the Act. The court also found that the search provisions of

[681] *R v March,* [2006] O. J. No. 664.

the Act did not infringe an employee's reasonable expectation of privacy within the environment of the correctional institution. The court determined that the search provision of the Act was tailored to balance the state's interest in preventing employee smuggling and the rights of Ministry employees to be free from unreasonable search and seizure. The evidence of the cannabis was admissible and Mr. March was found guilty.

Amalgamated Transit Union Local No. 569 v Edmonton (City) (2004) (Alberta Court of Appeal)[682]

An employee of the city of Edmonton's transit department, who suffered from various health conditions, was off work while his medical condition is investigated. The city ordered a video surveillance of him in a local greenhouse. The video showed him performing various strenuous physical acts. The employee subsequently refused a back-to-work plan proposed by the city and his employment was terminated. The video was admitted in evidence at a proceeding before the Board of Arbitration ("Board"). In an application for a judicial review of the arbitration decision the employee's union relied on s. 8 of the Canadian Charter of Rights and Freedoms ("Charter"*) to argue that the video violated the employee's right to privacy and should not have been admitted. The city argued that the* Charter *did not apply to it in its private actions or contracts.*

The court found that the Board was right in admitting the video and ruled that the Charter *guarantee of security from unreasonable search and seizure only protects a reasonable expectation of privacy. It does not protect a general right to privacy. The right to privacy, the court ruled, is determined by weighing the individual's interest in being left alone by the state against the state's interest in intruding on the individual's privacy in order to advance its goals. The court concluded that the right to privacy extends only to those things that an individual reasonably feels, wants or believes are or ought to remain private but does not extend to things done by the individual in public. The court further ruled that there is no general employee right of privacy in Alberta and that, as a governmental entity, the* Charter *applied to the city in all of its actions, including contracts. The court found no distinction between governmental and non-governmental actions and ruled that the* Charter *comes into play, not on the basis of the nature of the act, but because of the status of the city as a government entity.*

[682] *Amalgamated Transit Union Local No. 569 v Edmonton (City)* (2004), 356 AR 228 (Alberta Court of Appeal).

Goodyear Canada Inc. and U.R.W., (1994) (Newman)[683]

The company experienced a loss of goods valued in the area of $100,000 over three years, which it attributed to internal theft. When a $2,400 sophisticated electronic balance scale went missing from the plant laboratory, a general search for it turned up "stashed" prior stolen goods in certain unoccupied lockers. Due to the serious problem of theft and the continued urgent search for the recently missing scale, the company was found to have a right to conduct locker searches. But the arbitrator found that failure to give the employees with unlocked lockers notice of the upcoming searches and the opportunity for them to be present during the locker inspections was unreasonable. An unlocked locker was not tantamount to consenting to having the locker searched.

R v Cole**,** 2012 Supreme Court of Canada 53.

A in school computer technician gained access through the school's server to the contents of a teacher's employer provided laptop. The technician discovered sexually suggestive images of a naked tenth year student which was reported to the school board. The board kept the computer, a copy of the images and a temporary Internet file which was eventually turned over to the police without a warrant. The teacher was then charged under the Criminal Code for possession of child pornography. The accused argued that the search and seizure by the police violated their Charter rights and as such the evidence should be excluded.

The court addressed whether the school had the right to search the accused's laptop by examining whether the accused had a reasonable expectation of privacy. The court found that due to the personal use of the computer and the private nature of its contents there was a reasonable expectation of privacy. Further, the accused privacy rights were not erased simply because the computer was the property of the school and there were workplace privacy polices and practices in place. In the circumstances though the school had that authority to seize and search the laptop to maintain school safety.

The court also stated that although the board had the authority to conduct a search and seizure of the laptop the police could not. This power of an employer is not transferable and does not give

[683] *Re Goodyear Canada Inc. And United Rubber, Cork, Linoleum & Plastic Workers of America, Local 189* (1994), 44 Labour Arbitration Cases (4th) 203 (Ab. Bd.).

the employer the right to disclose the evidence to the police without a valid warrant. Due to this the accused's section 8 Charter interests were violated. Despite this the court held that the evidence should be admitted since, in the circumstances, a warrant would have been given that likely would have resulted in the discovery of the evidence.

***Drug Trading Co. and Energy and Chemical Workers* (1988)** (Foisy, Q.C.)[684]

In a warehouse, employees filled out orders for drugstores, including narcotics, and had the merchandise shipped out. The company did a random search of some lockers and personal effects at shift end. They were interested in searching two persons in particular, but in order to make it appear fair, they searched a total of 15 employees who were each paid for the additional time they were kept after work. The arbitrator found that in the employment contract the employer had an implied right/management rights clause to search employee lockers, their personal effects and, to a limited extent, their persons, so the company was not obligated to justify why it did a search. The arbitrator, however, found that the actual search, singling out of only certain employees and having the searches conducted in a public hallway in full view of the next shift's employees and supervisors, was conducted in an unreasonable manner. The arbitrator held that the existence of an implied right to search does not allow the employer to disregard the employees' right to privacy. The company must devise a method which will ensure that employees being searched will not feel singled out and embarrassed in front of others. The arbitrator also found that if the company is to search personal effects such as purses and pockets, then employees have a right to be notified so that they can make the decision of what to carry into work.

[684] *Re Drug Trading Co. Ltd. & Druggists' Corp. Ltd. and Energy & Chemical Workers, Local 11* (1988), 32 Labour Arbitration Cases (3d) 443 (Ab. Bd.).

5.0 INTRODUCTION TO DRUG TESTING

What is the history of drug testing and drug legislation?

Virtually every culture appears to have had a drug of its choice. While the European culture used alcohol, and the Asians were associated with opium, other drugs like Cannabis, Coca plant leaves and Peyote were favorites of other cultures. When the early drug prohibitions were put in place, they were not based on sound scientific knowledge of the negative health effects of drugs but were driven by the demands of the public to protect the moral values of the dominant culture. From this view, drug legislation is not only an attempt to help protect society from moral degradation, but it is a form of censure against the moral values of the various other cultures that the majority culture repeatedly defines itself against. Cultural bias has largely been the main motivation for much of the legislation against drugs and, even though the advocates of drug testing generally avoid discussing this social inequity, it should be borne in mind when weighing the arguments supporting drug testing against the intrusiveness of drug testing.[685] Drug testing is not only about protecting the public, it is also about a particular attitude towards the perceived users of drugs.[686]

What is drug testing?

Drug testing is the analysis of a sample that is taken from a person in order to determine the presence of certain substances in him or her. It is usually done when someone wants to confirm a person's impairment, but as will be demonstrated, drug testing reveals more about a person's lifestyle than it might on their possible impairment. Drug testing can involve many variables. There can be a variety of reasons for the testing, a wide variety of combinations of drugs that can be tested for in different concentrations, a wide range of people who could be tested, and many different testing methods.[687] All of these variables must be considered in order to determine the best drug testing program to meet a specific goal.

How is drug testing done?

There are many ways that drug testing is done, including:

---

[685] John Weir, "Drug Testing: A Labour Perspective" (1994) 2 Canadian Labour Law Journal 451 at 452-453 (hereinafter Weir).

[686] Eugene Oscapella, "Drug Testing and Privacy: 'Are You Now, or Have You Ever Been, A Member of the Communist Party?' McCarthyism, Early 1950's. 'Are You Now, or Have You Ever Been, A user of Illicit Drugs?' Chemical McCarthyism, 1990's" (1994) 2 Canadian Labour Law Journal 325 at 326 (hereinafter Oscapella).

[687] Privacy Commissioner of Canada, *Drug Testing And Privacy* (Ottawa: Minister of Supply and Services Canada, 1990) at 5 (hereinafter Privacy Commissioner).

- urinalysis,
- breathalyzer,
- blood testing,
- hair testing,
- Saliva drug testing or
- psychological testing.[688]

A breathalyzer test consists of measuring a person's alcohol level through obtaining a sample of one's breath blown into a machine. It is possibly the least invasive drug testing method and offers virtually no further information as to the health of the person.[689] Blood testing, on the other hand, requires that a sample of blood be taken from the person. Because this creates some physical discomfort and a small risk of infection, it is considered the most invasive form of testing. The blood sample also contains lots of information on the biological and physiological status of the person.[690] Hair testing requires collecting a small hair sample from a person and sending the hair to a lab for analysis. Hair drug testing is less invasive than blood testing and can detect drug use of up to several months. Saliva drug testing involves placing a swab similar to a toothbrush but with a pad, between a person's lower cheek and gum for few minutes to collect saliva. Psychological testing involves the use of test to quantify a person's behaviour, abilities and problems, and making predictions based on the performance. There are several methods of conducting psychological testing, and most require soliciting answers from the person being assessed. When testing for the presence of drugs other than alcohol, urinalysis is the most commonly used drug test in Canada.

How is urinalysis drug testing done?

As the name suggests, urinalysis is carried out by obtaining and analyzing a urine sample. Diluting a urine sample with water or adding other substances to it like hand soap or salt will defeat this test,[691] so usually people giving the sample have to either undress or get searched. This helps ensure they are not hiding any chemicals that could alter the sample or are not hiding a separate clean sample to substitute for the one they are about to give. Another collection method, which also helps to ensure that there is no tampering with the sample, is to have a stranger watch the filling of the urine sample

[688] Privacy Commissioner, at 10.
[689] Weir, at 455.
[690] Weir, at 455.
[691] Stay Lanyon and Nerys Brown, "Controlling Drugs In The Workplace And Employee Privacy: The Balancing of Interest. Article two of two" (1992) 2.1 Employment and Labour Law Reporter 13 at 16 (hereinafter Lanyon and Brown).

container. If this method is used, people not only have to pass and handle a sample of human waste but must suffer the indignity of having someone they do not know watch the whole process. Despite its intrusiveness, urinalysis has become very popular with both the government and private sectors.[692]

What are some of the problems with urinalysis drug testing?

Urinalysis is not a single, well-defined process. Some methods of urinalysis are better at identifying certain drugs than others. Some methods are more expensive than others. And some methods of urinalysis require greater expertise to perform than others. Urinalysis cannot determine precisely when the detected drug was used nor how much of it was used. It cannot confirm past or present impairment. Urinalysis can only show that the substances for which it tested have been taken some time in the recent past.[693] Urinalysis has error rates of up to 40 percent.[694] Some of the errors are attributed to human error, some are equipment error, and some are due to the processes' limits in distinguishing between various substances.

What kinds of substances do urinalysis drug tests detect?

Urinalysis detects not only illegal drugs, but also legitimate ones—like some prescription drugs and over the counter drugs—which the test sometimes confuses with illegal drugs. Positive test results may occur when a test subject has taken such common substances as caffeine, asthma medicine, herbal tea, poppy seeds, cranberry juice, or a number of over the counter drugs like Midol, Dristan, Triaminic-DM cough syrup, Advil, Motrin, Anaprox or Propanylamine.[695] A person can also test positive by passively inhaling marijuana smoke[696] or by having higher levels of melanin pigment, which is found in persons of colour and is chemically similar to the active ingredient in marijuana.[697] Factors that affect the rate at which people process and excrete drugs, such as weight, stress, menstrual cycle and frequency of drug use, can also modify test results.[698]

What does a positive urinalysis test mean?

Because of the limitations, a positive urinalysis drug test result may mean that the person tested

- is a chronic user of the drug tested for,

[692] Privacy Commissioner, at 2.
[693] Privacy Commissioner, at 11.
[694] Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Random House of Canada, 1995) at 120 (hereinafter Cavoukian).
[695] Lanyon and Brown, at 16.
[696] Lanyon and Brown, at 16.
[697] Weir, at 451.
[698] Lanyon and Brown, at 16.

- has used the drug intermittently,
- is addicted to the drug tested for,
- is presently under the influence of the drug,
- is taking the drug under a physician's order, and / or
- has had a false positive test result occur.[699]

What does a negative urinalysis test mean?

On the other hand, a negative urinalysis drug test result may mean that the person tested

- is not using the drug tested for,
- has not taken the drug in a large enough dose to be detected,
- has not taken the drug recently enough to be detected,
- has had the sample tampered with, and / or
- has had a false negative test result occur.[700]

Neither a positive nor a negative test result alone can determine whether or not a person is actually impaired.

How does the new saliva drug testing work?

Some employers have switched from using urinalysis to a saliva tests to test for drug use. Saliva tests have become popular with employers because they are not prone to tampering in the same way urine samples are and they show current impairment. The procedure is also much less invasive and the collection of saliva is easier and safer than collecting urine. The procedure involves using a buccal swab the size of a toothbrush head to collect saliva from a person's mouth. The swab is placed between the cheek and gums for approximately two minutes. Once the swab is saturated it is placed in a collection vial. Many of the most commonly abused drugs can be detected in saliva such as marijuana, THC (Tetrahydrocannabinol), heroin, cocaine and amphetamines. A saliva test can only detect recent drug use and not historical drug. Drugs are only found in a person's saliva for 12-24 hours so the test is not useful for detecting if an employee was impaired a week ago while on the job.

[699] Privacy Commissioner, at 12.
[700] Privacy Commissioner, at 12.

5.1 DRUG TESTING BY THE GOVERNMENT

Who might be affected by government drug testing?

Drug testing programs for government clients may affect such people as government employees, parolees, inmates, public assistance applicants, students on scholarships, and athletes.[701]

5.1.1 Government Employee Drug Testing (EDT) in the Workplace

Are there any laws that pertain to government drug testing programs?

There are three areas of legislation that may have an impact on a drug testing program in a government regulated workplace or program: The *Canadian Charter of Rights and Freedoms ("Charter")*, federal and provincial privacy laws, and federal and provincial human rights legislation.

How does the Canadian Charter of Rights and Freedoms *apply to drug testing?*

The *Charter* applies to both federally and provincially run workplaces and programs. The *Charter* protects such rights as

- the right to life, liberty and security of the person and
- the right to be free from unreasonable searches and seizures,

which are possible grounds on which to challenge the constitutional validity of a government workplace, or legally required, drug testing program.

However, even if the drug testing program does violate an individual's *Charter* rights, it still may be found to be justified if it passes a well-defined test.[702] In this test, the court considers if the program is sufficiently tailored to help achieve a pressing and substantial objective, if the program impacts the individual's constitutional right as little as possible, and if the effects created are in proportion to the benefits of the program. If the program fails any one of these considerations, the program's violation of the *Charter* is said to not be justified. But if the program passes all the steps in this test, the drug testing program is said to infringe on a *Charter* right but is "saved" or allowed because this particular infringement is legally justified in a free and democratic society.

---

[701] Privacy Commissioner, at 10.
[702] *R v Oakes* (1982), 38 Ontario Reports (2d) 598 (Ont Prov Ct) affirmed (1983), 40 Ontario Reports (2d) 660 (ONCA) affirmed (1986), 50 Criminal Reports (3d) 1 (SCC).

Is the Charter *useful in challenging the validity of a drug testing program?*

Charter section 8, the right to be free from unreasonable search and seizure, would probably provide the strongest basis for a challenge to a drug testing program in a government run workplace or a drug testing program put in place to comply with government regulations. The urinalysis usually used in employee drug testing involves taking a sample of bodily fluids and this has been consistently held, in the context of criminal law, to be a search and seizure. Overall, the claimant would have to show that the specific drug testing program involved a state-controlled worksite or state required drug test, that the sampling process was a search and seizure, that they had a reasonable expectation of privacy, and that the search or seizure was unreasonable. It is important to remember, however, that in some safety-sensitive jobs, like that of an airline pilot, an employee's reasonable expectation of privacy may be greatly lessened by the over-riding interest of public safety.[703]

How does privacy legislation apply to government regulated workplaces?

Although drug testing is not addressed directly in the federal or any of the existing provincial *Privacy Acts,* these may indirectly impact on the gathering and treatment of the personal information collected through a drug testing program. For example, the federal *Privacy Act*,[704] imposes codes of "fair information practices" on the federal government by regulating what personal information it can collect, what uses it may make of the information, and to whom it can disclose the information. This Act applies to approximately 160 federal institutions. Although the act applies only to "personal information," once a urine, hair or other sample is taken from a person and identified as belonging to that person (labeling the container it is in), it becomes personal information. In the area of drug testing, the Act applies to the following personal information:

- any information that suggests the reason for the testing,
- the fact the test was done,
- the test results, and
- any other information associated with the testing, such as medical or physical conditions, medications or substances used by the person that may influence the test results.

[703] B. Hovius, S.J. Usprich and R.M. Solomon "Employee Drug Testing And The Charter" (1994) 2 Canadian Labour Law Journal 345 at 372-373 (hereinafter Hovius, Usprich and Solomon).
[704] *Privacy Act*, Revised Statutes of Canada 1985, chapter P-21 (hereinafter *Privacy Act*).

When can a federally regulated institution perform drug testing?

A federally regulated institution that wants to implement a drug testing program must also comply with the Act's requirement that no personal information is to be collected unless:

> 1) the collection is part of an activity or program that is within the statutory goal of the institution, and
>
> 2) the collection is a necessary part of the program or activity.[705]

Even if you consent, the drug testing will not be valid unless these two conditions are met. An institution may want the additional safeguard of getting Parliament's approval for a particular form of collecting information, especially for a highly intrusive form like urinalysis. Without this additional authority, determining whether or not a drug testing program complies with these two requirements is more difficult. In these cases, one must turn to the necessity principle and must weigh the public interest in collection against the privacy intrusion involved.[706] The desire(s) to improve efficiency, improve economy, reduce the demand for illicit drugs, and comply with foreign testing requirements are not by themselves good enough reasons to allow drug testing.

What does the Federal Privacy Commissioner say about drug testing?

In 1990, the Privacy Commissioner of Canada reported that a drug testing program may be legally justified under the federal *Privacy Act* if the following conditions are met:

- there are reasonable grounds to believe the use of drugs is significantly prevalent in a group or by an individual,
- the drug use poses a substantial threat to safety and drug testing will significantly reduce the threat,
- the individual / group cannot be adequately supervised in other ways,
- there are reasonable grounds to believe that drug testing can significantly reduce the risk to safety, and
- there are no practical, less intrusive alternatives such as having a regular medical, receiving education or counseling, or some combination of these that would reduce the risk.[707]

---

[705] *Privacy Act*, section 4.
[706] Privacy Commissioner, at 22.
[707] Privacy Commissioner, at 23-25.

How are federally regulated agencies supposed to collect private information from me?

The federal *Privacy Act* imposes the duty to collect information directly and to inform the person about the purpose for the collection.[708] There are four *exceptions* to these two requirements:

> 1) when direct collection is not possible,
>
> 2) when the person being sampled authorizes another form of collection,
>
> 3) when the personal information may be disclosed to another institution under subsection 8(2) for the purpose of enforcing any law of Canada or a province or in carrying out a lawful investigation, as long as the request specifies the purpose and describes the information to be disclosed, or
>
> 4) when direct collection would result in getting inaccurate information, would defeat the purpose, or prejudice the use for which the information is collected.

How does drug testing fit with the rules regarding information collection?

If the collection of drug testing information is a necessary part of a program and the test-subject truly volunteers to be tested, then the testing is a direct collection under the federal *Privacy Act*. A mandatory drug testing program, however, is considered to be an indirect collection and to be permitted it must satisfy one of the above four exceptions. When information is collected indirectly there is no duty to inform the person of the purpose for the collection. However, it is common policy for the government to do so.

How long can the government keep my personal (drug test) information?

Under the Privacy Regulations, personal information must be retained for a minimum period of two years. The appropriate maximum period may vary from case to case. The Privacy Regulations also impose a duty to dispose of personal information in accordance with guidelines used by the designated Minister.[709]

Where is the federal government currently performing drug testing?

In federal government regulated sites, drug testing is currently being carried out in such areas as Correctional Service of Canada, the Department of National Defense, Transport Canada, National Parole Board, and Sport Canada,[710] and are not necessarily aimed at employees.

---

[708] *Privacy Act,* section 5.
[709] *Privacy Regulations* SOR/83-508, section 7.
[710] Privacy Commissioner, at 38-45.

What about provincial government drug testing?

Alberta has similar privacy legislation governing provincial workplaces.

For a discussion of the rules and duties regarding privacy in government workplaces see Chapter 1: Privacy Protection and the Government, Chapter 3: Surveillance and Chapter 4: Searches.

What role does human rights legislation play in government regulated workplaces or programs?

A third area of legislation which applies to government regulated workplaces or programs, as well as private sector workplaces, is human rights legislation as discussed below under 5.15.

5.1.2 DRUG TESTING IN THE CRIMINAL CONTEXT

When can drug use result in criminal charges and conviction?

The existing criminal law does not punish people for simply using an illicit drug. The law focuses on the possession, trafficking, cultivating or manufacturing of a drug, but none of these things can be proved by a positive drug test result. The use of a drug in combination with some activities, however, can be a criminal offence. For example, driving, flying or boating while impaired (by use of a drug or otherwise) are all criminal offences.[711]

Why do the police use breathalyzer tests?

The breathalyzer test, which is referred to in the *Criminal Code*,[712] detects the presence and concentration of alcohol in the breath, and this is related to the blood alcohol levels in the body. Having the care or control of a vehicle when you have a blood alcohol concentration over a particular level is illegal, but this is a type of impairment which is presumed in law, not one confirmed by scientific evidence.[713] Currently the legal limit as set out in Canada's *Criminal Code* is eighty milligrams of alcohol in one hundred millilitres of blood. Breathalyzer tests cannot identify the use of or impairment by other drugs. If because of some physical condition, like unconsciousness, a person is unable to give a breath sample, then blood samples might be taken to determine the person's blood alcohol level if the qualified medical technician taking the samples is satisfied that the taking of the samples would not endanger the health of the person.[714]

---

[711] Privacy Commissioner at 13.
[712] *Canadian Criminal Code*, Revised Statutes of Canada 1985, chapter C-46, section 254.
[713] Privacy Commissioner, at 45.
[714] James A. Fontana *The Law of Search and Seizure in Canada* Fourth Edition (Toronto: Butterworths, 1997) at 456.

A roadside "Alert" breath test is not an official breath sample; it is a screening test. The police cannot use the roadside breath sample as evidence against you in court. It simply indicates that you might have drank more than the legal limit of alcohol which gives the police more reason to believe that the more formal breathalyzer test should be done.

Why else would the police want to collect samples from my body?

Aside from the testing for "legal limit impairment" by alcohol, many of the bodily samples collected under *Criminal Code* authority are collected for DNA analysis, not drug use. The Canadian criminal courts have consistently held that the taking of samples of bodily fluids, like blood, urine or saliva, are searches and seizures in the area of criminal law enforcement[715] and, as such, require a warrant to collect.

For more information on police searches and seizures see Chapter 4: Searches and for more information on forensic DNA testing see Chapter 6: Genetic Testing.

5.1.3 DRUG TESTING OF INMATES

Why do prisons have drug testing programs?

Drugs are a persistent problem in prisons. Not only do prisons house a large number of drug traffickers who already have established networks of supply, but there are many drug users in prisons. According to a research paper published by Correctional Services of Canada in 2004, about 80 percent of offenders admitted to federal corrections have substance abuse problems.[716] Prisons also house a large number of inmates who are prone to violence.

What are the possible benefits of a drug testing program in prisons?

Drug testing in prison could help to:

- reduce the demand for drugs in the prison system,
- reduce the pressure on inmates to bring drugs back into prison when they are returning from community programs or leave,
- reduce the pressure on visiting family members to bring drugs into prison,

[715] Hovius, Usprich and Solomon, at 365.
[716] See: Use of Random Urinalysis to Deter Drug Use in Prison: A Review of the Issues; available at http://www.csc-scc.gc.ca/text/rsrch/reports/r149/r149-eng.shtml

- reduce the extent that property and sexual favors are exchanged for drugs,
- remove the practices of frisk-searching visitors or restricting the closeness of the visitors,
- reduce the violence associated with the prison drug market,
- identify those who need treatment, and
- ensure that Correctional Services of Canada offers inmates and staff a safe place in which to live or work.[717]

What is the legal history of drug testing programs in Canadian prisons?

In 1985, the Penitentiary Service Regulations were amended to give Correctional Services of Canada the authority to conduct "for cause" urine tests.[718] Urinalysis could be ordered on an inmate if a member of Correctional Services felt it was necessary in order to confirm their suspicion that an inmate had taken an intoxicating substance. Inmates who either refused to give a sample or tested positive for an intoxicant faced discipline.

In 1990, the Federal Court of Canada reviewed this particular drug testing program to see if it violated the *Charter*.[719] Although the court was presented with clear evidence of the general effects of drug use and the limited expectation of privacy that an inmate has in a prison setting, the court found that the random testing involved in this program violated sections 7 and 8 of the *Charter* and was not saved or justified in these particular circumstances. The court said that although there was reported to be substantial drug use in prisons and that the trade in drugs in prisons was said to fuel the violence and coercion associated with a prison's atmosphere, there was no firm, conclusive evidence that the drug use or impairment posed a substantial threat to the safety of prisoners, prison staff or the public, nor that testing could significantly reduce the risk to safety in a way that adequate supervision of prisoners could. The interference with the prisoner's bodily integrity and the potential for abuse outweighed the government's interest in controlling the drug problem in prisons. The court found that the legal authority for this program was invalid.

At the time, this Canadian court's decision ran contrary to similar cases decided in the American courts, where drug testing was not seen as violating a prisoner's constitutional rights and where it

[717] Privacy Commissioner, at 61.
[718] *Penitentiary Service Regulations* sections 39(i.1) and 41.1. These have been repealed and replaced with *Corrections and Conditional Release Regulations* SOR/92-620 (1992) section 60.
[719] *Jackson v Joyceville Penitentiary* (1990), 75 Criminal Reports (3d) 174 (FCTD).

was not even necessary to have reasonable and probable grounds for ordering a particular inmate to submit a urine sample.[720]

Can Canadian prisoners be tested for drugs?

Today, the *Corrections and Conditional Release Act*[721] authorizes Correctional Services of Canada to establish a random selection urinalysis program to screen inmates for uses of intoxicating substances.[722] The scope of "intoxicants" screened for could include any substance which if taken has the potential to impair or alter the person's judgment, behaviour or the capability to recognize reality or meet the ordinary demands of life, but does not include caffeine or nicotine.[723] Regulations passed under the Act provide the authority for Correctional Services to collect this type of information, to ensure security of the penitentiary and the safety of persons, using a urinalysis program based on random selection.[724] Random selection is defined as a procedure that ensures that every inmate has an equal chance or probability of being selected on a periodic basis.[725] Who is to be selected to provide a urine sample is not to be influenced by human opinion or subjectivity.

What if a prisoner refuses to provide a urine sample?

The Act makes it a disciplinary offence for refusing to provide a urine sample when demanded or for having a positive test result. It allows the head of the prison to designate these as either minor or serious offences.[726] If an inmate is found guilty of a serious offence the maximum penalty is for them to be put in segregation for a period of up to 30 days.[727]

When does Correctional Services Canada currently require drug testing?

Correctional Services Canada presently performs drug testing when:

- there is individualized suspicion—where it is reasonably suspected that an inmate is actually using drugs,
- it is a pre-condition for access to a community program if an inmate has a history of drug use, and

[720] Lanyon and Brown, at 15.
[721] *Corrections and Conditional Release Act*, Statutes of Canada 1992, chapter 20 (hereinafter *Corrections Act*).
[722] *Corrections Act*, section 54(b).
[723] *Corrections Act*, section 2(1).
[724] *Corrections Act*, section 54(b).
[725] *Corrections and Conditional Release Regulations* SOR 92/620, section 60.
[726] *Corrections Act*, section 41(2).
[727] *Corrections Act*, section 44(1)(f).

- it receives a request from the National Parole Board to do so on a parolee whose file has a drug testing condition in it or when this becomes an added condition of his or her release.[728]

5.1.4 DRUG TESTING PAROLEES

When can the National Parole Board (NPB) perform drug testing on parolees?

The NPB gets its authority for monitoring parolees, who are inmates who were incarcerated in federal prisons, from the *Corrections and Conditional Release Act*. The NPB's monitoring program can include periodic urinalysis on parolees only when:

- it is deemed necessary in order to reduce or manage the risk that the offender would otherwise represent, and
- drug testing is the least restrictive measure available.

Drug testing under the NPB's monitoring program is not random. The introduction of a drug testing condition on a parolee's file must be based on evidence that supports a reasonable belief that the parolee's history of substance abuse, which has been linked to a past offence, may continue without this special monitoring.

[728] Privacy Commissioner, at 61.

Once a parolee has a drug testing condition on their file, who determines when and where a parolee is tested for drugs?

After the NPB has made drug testing a condition for a particular parolee, it is left to the parolee's Parole Officer to determine the number and timing of drug tests necessary for effective monitoring. Parolees whose urine samples test positive may have their parole revoked.

5.2 DRUG TESTING IN THE PRIVATE SECTOR

5.2.1 Employment

Can an employer demand its employees or job applicants take a drug test?

The main question in this area is whether or not employers can demand bodily fluid samples from their employees or job applicants for drug testing, when these materials could also show such conditions as HIV, the presence of a cancer gene or pregnancy. The answer to this question is largely dependent on the particular workplace, and is decided on a case by case basis, taking into account such factors as:

1) whether the workplace is federally or provincial regulated, which in turn will determine which level of government legislation may impact on it;
2) whether the employer is from the private or public sector, as there are differing privacy laws applicable to either the government or the private sector and
3) whether the employees are unionized or non-unionized, for if the employment contract for a position is regulated by a contract that a union has negotiated, this comprehensive agreement will impact on both parties' expectations and actions.

Why would employers want to have a drug testing program?

While drug testing is far less expensive than it used to be, it is still very expensive for a large organization to use such a program. Implementing a drug testing program, therefore, is a business decision, motivated by more than an employer's passing curiosity in the lives of its employees. Some of the justifications employers give for implementing a drug testing program are:

- ***Employer duties:*** this includes maintaining a safe work environment for all employees and the public, as required by occupational health and safety and occupier's legislation.[729]
- ***Employer liability:*** employers may be held legally responsible for the actions of their employees while they are performing their job duties. Because drug and alcohol use can increase the likelihood of an employee having or creating an accident for which the employer will be liable, drug testing can be an efficient way of limiting the damage for which an employer might be vicariously liable. Increasingly, insurers are including blanket exemption clauses in their insurance policies so that insurance companies do not have to pay out if alcohol or drug use were associated with the accident.[730]
- ***Business efficiency interests:*** it is believed that drug use increases the likelihood of absenteeism, property damage, and poor morale from the general frustration of the organization tolerating the loss of productivity in a drug user. Persons who possess or sell illicit drugs are breaking the law. If employees break the law in this manner, employers may believe that they will break the law in other circumstances too. Employees may feel forced to commit crimes, including work-related crimes, to ensure they can afford to continue their drug use.[731]
- ***Employer policing:*** there is a persistent need to reduce the demand for illicit drugs and to reduce the health care costs associated with treating the ill effects of drug use. Drug testing for illicit drugs serves as a deterrent to illicit drug use, if the consequence of a positive test is the refusal or termination of employment.[732]
- ***Harmonization with requirements established by other countries:*** the United States government and private sector have both strongly supported testing for illicit drug use. These American programs reach into Canada through American transportation regulations and the implementation of the drug testing policies of American parent companies in their Canadian based offices.[733]

---

[729] Douglas Isbister, "Justifying Employee Drug Testing: Privacy Rights Versus Business Interests" (1996) 5 Dalhousie Journal of Legal Studies 255 at 266 (hereinafter Isbister).
[730] Isbister, at 267.
[731] Isbister, at 268.
[732] Weir, at 457-458.
[733] Privacy Commissioner, at 8.

- ***Drug use rehabilitation:*** if it is used to monitor a person's compliance with a drug treatment program, drug testing can be a useful tool in the rehabilitation of a person who abuses drugs or alcohol.[734]

Because an employer and employee enter into an employment relationship voluntarily, the employer is justified in considering factors beyond public safety when deciding whether or not to use an employee drug testing program. As already shown, an employer can have many good business reasons for using a drug testing program.

Why might employees be concerned about drug testing?

Employees generally accept that an employer may have a right to know if an employee is impaired at work, but they don't like random drug testing being used as the way of identifying these occurrences. Some of the main concerns employees have about employee drug testing programs, and urinalysis in particular, are:

- ***Inadequate legal protections:*** drug testing procedures in the workplace may leave employees with less rights protection than a member of the public suspected of a similar offence. Criminal law has rules which protect the individual's rights, such as a presumption of innocence, the guarantee of a hearing where collected evidence is presented by two separate sides, rules regarding searches and seizures, and state-imposed guidelines for penalties. The same cannot be said for employment law.[735]
- ***Mass punishment:*** the privacy rights of all workers should not be compromised in order to deal with the performance problems of a small minority of the workers.[736] Urinalysis can tell you a great deal about a person's lifestyle, but it tells you virtually nothing about an employee's ability to do his or her job.[737] If recreational drug use causes no ill effects at work and does not impair productivity, it gives no basis for punishing the employee.[738]
- ***Substitution effect:*** once aware that a specific drug is being screened for, a drug user may switch to an equally harmful drug that is not being tested for.[739]

---

[734] Weir, at 455.
[735] Weir, at 457.
[736] Weir, at 451.
[737] Cavoukian, at 121.
[738] Lanyon and Brown, at 16.
[739] Privacy Commissioner, at 18.

- ***Discrimination:*** drug tests cannot establish whether someone is impaired. To fire employees who test positive for drugs is discriminatory and may overlook those who are truly impaired due to other factors like inadequate sleep or poor nutrition.
- ***Creation of unemployables:*** when used as a method of screening out job applicants, pre-employment drug testing creates a class of unemployables who may be qualified and capable workers but are denied employment because of their lifestyle choices during their leisure time.
- ***Unreliable information:*** there is a high rate of error in urinalysis results. Drug testing is dull, repetitive work which requires highly skilled technicians with acute attention to detail and process, which make ideal conditions for human errors. There are also the errors due to the test's inability to consistently distinguish between some illicit and non-illicit substances.[740]
- ***Drug use as a scapegoat:*** by focusing on drug use, employers may overlook other causes of accidents.[741] For instance, the notion persists that Alberta's Hinton train disaster was caused by drug impairment even though the inquiry determined that the human causal factor was created by the train crew's pattern of working an exhausting and unrestricted number of hours.[742]
- ***Insufficient evidence of relevance:*** there is a lack of sound evidence that drug testing actually enhances workplace safety.[743] From 1979 to 1983, Alberta tracked workplace fatalities for drug involvement and performed toxicology tests on 254 of the 399 victims.[744] Six showed traces of marijuana, 23 showed they were using prescription drugs, 36 had traces of various other illicit drugs and 54 showed evidence of alcohol, 12 of which were over the legal alcohol limit. Only in the alcohol related cases was there some inference that the substance found may have been a contributing cause to the fatality. There was no evidence of a causal connection between other types of drug impairment and the causes of the fatalities.

---

[740] Erin Shaw, John Westwood and Russell Wodell, *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How To Protect Them* (Vancouver : B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association, 1994) at 130 (hereinafter Shaw, Westwood and Wodell).
[741] Privacy Commissioner, at 19.
[742] Weir, at 456.
[743] Bruce Phillips, "Privacy In A 'Surveillance Society" (1997) 46 University of New Brunswick Law Journal 127 at 131.
[744] Weir, at 456.

- ***Timeliness:*** urinalysis test results are not available quickly enough to have the impaired and dangerous employee immediately removed from the worksite.
- ***More appropriate alternatives****:* there are less intrusive alternatives that can more effectively deal with the conditions that cause harmful levels of drug use include having supervisors who are properly trained to detect and handle impaired employees, peer intervention programs, and comprehensive employee health assistance and education programs.

When might drug testing be appropriate in the workplace?

Drug testing may be appropriate for safety sensitive positions like airline pilots and train engineers, but these employees are in exceptional jobs that are not similar to the work lives of most of us.[745]

What are some other consequences of workplace drug testing?

The invasion of one's medical, genetic, and off hour recreational privacy are very serious consequences of workplace drug testing. Employees do not want these intrusions thrust upon them because of the behaviour of a few individuals in the workplace. Often there is not even a rational connection between the methods of drug testing, like urinalysis, and the information sought about impairment. From an employee's perspective, widespread mistrust and monitoring through employee drug testing is not the best answer or even a good solution to detecting and reducing impairment in most workplaces.

Why should I be concerned about drug testing, if I have nothing to hide?

Drug testing not only repeatedly violates your right to protection against physical intrusion and your right to control the kind and amount of personal information that you want to share, but also threatens to create an "automatic docility," or complacency about these intrusions. Drug testing is having one's body used against oneself, and there is no greater invasion of privacy. If people are willing to tolerate the requirement to surrender samples of their bodily fluids, how can they later claim that they have any real interest in their other forms of privacy? Submission to repeated testing is like a training procedure that generates the acceptance of unacceptable intrusions, while not addressing the social or worksite problems leading to substance use and abuse.[746]

Are there different times an employer might use drug testing in a workplace?

[745] David Flaherty, "Workplace Surveillance: The Emerging Reality" (1992) Labour Arbitration Yearbook 189-192 (hereinafter Flaherty).
[746] Oscapella, at 342.

Please see the chart below for the types of testing and the corresponding law surrounding that particular type of testing.

DRUG/ALCOHOL TESTING IN THE WORKPLACE	
***Please Note**: The information below is a general overview of the law as it currently applies. For unionized employees the first place to look is in the collective agreement between the employer and the union. It will outline the drug/alcohol policy in place. Because each policy is different it is important to study the policy carefully to assess its reasonableness in light of the employee's position (whether it is a safety-sensitive position or not) and any other problems unique to the workplace (such as prolonged or widespread drug/alcohol abuse by employees).	
Type of Testing	Law
Pre-employment Testing	**Alberta**: Pre-employment drug testing/alcohol testing for safety-sensitive positions are justified for safety reasons (it is not *prima facie* discriminatory and does not treat all future employees as addicts). If the person tests positive and is an addicted to alcohol or drugs they will be covered under human rights legislation. This means the employer must accommodate the person to the point of undue hardship. If the person tests positive and is a casual user they are not considered to have a disability and thus are not covered under human rights legislation so no accommodation is required by the employer.[747] Alberta is the first province where a Court has explicitly recognized an employer's right to impose pre-employment drug testing in safety sensitive positions.[748]

[747] *Alberta (Human Rights and Citizenship Commission) v Kellogg Brown & Root (Canada) Co.,* 2007 ABCA 426.
[748] William Hlibchuk, Emily Sternberg and Anouk Violette, *Drug and Alcohol Testing by Employers in Canada – A legal pulse check,* May 2008 Focus Ogilvy Renault LLP Focus on Ontario Employment and Labour.

	Ontario & Quebec: Pre-employment drug testing/alcohol testing even for safety sensitive positions are a violation of human rights (and are *prima facie* discriminatory).[749] **Ontario**: However, in certain unique safety-sensitive circumstances, pre-employment alcohol testing may be found to be reasonably necessary as a *bone fide* occupational requirement.[750] Employers should be extremely cautious before adopting such policies, and ensure that they consider whether they pass the reasonable necessity test given their unique circumstances, and they have appropriate procedures and policies in place to accommodate the employee to the point of undue hardship if they fail the pre-employment test.[751] Under the Canadian Human Rights Commission Policy on Alcohol and Drug Testing, pre-employment drug and alcohol testing is permitted, but only in limited circumstances.[752] <u>Important to any kind of testing</u>: if an individual tests positive it is important to find out if the individual is disabled due to addiction (substance abuser) or if the employer perceives the individual as disabled due to drug use (substance abuser/casual user) (Does the employer's policy treat all those that test positive as substance abusers or does it distinguish between those who are addicted and those who are casual users?). If the individual is disabled or the employer perceives the individual to be disabled due to drug use (because of either dependency or casual use) the individual must be accommodated by the employer in the workplace, unless the

[749] *Entrop v Imperial Oil Limited,* 2000 ONCA, 50 O.R. (3d) 18; *Communications, Energy & Paperworkers Union of Canada, Local 900 v Imperial Oil* (2006) 157 L.A.C. (4th) 225.
[750] *Entrop v Imperial Oil Limited,* 2000 ONCA, 50 O.R. (3d) 18; *Communications, Energy & Paperworkers Union of Canada, Local 900 v Imperial Oil* (2006) 157 L.A.C. (4th) 225.
[751] Brian Thiessen, *Canada: Drug and Alcohol Testing In the Workplace,* Originally published in Blakes Bulletin on Labour and Employment, August 2007, Blake Cassels & Graydon LLP.
[752] Canadian Human Rights Commission Policy on Alcohol and Drug Testing 2009, http://publications.gc.ca/ccdp-chrc/HR4-6-2009E.pdf.

	employer can demonstrate it is not possible without causing undue hardship.[753] If there is no disability or no perception of disability accommodation is not required.
Random Testing	**Ontario & Quebec**: Random drug testing of employees in safety sensitive positions is not permissible and will not be considered a bona fide occupational requirement.[754] In earlier caselaw, drug testing was not permitted because it didn't allow for detection of current impairment, but was limited to previous impairment. New saliva tests have been able to prove current impairment, but their validity has not been challenged against the *Ontario Human Rights Code* (OHRC). Presently saliva tests have been challenged against a collective agreement with greater protections than the OHRC and held to violate the collective agreement.[755] **Ontario**: Random alcohol testing of employees in safety sensitive positions may be permissible (if part of a bona fide occupational requirement).[756] **Quebec**: Random alcohol testing of employees in safety sensitive positions is not permissible.[757] **Alberta**: Random drug/alcohol testing is permitted so long as the policy is not *prima facie* discriminatory.[758]

[753] *Weyerhaeuser Co. (c.o.b. Trus Joist) v Ontario (Human Rights Commission)*, [2007] OJ No. 640.
[754] *Greater Toronto Airports Authority v Public Service Alliance of Canada, Local 0004* [2007] CLAD No. 243. and *Section locale 143 du Syndicat canadien des communications, de l'energie et du papier v Goodyear Canada Inc*. 2007 QCCA 1686.
[755] *Imperial Oil Ltd. v Communications*, Energy and Paperworkers Union of Canada, Local 900, [2008] OJ No. 489
[756] *Greater Toronto Airports Authority v Public Service Alliance of Canada, Local 0004*, [2007] CLADD No. 243.
[757] *Section locale 143 du Syndicat canadien des communications, de l'energie et du papier v Goodyear Canada Inc*. 2007 QCCA 1686.
[758] *Alberta (Human Rights and Citizenship Commission) v Kellogg Brown & Root (Canada) Co*. 2007 ABCA 426.

Post-Incident Testing	Post incident, near miss, or "reasonable cause" testing for either alcohol or drugs is acceptable, especially in a safety-sensitive environment, so long as it is one facet of a larger assessment of drug and alcohol abuse and the employer meets its duty to accommodate by offering supporting treatment or a rehabilitative program.[759]
Post-Reinstatement (Rehabilitation) Testing	Post-rehabilitation testing must be just one facet of the larger process of assessment for positions in which testing to ensure safety standards are met can be considered a bona fide Occupational Requirement for the position.
Pre-Access Testing	Pre-access testing is when an employer tests employees for alcohol/drugs before they are allowed onto the work site. In Alberta, the Alberta Court of the Queen's Bench has held in a recent case that pre-employment and pre-access alcohol and drug testing is consistent with the Canada Model S. 4.7 so long as the testing is mandatory and universal (not random).[760]

Does the type of work I do affect whether my employer can require drug and alcohol testing?

Yes. Jobs that are considered "safety sensitive" require a higher level of concentration and can lead to large and potentially dangerous accidents if performed under the influence of alcohol or drugs.

What is the Definition of "Safety Sensitive"? Safety sensitive positions can be defined as those having: "a key and direct role in an operation where impaired performance could result in a catastrophic incident affecting the health or safety of employees, sales associates, contractors, customs, the public or the environment; and, having no direct or very limited supervision available to provide frequent operational checks."[761] Factors that are often assessed when determining whether a position can be considered as safety sensitive are things such as the work of the employee, the nature of the equipment he or she operates, and the nature of the material he or she handles.

[759] *Entrop v Imperial Oil Limited,* 2000 ONCA, 50 OR (3d) 18.
[760] *United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada, Local 488 v Bantrel Constructors Co.,* 2007 ABQB 721.
[761] *Entrop v Imperial Oil Limited,* 2000 ONCA, 50 O.R. (3d) 18.

Are there any laws dealing with drug testing in private sector workplaces?

There are no federal or provincial Canadian laws which specifically prohibit drug testing in private sector workplaces. Likewise, there is no legislation which promotes or permits drug testing. But in the absence of a prohibition, it would appear that drug testing in the private sector is allowable. There has been case law to provide guidance in this area, but it has been very situation specific and can be different depending on the province as seen in the table above. This provincial difference has meant that in general, employees' privacy rights are afforded greater protection in Ontario and Quebec than in Alberta. However, there are many factors involved in determining whether the type of testing is allowed such as:

- When the testing took place (pre-employment, randomly, post-incident etc.)
- Why the testing took place (an incident occurred, an employee's performance was inadequate etc.)
- The nature of work (safety-sensitive or non-sensitive)
- Whether the workplace is unionized or not
- The type of policy in place (does it allow for accommodation in the event of a positive test?) and whether or not the union has agreed to it if applicable
- Whether the employment sector is federally or provincially regulated.[762]

Is the caselaw the same in each province or are there different rules for drug testing across the country?

As seen in the chart above the case law surrounding drug/alcohol testing in Canada is not consistent across the country. There are important differences between Ontario/Quebec and Alberta with respect to pre-employment and random drug testing. In Alberta, pre-employment drug testing is not considered to be initially discriminatory like it is in Ontario/Quebec. An Arbitration Board or court will look into the pre-employment testing process to determine whether it is discriminatory. In Ontario/Quebec because pre-employment drug testing is always considered discriminatory, it violates a person's human rights and is generally prohibited. In Ontario there has been an exception made for positions that are safety-sensitive and require US drug policies to be met, such as for international truckers. Random testing for either drugs or alcohol is prohibited in Quebec. In Ontario it is not prohibited for drug or alcohol testing when the employee is in a safety sensitive position. In

[762] Flaherty, at 143.

Alberta, random drug and alcohol testing are permitted for safety sensitive positions so long as the testing is not itself discriminatory. Because the law is quickly evolving in this area it is important to keep up to date! Possible sources of up to date information on these issues are the provincial and federal Human Rights Commissions.

Has the private sector created a unified policy for employee drug and alcohol testing in Canada?

In Alberta, a group of private sector companies have created **The "Canadian Model" for providing a safe workplace.** The Canadian Model is a best practice alcohol and drug testing policy that all stakeholders within the construction industry across Canada can adopt and follow. It is a volunteer based policy meant to be a guide and does not require specific adherence. The purpose of the Canadian model is to ensure a safe workplace for all workers by reducing the risks associated with the use of drugs and alcohol. The Model is part of an overall approach to safety and is intended to be an integral part of a safety or loss management strategy. The Model outlines guiding principles, alcohol and drug guidelines, and establishes a minimum industry standard for a safe workplace and includes provisions for site access and random testing for those companies that wish to adopt those practices based on the specific needs of the their business.[763] The model is a valuable resource for both employers and employees because it also includes reference material such as frequently asked questions, an alcohol and drug awareness guide for employers, supervisors and employees, as well as independent legal and medical opinions on the law surrounding drug and alcohol testing, the effects of drugs and alcohol and the effectiveness of drug and alcohol tests.

Could an employee rely on the Charter *for some protection from drug testing?*

The *Charter* could indirectly affect a private sector employer's drug testing program if the program was being used to help comply with a government regulation, like airline pilots and train engineers being virtually drug free. In these situations, the argument could be made that mandatory drug testing is a violation of *liberty* and *security of the person* as well as being an unreasonable search and seizure. But even if the program was found to violate an individual's *Charter* rights, it could still be judged to be reasonable if the interests of society in general are found to outweigh the interests of the individual. To determine if the violation created by the drug testing program was justified, the court applies a test to ensure the program is not arbitrary but tailored to the pressing

[763] Canadian Model for Providing a Safe Workplace: Version 6.0, July 2018.

and substantial goal being sought, that the program impairs the person's right as little as possible, and that the effects created are in proportion to the intended benefits of the program.[764]

How does human rights legislation apply to drug testing in the private sector?

Currently the legislative framework which offers the greatest chance of successfully challenging a drug testing program in the private sector is human rights legislation, which applies directly to both the private and public sectors.

5.2.2 Human Rights Legislation

Human rights legislation applies to both government and private sector workplaces.

Which human rights legislation applies?

Whether it is the federal or provincial human rights legislation which applies to the workplace depends on whether the business is federally or provincial regulated. For example, in Alberta, 80% to 90% of the businesses[765] fall under Alberta's provincial laws,[766] while the others, like CN Rail, Canada Post, federal government departments, airlines, chartered banks, inter-provincial trucking, and broadcasting and telecommunication companies, fall under Canada's federal laws.[767] Federal and provincial human rights laws are similar in that their goals are to protect equality rights by prohibiting discrimination.

How do human rights laws work to protect people from employer drug testing?

The federal and provincial Human Rights *Acts* do not specifically prohibit drug testing. However, "positive" drug test results might be used in ways that are discriminatory, which the *Acts* do not allow. It is discriminatory to fire, or to refuse to hire an individual on the basis of a disability, and for the purposes of the *Acts*, disability includes previous or present dependence on alcohol or a drug. So, if you have been treated differently by your employer (fired, not promoted, transferred) because of a drug dependency, you have probably been discriminated against on the basis of a recognized **disability**. Bodily fluid samples given for drug tests might also reveal personal information about other conditions, such as epilepsy, venereal disease, diabetes and various other mental and physical conditions. If this information is used against you this amounts to discrimination on the basis of

---

[764] Lanyon and Brown, at 15.
[765] Alberta Human Rights and Citizenship Commission "Drug and Alcohol Testing and Human Rights" (2001) web site: http://www.albertahumanrights.ab.ca/publications.asp (hereinafter Alberta Human Rights Drug Policy).
[766] *Alberta Human Rights, Act,* Revised Statutes of Alberta 2000, chapter A-25.5.
[767] *Canadian Human Rights Act*, Revised Statutes of Canada 1985, chapter H-6.

disability. Pregnancy may also show up in some drug tests. The negative use of such a result—such as firing you because you are pregnant—is discrimination on the basis of **gender (sex)**.[768] Since the majority of drug users are between 18 to 29 years of age, drug testing alone might discriminate on the basis of **age**.[769] People who are visible minorities may have higher levels of melanin pigment, and since this is chemically similar to the active ingredient in marijuana it may influence drug testing results.[770] Reliance on such a test result could be discrimination on the basis of a person's **colour**.

Is there difference in law between someone who uses drugs because they are addicted and someone who uses drugs for casual use?

This is largely a question of whether a person can claim accommodation when testing positive for either drugs or alcohol. Under human rights law an addiction to drugs/alcohol is considered a disability or a handicap while casual use is not. When a person has a disability he/she must be accommodated to the point of "undue hardship" by the employer. What is important is whether an employer knows a person is addicted based on testing or whether the employer perceives the person to be addicted even without confirmation. If an employee tests positive because of either casual use or addiction, and the employer believes the positive test is either because of actual or perceived dependency, human rights legislation applies. This would mean that both persons who are addicted to drugs or alcohol and casual users are treated alike. If the employer does not believe the person is addicted and they are found not to be addicted, but rather to be a casual user, they are no longer considered to be covered by human rights legislation and no accommodation is mandatory. Thus, an employer's approach to an employee who is just a casual user, but who tests positive, can impact whether or not they receive accommodation.

What do I do if I think I have been discriminated against on the basis of a drug test?

You could contact the appropriate Commission Office[771] to lay a complaint. The federal and provincial Human Rights Commissions deal with many different types of discrimination complaints in the area of employment, including those based on the grounds of disability, age, gender or colour.

---

[768] Privacy Commissioner, at 66.
[769] Privacy Commissioner, at 66.
[770] Privacy Commissioner, at 66.
[771] Canadian Human Rights Commission, Ste. 308, 10010-106 Street, Edmonton, Alberta T5J 3L2 (780-495-4040). Alberta Human Rights and Citizenship Commission, Northern Regional Office, 800 Standard Life Centre, 1045 Jasper Avenue, Edmonton, Alberta T5J 4R7 (780-427-7661) or Southern Regional Office, Suite 310, 525-11th Avenue S.W., Calgary, Alberta T2R 0C9 (403-297-6571).

The Human Rights Commissions are impartial. They will work for both sides in helping to bring about a fair resolution to a conflict. There is no fee for the Commissions' services and all the information is kept confidential. Someone other than the two parties directly involved may make a complaint on behalf of one of the parties involved, and a complainant may stop the complaint process at any time.

Can the Commission determine that a drug or alcohol testing program is discriminatory?

Yes. The current law on drug and alcohol testing is that random, blanket drug testing of employees or prospective employees is on its face discriminatory, even for safety sensitive positions.[772] On the other hand, a positive breathalyzer test for alcohol shows that the person is currently impaired and is acceptable for safety-sensitive positions. However, requiring disclosure of past substance abuse is discriminatory for current or prospective employees.

Are there any defences available under human rights legislation?

Yes. To defend a program that appears to be discriminatory, an employer must show that the testing is either "for cause" or justifiable in the circumstances.[773] To demonstrate "for cause testing" of an individual employee the employer must have reasonable grounds such as the employee being involved in an accident or evidence of intoxication. Additionally, random drug testing may be justifiable if the employer can demonstrate that there is a generalized problem of drug or alcohol abuse in a particularly dangerous workplace.

Do Provincial Human Rights Commissions have views about drug testing?

Yes. For example, it is the Alberta Human Rights Commission's view that pre-employment drug testing or random drug testing of employees may be a violation of human rights. Drug tests should be given only where there is a reasonable suspicion of an impaired ability to safely and satisfactorily perform job duties.[774] For the view of other particular jurisdictions' human rights commissions, it is recommended that you contact the desired office.

---

[772] *Entrop v Imperial Oil Ltd. (No. 5)* (1995), 23 Canadian Human Rights Reporter D/191, affirmed [1998] OJ No 422 (Ont. Gen Div), varied (2000), 50 Ontario Reports (3d) 18 (ONCA) (hereinafter *Entrop*). See also: *Canada (Canadian Human Rights Commission*) *v Toronto Dominion Bank (re Canadian Civil Liberties Assn.),* [1998] Federal Court Judgments No. 1036 (Fed CA), where the Canadian Human Rights Commission's found that a mandatory drug testing program for all new and returning employees in a bank was discriminatory under human rights legislation. See also: Denise Workun "Alcohol and Drug Testing in the Workplace – Balancing Human Rights and Safety" (2001) 11(1) Health Law Newsletter.
[773] *C.E.P., Local 30 v Irving Pulp & Paper, Ltd*., 2013 SCC 34.
[774] Alberta Human Rights Drug Policy.

Are there limits to the protections provided for in human rights legislation?

Yes. In order to access the protections or remedies in human rights legislation, one must be an employee. Having a job, however, does not necessarily mean that you fit into the definition of an "employee". There are many different employment relationships or arrangements in which a worker might not be legally recognized as an employee for a particular law. It is also possible that a worker's employment relationship with her or his employer might make the worker an employee for the purposes of human rights laws, but will not fit the definition of employee as is used in the *Income Tax Act*. Similarly, the person who the worker complains about being discriminated by must also meet the legal definition of employer in the applicable human rights legislation.

Also, human rights legislation does not specifically deal with privacy protection. It may be said that human rights legislation does provide some degree of privacy protection in an indirect way, such as when a person is discriminated against on the basis of a ground prohibited in the legislation (for example, disability).

5.2.3 Effects of Unionization and Non-Unionization

If I work in a non-unionized workplace, what limits are there on drug testing?

Generally, if a workplace is non-unionized or without a formal, comprehensive agreement of employment conditions, a boss is able to bring drug and alcohol testing into the workplace since at the time of hiring, there was no agreement that he would not change the workplace's working conditions in the future. The boss, however, should give the employees reasonable notice that he will be starting to use testing, so the employees can decide if they want to continue to work under these new job conditions or start looking for other work and quit the job when the testing actually starts. As discussed earlier, this employer will also have to comply with human rights legislation, which will help ensure that the employer is not using the drug testing in a way that is discriminatory. If this employer is the government, then it must also comply with any existing privacy legislation that applies to their particular level of government. Refer to the chart above to see when different types of drug testing are considered to be legitimate uses of testing. It is important for employees who do not work in a safety-sensitive positions to be aware of potential human rights violations when an employer institutes a random drug/alcohol testing policy with no accommodation for positive tests.

If I work in a unionized workplace with a collective agreement do I have to submit to drug testing?

In a unionized workplace where there is a collective agreement— a work contract that a union has negotiated for the employees—the issue of whether or not there will be drug testing may have been negotiated and included in the contract. Most unions are opposed to drug testing in the workplace. Some see this as unions defending the rights of the guilty at the expense of the innocent.[775] Unions, however, argue that those employers who want drug testing are rarely concerned with the root causes of drug abuse, such as occupational stress, and are just preoccupied with controlling individual behaviour and placing fault on individuals rather than on the structure of their work or workplace. Evidence suggests that alcohol is the main cause of concern on worksites, yet most screening programs do not test for this substance and therefore have little value in addressing the most significant substance abuse problem in the workplace. Unions are not prepared to bargain away the privacy of all employees just because of the performance problems of a small group of employees.

What if the union and the employer do not agree about drug testing?

If a conflict arises in a unionized workplace over the use of a new drug testing program, the matter is usually sent to an arbitrator to decide. Arbitrators making these decisions do not follow one public policy on whether or not employee drug testing is appropriate. Each conflict is dealt with as a discrete, private problem between the two parties in a particular workplace. But the arbitrators do have a set of steps they routinely go through to help ensure they have fully considered all sides of the conflict.

What steps will an arbitrator follow to resolve a disagreement about drug testing?

First, an arbitrator will check to see if employee drug testing is expressly or implicitly mentioned in the existing collective agreement or if the employer is implementing it in order to comply with a legal requirement. Second, if drug testing is not mentioned in the contract, then an arbitrator will determine if starting a drug testing program falls within the scope of what is commonly called "Management's Reserve Rights" (management's right to decide the issues that are necessary to run the workplace and that have not already been addressed in the employment contract), by balancing employee privacy with an employer's need to continue to effectively run the enterprise. An employer cannot automatically assume that if something was not mentioned in the collective

[775] Weir, at 452.

agreement, it falls within "Management's Reserved Rights" to decide. Third, if the arbitrator finds that management has the authority to use drug testing, he or she will review the drug testing program to determine if it is fair.[776]

What things will an arbitrator look at in deciding whether a drug testing program is fair?

In coming to a decision, some of the things an arbitrator will look at are:

- if drug testing is inconsistent with the existing employment agreement,
- if drug testing relates to matters that directly pertain to the employment relationship,
- if there is a connection between the new drug testing policy and the efficient operation of the workplace,
- if the drug testing policy intrudes as little as possible while still being effective,
- if the change in the workplace drug testing policy was adequately brought to the employees' attention,
- if the new workplace drug testing policy is consistent with privacy legislation and human rights legislation, and
- if the drug testing policy respects the values in the *Charter*.[777]

So, although the personal or private concerns of employees are not the starting point in reviewing an employer's residual power to run the workplace, employees should get due process and notice.

How binding is the decision of an arbitrator or arbitration board?

The decision of an arbitrator is binding unless quashed by a court. A person/ party who wishes to enforce an arbitration decision can apply to the court for an order to enforce the arbitration. The party/person unsatisfied with the arbitration decision can apply to the court for a judicial review of the decision. If the decision is upheld, the decision will apply as an order of the court. For instance, in February 2018, the Alberta Court of Appeal upheld an injunction of an Alberta Board of Arbitration regarding a grievance filed against Suncor Energy by Unifor Union, Local 707-A, challenging its random drug testing of its employees in safety-sensitive positions at its

[776] Catherine Wedge, "Limitations on Alcohol and Drug Testing In Collective Bargaining Relationships" (1994) 2 Canadian Labour Law Journal 461 at 465 (hereinafter Wedge).
[777] *K.V.P. Co*., as discussed in Allan Barss "Search and Surveillance in the Workplace: The Employee's Perspective" (1992) Labour Arbitration Yearbook 181-187.

Fort McMurray site. The court found the action as a violation of Suncor's collective agreement with the union.

5.2.4 Return to Work and Drug Testing

After my treatment for a drug addiction, can my employer make drug testing a condition of my returning to work?

Yes. A testing program which monitors one's continued abstinence from a substance after one's treatment for a substance abuse problem is called post-rehabilitative testing. Post-rehabilitative testing is merely used to detect drug use, not impairment. A drug test like urinalysis is one such example. If an employee has a confirmed addiction to substances, but wishes to return to a worksite where safety is a concern or where there is access to these types of substances, management has the inherent right to ensure a safe workplace and employee fitness by implementing random urinalysis testing of this returning employee.[778] The addiction, however, must have been a confirmed addiction, not just an admission of repeated drug use at work.[779] The recovering employee has the choice of consenting to the random drug testing or else could be denied access to the workplace and employment there.

5.3 CONCLUSION TO DRUG TESTING

As we have seen, privacy rights are not absolute. An individual's privacy must sometimes yield in order to accommodate other important interests, such as the safety of the public. Drug testing might be an acceptable intrusion on our privacy if the public benefits sufficiently from it. But drug testing is not only about protecting the public; it may also be about a prevailing attitude towards drugs in society that was originally based on misinformation and fear. Drug testing may also be about controlling the lives of others, and our complacent attitude towards technology—unquestioning acceptance of whatever new techniques that technology brings.[780] Some methods of sample collection are as intrusive as those powers that can be exercised by police officers in certain situations, yet those using drug testing programs are not required to follow the same rules and safeguards that the police must adhere to. Except in government institutions that are subject to the data protection and principles such as those contained in the federal *Privacy Act* and the provincial

[778] Wedge, at 481.
[779] *Cominco and United Steelworkers of America, Local 480* (unreported), December 16, 1992 (Williams, Q.C.) as discussed in Wedge.
[780] Oscapella, at 345.

privacy laws,[781] there is virtually no control on the sharing of the information that is generated by drug testing. The person who is tested loses control over what could be highly sensitive information. Even the legislation regulating government institutions is not solid assurance of privacy, as it can be sidestepped by other legislation authorizing drug testing. It is short-sighted to allow drug testing technology to determine the limits of our privacy. Our respect for privacy should limit the uses of drug testing technology.

[781] In Alberta - *Freedom of Information and Protection of Privacy Act* Revised Statutes of Alberta 2000, chapter F-25.

5.4 CASE STUDIES

Imperial Oil Ltd. v Communications, Energy and Paperworkers Union of Canada, Local 900,[782] (2009)

Random employee drug testing.

This was an appeal from the judgment of the Divisional Court dismissing an application for Judicial review of a final arbitral award which held that a random drug testing of certain employees by Imperial Oil Limited ("Imperial") absent a reasonable cause violated the collective agreement between Imperial and its work Union. Imperial introduced an alcohol and drug policy at its worksite at Nanticoke in 1992 at which time no trade union or collective agreement was in place. This policy required a random breathalyzer alcohol testing and random urinalysis testing of the employees in safety sensitive positions.

In 1996, Imperial and the Communications, Energy & Paperworkers Union of Canada, Local 900 (the "Union") entered into a collective agreement. The agreement contained a management clause that gave Imperial the exclusive rights to manage and direct all aspects of the worksite. This clause empowered Imperial to discipline, suspend or terminate the employment of any employee for just cause and to make, enforce and alter work rules among other matters. The policy also provided that the parties jointly commit to a work place environment that is free of harassment and where individuals are treated with respect and dignity.

Imperial's policy was first challenged by an Imperial employee and resulted in a Board of Inquiry hearing. The Board concluded that several aspects of the random alcohol and drug testing provisions of the policy contravened the Human Rights Code. Imperial appealed the decision to the Ontario Division Court: Entrop v Imperial Oil Ltd (1998), and further to the Ontario Court of Appeal: Entrop v Imperial Oil Ltd (2000), where the breathalyzer testing was found reasonable and the urinalysis test found unreasonable. Imperial stopped random urinalysis following this decision, but continued the breathalyzer testing.

Imperial resumed a random drug testing by saliva sampling in 2003 and this led to the Union's grievance and the subsequent challenge of both the saliva testing and the random breathalyzer

[782] *Imperial Oil Ltd. v Communications, Energy and Paperworkers Union of Canada, Local 900,* [2009] OJ No 2037.

testing that remained in place. At the preliminary award hearing, the arbitration panel ruled that the Union had acquiesced the breathalyzer testing as it did not file any grievance concerning the testing until 2003. The Union did not challenge this finding. On the final award, the majority of the arbitration panel found Imperial's policy provisions authorizing random drug testing absent a reasonable cause null and void and in violation of the collective agreement. Imperial appealed for judicial review, (to the Divisional Court), and argued (among other things) that the panel had improperly relied on facts from other proceedings and had failed to apply the collective agreement. The Divisional Court dismissed Imperial's appeal and rejected Imperial's claim that the majority of the arbitration had failed to apply the Collective Agreement resulting in a further appeal. The Ontario Court of Appeal dismissed the appeal, holding that there was no evidence showing that the Arbitration Panel accepted evidence or authorities from the Union and denied Imperial an opportunity. The court also found the that the facts Imperial claimed the panel relied on in reaching its decision came from the jurisprudence submitted by both parties. Finally, the panel did not improperly interpret the collective agreement.

Pereira v Business Depot Ltd. (c.o.b. Staples Business Depot),[783] (2009) British Columbia Supreme Court

Termination of employment during leave of absence for depression and drug addiction

The plaintiff, Mr. Pereira was recruited by the defendant, Staples Business Depot ("Staples") to work in Prince George in 1997. In 2000 Mr. Pereira was promoted to a general manager of a store in Nanaimo and continued to be a good employee who took his responsibilities seriously and was well regarded. Mr. Pereira's professional conduct took a dramatic turn in June 2003. He began showing up late at work, leaving early and sometimes not showing up at all. Mr. Pereira was aware that his conduct was unacceptable and went to his District manager explaining that he felt depressed, very fatigued and unwell. Mr. Pereira took a medical leave of absence and went on short term disability for depression and drug addiction. He attempted to return to work in November 2003 on a graduated return-to work program that he established with his physician. Things went well until the latter part of December 2003 when his matter deteriorated resulting to a further medical leave. At some point he went to Kamloops to stay with a friend whose assistance he hoped will help him take better care of himself. His disability benefit was subsequently converted to a long-term disability benefits. In the summer of 2004, Mr. Pereira learned that he needed to attend a treatment facility to be able to maintain the long-term disability benefits. He tried to withdraw his RRSP monies he had with Staples, but Staples could not assist him and advised him to apply for unemployment benefits. Mr. Pereira later assembled the funds for the treatment facility from other sources and attended a treatment facility (Crossroads) in Kelowna for 28 days. He indicated to Staples soon after his admission that he anticipated returning to his life and job at the conclusion of his stay at the facility. Mr. Pereira's treatment program ended on September 2004 and he returned to his friend's house in Kamloops to pick up a disability cheque he hoped would be waiting for him. He needed funds to travel to and get set for Nanaimo, and Staples was aware of this development. Staples terminated Mr. Pereira's employment on September 27, 2004 on the position that Mr. Pereira abandoned his employment. At the time of termination Mr. Pereira was 38 years old and had worked with Staples for seven years earning $58,000 per year in addition to bonuses and stock options. The issues considered by the court included: whether Mr. Pereira was wrongfully

[783] *Pereira v Business Depot Ltd. (c.o.b. Staples Business Depot)*, [2009] BCJ No. 1731.

dismissed, what would amount to a reasonable notice in his circumstance if found to be wrongfully dismissed, and whether he mitigated his losses.

The court found that Mr. Pereira's employment was wrongfully terminated and that Mr. Pereira's expressed hope or intention to return to work, subject to his physician's agreement, was clear and consistent and that it was unreasonable on an objective basis for Staples to have concluded that he abandoned his employment. On the question of what the appropriate notice period was, the court found that notice is a determination that is decided based on the circumstance of each particular case. The court held that In Mr. Pereira's circumstance, a notice period of 10 months was reasonable and that the plaintiff's health problem and his vulnerability increased the notice from 8 months to 10 months. The Court also found that Mr. Pereira was entitled to the stock option for 6 months beyond the 10 month's notice period and that his physical and mental condition impaired his ability to look for work.

R v Shoker,[784] 2006 (Supreme Court Of Canada)

Collection of Bodily Samples under the *Criminal Code*

The accused, Mr. Shoker, was convicted of breaking and entering a dwelling house with intent to committed sexual assault. A pre-sentencing psychological report prepared for the Mr. Shoker's sentencing showed that he blamed his drug use for his behaviour. The report recommended that the Mr. Shoker undertake random urinalysis to manage his risk to the community. The trial judge sentenced Mr. Shoker to 20 months imprisonment followed by a two-year period of probation. The probation order required Mr. Shoker to absolutely abstain from consuming alcohol and non–prescription narcotics, to attend treatment and counseling as directed by the probation officer, and to submit to urinalysis, blood tests or breathalyzers upon the demand of a peace officer. The order stated that any positive reading would be a breach of the abstention condition. Mr. Shoker appealed his sentence to the British Columbia Court of Appeal (BCCA). In determining the appeal, the BCCA deleted the treatment condition as the Criminal Code *section relevant to treatment conditions required the consent of an offender. The court also noted that the there was no program at the time in British Columbia for curative treatment in relation to alcohol or drug consumption as described in the trial court condition.*

The BCCA also deleted the paragraph of the condition which stipulated that any positive reading will be a breach of the Mr. Shoker conditions and found that the trial judge did not have jurisdiction to make such determination. The BCCA considered whether at law an offender could be required under the terms of a probation order to submit to a demand of a sample of bodily substances, including breath, urine and blood and held that the requirement to provide bodily samples violated section 8 of the Charter *in the absence of a regulatory or statutory framework. The Crown appealed these decisions to the Supreme Court of Canada ("Supreme Court").*

At the Supreme Court, the Crown submitted that the abstention conditions of the section in question, (section 732.1 (3) (c) of the Criminal Code*) were highly desirable for the rehabilitation of Mr. Shoker and the protection of the public. The Crown argued that read together with another section, [section 732.1 (3) (h)], section 732.1(3)(c) authorizes the imposition of random sampling of an*

[784] *R v Shoker,* [2006] SCJ No 44.

offender's bodily substance to ensure compliance with the abstention condition. Mr. Shoker, on the other hand, argued that the power to impose enforcement terms on the abstention condition did not flow from those sections and that if Parliament had intended to authorize the seizure of bodily samples it would have expressly stated so. The Supreme Court rejected the Crown's argument, pointing out that breach of probation is a criminal offence under the Criminal Code, *and, as such, is subject to the usual investigatory techniques and manner of proof required of other criminal offences. It rejected the Crown's further argument, pointing out that the* Criminal Code *sections in question could be read together to authorize the collection of bodily samples. The Court reaffirmed that the seizure of bodily samples is highly intrusive and subject to stringent standards and safeguards to meet constitutional requirements, and was not authorized by the common law power to search incident to arrest. The court concluded that trial judge had no statutory authority for requiring Mr. Shoker to submit bodily samples, and that the enforcement of abstention conditions must be done in accordance with existing investigatory tools. The Supreme Court held that the majority of the Court of Appeal was correct in deleting parts of the trial judge's conditions and dismissed the Crown's appeal.*

CEP Local 30 v Irving Pulp & Paper, 2013 (Supreme Court of Canada)

As part of their employment policy Irving Pulp & Paper implemented a random alcohol testing program for all of their employees. The Union (CEP) brought a grievance with the program through the arbitration system arguing that it was overly-broad and should be struck down. The arbitrator agreed with CEP and dismantled the program. After judicial review the decision of the arbitrator was quashed in the Court of Queen's Bench, which was later upheld by the New Brunswick Court of Appeal. The Union once again appealed to the Supreme Court of Canada which resulted in the arbitrator's decision being restored.

In her decision Justice Abella stated that the appropriate approach to addressing whether a random drug and alcohol testing policy is valid requires recognizing the interest of both the parties and then balancing the two. In order for the interest of the employer to outweigh the privacy interest of the employees the employer must establish actual evidence of a substantial safety problem due to drug or alcohol abuse. In the case at bar, Irving lacked sufficient documentation of alcohol use and impairment within their workplace. Due to this the invasion of the employees privacy rights was not justified.

6.0 INTRODUCTION TO GENETIC TESTING

Information from genetic testing can help identify which people carry genes that are associated with getting certain diseases. Over the last ten years, tremendous advances have been made in this field.[785] In Canada, however, the use of genetic testing is still quite rare.[786] As our knowledge of genetics continues to increase and the cost of testing decreases, there will likely be greater use of genetic testing, especially in areas where the status of a person's health is very important, such as before getting an insurance policy or deciding who to hire for a job. This section looks at the impact genetic testing can have on an individual's privacy and how the current laws do or do not apply to this information.

What is genetic testing?

"Genetic Testing" is a term used to describe many different types of testing. They can be divided into three main categories:[787]

1) **Genetic Screening**: this involves getting a picture of one's genes at a particular time. This picture helps detect a number of gene-related disorders such as adult polycystic kidney disease, fragile X syndrome, sickle cell anemia, cystic fibrosis, and hemophilia. A genetic screening test is a one-time test used to detect a single trait. Genes can mutate or change over time, so a test taken long ago may not show exactly the same results as one's genetic make up today. Genetic Screening is often used to find what is making a person not feel well or to advise people who are thinking of having children.

2) **Genetic Monitoring**: this involves looking at a person's genes regularly to help spot changes, which may have happened from being exposed to things like toxic chemicals, radiation or viruses. To do this, you have to take many genetic tests over a period of time.

---

[785] M. Lombardi, "Genetic Testing: The Coming Consumer Issue" (July/August, 1997) 138 Marketing Options at 1 (hereinafter Lombardi).
[786] E. Shaw, J. Westwood and R. Wodell, *The Privacy Handbook: A Practical Guide to Your Privacy Rights in British Columbia and How To Protect Them* (Vancouver: B.C. Civil Liberties Association, B.C. Freedom of Information and Privacy Association, 1994) at 145 (hereinafter Shaw, Westwood and Wodell).
[787] Privacy Commissioner of Canada, *Genetic Testing And Privacy* (Ottawa: Minister of Supply and Services Canada, 1992) at 10-15 (hereinafter *Genetic Testing and Privacy*).

Genetic monitoring can help identify changes in a person's genetic make-up that require treatment, such as HIV, and it can also help identify environmental hazards that need to be reduced or eliminated, such as toxins leaking from a nearby factory.

3) **Forensic DNA Analysis**: this is used in criminal investigations to determine if a human sample left at the scene of a crime came from a certain suspect or not. It is not used to identify genetic disorders, nor is it used to detect changes in genes.

In Alberta, genetic testing is done in molecular diagnostic labs located in Calgary and Edmonton.[788] A list of other Canadian medical Genetic Clinics is available at the Canadian Association of Genetic Counsellors webpage at:
https://www.cagc-accg.ca/?page=225

What is the role of genetic testing?

Each of your cells contains 46 chromosomes, 23 from your biological mother, which are paired with 23 from your biological father.[789] Every chromosome contains a long molecule of DNA, which is the abbreviation for Deoxyribonucleic Acid. DNA looks like a long, very thin string that is twisted into a spiral (like a ladder). The DNA contained in each cell would be about a yard long if unraveled.[790] A strand of DNA is made up of tiny building blocks.[791] Different combinations of these building blocks along this string of DNA identify different genes. Genes are like sets of instructions on how we are to grow—like a blueprint directs how a house is to be built.[792] In these genetic instructions, there are about three billion bits of information that will determine everything from eye color, hair color, and body shape to the diseases that will be inherited. Virtually all of our body's cells, whether they are muscle cells, brain cells, sperm cells or other cells, contain a

---

[788] Calgary Genetics Clinic
Alberta Children's Hospital
Ph 403 - 955 - 7373

Edmonton Genetics Clinic
University Hospital
Ph: 780 - 407 - 8822

[789] A. Cavoukian and D. Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Random House of Canada, 1995) at109 (hereinafter Cavoukian and Tapscott).
[790] *Genetic Testing And Privacy*, at 6.
[791] D. E. Riley, "DNA Testing: An Introduction For Non-Scientists" *Scientific Testimony: An Online Journal* (University of Washington, 1998) Website www.scientific.org/tutorials/articles/riley/riley.html (hereinafter Riley).
[792] Cavoukian, and Tapscott, at 109.

complete sample of our DNA.[793] Even though red blood cells do not contain DNA, blood samples can be used to collect genetic information because the white blood cells do contain DNA.[794]

What does genetic testing do?

During genetic testing, a gene probe is used to look for specific genes that cause genetic disorders or for things called genetic markers. Genetic markers are genes or stretches of DNA that are known to lie close to the gene that causes a genetic disorder.[795] As gene research continues, we are learning that certain genes are responsible for causing specific diseases.[796] However, while some genes clearly cause certain diseases, like Huntington's or Tay Sachs diseases, other genes may only show that the person has an increased risk of developing certain illnesses like Ovarian, Colon or Breast Cancer.[797] In these types of cases, a specific gene might need to be present for a disease to develop, but the gene alone may not be enough to cause the disease. Sometimes more than one gene may be needed or more than one gene may need to be faulty for a disease to develop. Other times, things in one's environment (pollution) or behaviour (eating a poor diet) might also trigger the onset of a disease.[798] Genetic testing cannot predict when in the future a disease may start to show, nor can it predict how severe or disabling some diseases may be in a particular person.[799] While genetic testing information can be helpful, it cannot always be used to make accurate predictions.

Are genetic test results private?

The results of genetic testing contain a great deal of information about a person. They not only contain information about a person's personal characteristics, such as height, build and skin color, but test results can also contain information about a person's behaviors that could be associated with having certain genes. Nearly every cell in the body contains DNA, so you cannot easily alter or tamper with your genetic information. You will find it difficult to challenge this information once a sample is given and tested. Because many of your genetic traits are inherited, your genetic testing

---

[793] Riley.
[794] Riley. See also *Genetic Testing and Insurance*, Film Clip. First aired on Market Place, March 29, 1994 (hereinafter *Genetic Testing and Insurance*) for the role of genetic testing in insurance companies.
[795] *Genetic Testing And Privacy*, at 10.
[796] *Genetic Testing And Privacy*, at 8.
[797] M. A. Mullen, "Ethical Issues in Privacy and Genetic Data: Implications for Public Policy." (February, 1997) 17.3 Health Law in Canada 96 at 96-97 (hereinafter Mullen).
[798] S. Alter, N. Holmes and W. Young, *Privacy Rights And New Technologies: Consultation Package*. (Ottawa: Library of Parliament Research Branch, 1997) at 25 (hereinafter Alter, Holmes and Young).
[799] Council for Responsible Genetics. *Position Paper on Genetic Discrimination* (hereinafter *Position Paper on Genetic Discrimination*) Online: http://www.councilforresponsiblegenetics.org/pageDocuments/2RSW5M2HJ2.pdf

information also provides some information on your biological relatives.[800] This is information you may not wish to share or even know about. Before intruding upon a person's privacy through genetic testing, people must have an important reason for wanting the information and a very secure way to store it.

Because genetic test results include some information about your relatives, other people may claim that they "need to know" this information or that you have a "duty to disclose" or tell them about it.[801] Many in the medical community support population-wide screening for so called "cancer genes" so that carriers can be diagnosed and treated to minimize the ill effects long before any symptoms of the upcoming disability or disease are noticed.[802] A person may claim that you have a duty or obligation to disclose your genetic information to him when you know that he might have an inherited gene that causes an illness. Even if a certain disease does not have a cure, these relatives may want to know this information so they can adjust their long term goals and present lifestyles. A person may also claim that he needs to know about your genes in situations such as using donated eggs or sperm to have children. Genetic privacy, then, has two parts:

- being protected from one's own unknown secrets about who we are and what we may become, and
- being protected from the intrusions of others who want any information you may have about who they are and what they may become.[803]

6.1 GENETIC TESTING BY THE GOVERNMENT

6.1.1 GENETIC TESTING IN CRIMINAL CASES

How is genetic testing done in criminal cases?

Currently, there are two main forensic DNA testing processes used in criminal investigations. One is called Restricted Fragment Length Polymorphism (RFLP).[804] In this process, an enzyme is used to break up a strand of DNA. The genes then get plotted as dashes or dots along a strip of paper. This is an older DNA testing technique which requires a larger, non-degraded sample.[805] RFLP testing is

[800] Alter, Holmes and Young at 24.
[801] Mullen at 97.
[802] *Position Paper on Genetic Discrimination*.
[803] *Genetic Testing and Privacy*, at 4.
[804] *Genetic Testing And Privacy*, at 16.
[805] J. Clay, "The Law of DNA" (April/May, 1996) 21 Law Now (hereinafter Clay).

often not suitable for crime scene evidence that is old, or only of a small amount. The other main type of forensic DNA process is called Polymerase Chain Reaction (PCR). PCR itself does not analyze DNA, it only increases the amount of DNA available for analysis.[806] Through this process, a single molecule of DNA is duplicated into millions or billions of DNA molecules in about three hours.[807] PCR is good for copying DNA if the initial DNA is in good condition. Extreme caution must be used in this process, for one contaminated molecule may be repeatedly duplicated and eventually lead to a false or misleading result.[808]

Forensic DNA testing gives a "match" or "no match" result when comparing two samples. Aside from identical twins, no two people have the same DNA. Because a person's DNA is the same in every one of her cells, it is not necessary that the samples being compared be of the same type.[809] For example, the DNA in the blood of a suspect can be compared to the DNA found in semen left on a victim. Forensic DNA testing does not identify any genetic traits nor give any medical information on a person.[810]

What rules must the government follow when doing forensic DNA testing?

The federal government planned to regulate a process of forensic DNA testing, which the police could use to help identify offenders who left traces of DNA at a crime scene.

Phase one of this plan was Bill C-104. When this Bill became law in 1995, it allowed the police to apply for a special warrant to collect DNA samples from suspects.[811] The procedure for both getting the warrant to collect a DNA sample and the actual taking of the sample from the suspect is detailed in the *Criminal Code* under "Forensic DNA Analysis."[812]

Phase two of the government's plan[813] was to pass legislation that would allow the police to have a DNA data bank of samples taken from convicted offenders. The police could then use these samples to help them identify those people who were involved in unsolved crimes. But the original data bank

[806] Riley,
[807] Riley.
[808] Riley.
[809] Clay.
[810] *Genetic Testing And Privacy*, at 16.
[811] A. Scott, "Solicitor General Andy Scott Introduces Bill to Establish National DNA Bank" News Release. Solicitor General of Canada. 25 Sept. 1997 (QL LNCR database) (hereinafter "National DNA Bank").
[812] See *Criminal Code*, Revised Statutes of Canada 1985, chapter C-46, sections 487.04-487.09.
[813] Scott

bill did not become law. In 1998, the government passed an almost identical data bank law, the *DNA Identification Act*.[814]

When can the police apply for a forensic DNA warrant?

A DNA warrant is available only when certain *Criminal Code* offences have been committed. The list of offences, for the most part, are serious offences that involve violence or injury to a person—sexual offenses, assaults and homicides. But the list is not restricted to serious offences or only to offences against a person.[815]

Forensic DNA warrants should not be confused with what are commonly called "blood warrants." Blood warrants are only available if there is an alcohol-related driving offence believed to have caused death or bodily harm.[816] With a blood warrant, a blood sample is collected and analyzed to determine the level of alcohol in an individual's bloodstream.

When will a judge grant a forensic DNA warrant?

A forensic DNA warrant may only be issued by a Provincial Court Judge.[817] Before issuing the DNA warrant, the judge must have reason to believe the following four things:[818]

> 1) that one of the specifically listed offences has been committed;
> 2) that a bodily substance has been found either at the place where the offence was committed, on or within the body of the victim of the offence, on anything worn or carried by the victim at the time when the offence was committed or on or within the body of a person, place or thing associated with the offence;
> 3) that the person was a party to the offence; and
> 4) that forensic DNA analysis of a bodily substance from the person will provide evidence about whether or not the substance at the scene was from that person.

The judge must also consider whether or not the offence is serious enough to justify the intrusion of searching and sampling a person, and whether or not there is someone available who is trained to do

---

[814] *DNA Identification Act*, Statutes of Canada 1998, chapter 37.
[815] *Criminal Code*, section 487.04.
[816] *Criminal Code*, section 256 as discussed in R. M. Pomerance, "Bill C-104: A Practical Guide To The New DNA Warrants." (1995) 39 Criminal Reports 224 at 227(hereinafter Pomerance).
[817] Pomerance, at 229.
[818] *Criminal Code*, section 487.05(1).

this type of sampling.[819] DNA from people who are biologically related to the suspect also might contain information on the suspect that would be useful in a criminal investigation. Parliament, however, did not want these innocent relatives subjected to mandatory sampling. The law clearly says that the forensic DNA warrants may only be used to obtain a sample from a person who is suspected of being directly involved in the crime being investigated.[820]

What can the body samples be used for?

The *Criminal Code* places strict limits on what the body *samples* may be used for. They may only be used for forensic DNA analysis and only in the investigation of the offense for which the warrant was originally obtained.[821] However, the law outlining what uses the actual *information* from the samples can be used for is not as clear. For example, the Minister of Justice reassured that that the DNA results could only be used in the particular investigation for which they were originally taken. However, it could be argued that the actual wording of the law allows the information from a sample already collected to be used in the investigation of another separate offense.[822] So far, the Supreme Court of Canada has only confirmed that a DNA sample, validly obtained on consent, can be used in the investigation of other offenses in respect of which the individual later becomes a suspect.[823] Regardless of what was intended by the law or how it is eventually interpreted by the court, there is nothing to stop the police from applying for a second forensic DNA warrant and collecting yet another sample from the suspect for the analysis in the investigation of another offence.[824] Not only does this second physical intrusion appear excessive and unnecessary, re-doing the DNA analysis seems like a waste of scarce lab time and money.

What happens to the samples if I am acquitted?

Presently, the *Criminal Code* requires that both the samples and the results of forensic DNA analysis must be destroyed when the accused is acquitted, when it is determined that the crime scene sample did not come from the person sampled or after one year from the date of discharge, withdrawal or stay of the charge.[825] If, however, a new charge is laid for the same person in relation to the same investigation, the forensic DNA warrant sample and information do not have to be

[819] *Criminal Code*, section 487.05(2).
[820] *Criminal Code*, section 487.05(1).
[821] *Criminal Code*, section 487.08(1).
[822] *Criminal Code*, section 487.08(2) as discussed in Pomerance, at 236.
[823] *R v Borden*, [1994] 3 Supreme Court Reports 145 as discussed in Pomerance, at 237.
[824] Pomerance, at 237-238.
[825] *Criminal Code*, section 487.09

destroyed. These particular legal requirements only apply to the samples and the information from forensic DNA warrants. They do not apply to samples given by consent or those obtained through other types of warrants.

Are there DNA data banks? Who looks after them?

A DNA data bank has been established and is maintained by the RCMP, which operates six forensic laboratories across Canada.[826] In 1998, it was estimated that this data bank will cost approximately three million dollars a year to run.[827] Under data bank laws, if someone is convicted of a serious violent offence and the offence is on the "primary list", a court will direct that bodily substances be obtained from the person for the purpose of data banking. If a person is convicted of an offence listed on the "secondary list", then the Crown prosecutor can argue to the court that it is in the best interest of the administration of justice to have this person also submit bodily samples for data banking. Offender information in the data bank will be cross-referenced with information from unsolved crimes to help identify and apprehend repeat offenders and exclude the innocent suspects from suspicion more quickly. Access to the information in this data bank is supposed to be strictly limited to those responsible for the operation of the data bank. This law also creates criminal penalties if the information or samples in the data bank are misused.

Should I have some concerns about the DNA data bank?

There are still some people who have concerns about data banks. To understand some of these remaining concerns, it is important to first appreciate that the data bank law requires that the DNA samples themselves be kept in a data bank, rather than just keeping the DNA information from the analysis of these samples in a database.[828] There also appears to be nothing in the law that prevents putting in samples and information from innocent people who volunteer their DNA to help with police investigations.[829]

At first glance, a data bank of samples appears to be more convenient and less costly to maintain than just an information database because new forensic DNA identification techniques could be applied to existing samples in a data bank without having to obtain new samples from the same

[826] Royal Canadian Mounted Police, "Canada opens National DNA Data Bank" News Release, July 5, 2000.
[827] B. Phillips, Privacy Commissioner of Canada. "Bill C-3, the DNA Identification Act" *Presentation to the Standing Committee on Justice and Human Rights* Privacy Commissioner of Canada: February 12, 1998 (hereinafter "Bill C-3, the DNA Identification Act").
[828] "Bill C-3, the DNA Identification Act."
[829] "Bill C-3, the DNA Identification Act."

people again.[830] However, there are many people who have concerns about the possible future wider use of these banked samples. As the list of offenses for which forensic DNA testing is allowed increases,[831] or as curiosity and public pressure leads to using the samples to look for common genetic traits associated with offenders,[832] the approved uses for these samples may be expanded beyond that for which what they were originally given. People who do not like the idea of keeping the forensic DNA samples in a data bank argue that once DNA analysis is done, the samples are no longer required to compare data bank DNA to the DNA extracted from evidence at a crime scene. All that is needed is the information from the forensic DNA analysis. The goal of forensic DNA analysis, which is to link a suspect to a crime scene, can be met without keeping the offender's sample on file.[833] While it seems sensible to use the least intrusive measure and keep the offender's DNA information on file, it is privacy's best interest to discard the offender's actual sample.[834]

Some uses of banked DNA may be appropriate for law enforcement agencies, but the potential for civil rights violations and the use of these samples and information beyond the original purposes are too great.[835] One author says that the government's approval of the DNA bank is based on the false impression that genetic tests are accurate and that communities will be safer with such a data bank.[836]

How do the police actually take forensic DNA samples?

The *Criminal Code* clearly sets out how a sample is to be collected under a forensic DNA warrant[837] prior to taking the sample, the police must tell the person named in the warrant:

- what is in the warrant;
- the type of sampling to be done;
- the purpose of obtaining the sample;

---

[830] "Bill C-3, the DNA Identification Act."
[831] Alter, Holmes and Young, at 26.
[832] Privacy Commissioner of Canada. Response of the Privacy Commissioner of Canada to Department of Justice consultation paper, "Obtaining and Banking DNA Forensic Evidence" January 9, 1995 at p. 6 (hereinafter Response to Department of Justice) Website https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_dna_950109/ .
[833] Remarks to the Standing Committee on Justice and Human Rights, at 4.
[834] Remarks to the Standing Committee on Justice and Human Rights, at 4.
[835] Mullen, at 97.
[836] Christina Scowby "Private Costs of Safer Communities: DNA Evidence and Data Banking Canada" (1999) 5 Appeal 86-96.
[837] Pomerance, at 233.

- the possibility that the results of the DNA analysis may be used in court as evidence; and
- that under the warrant the police can detain the person as long as is reasonably necessary and use as much force as is necessary in order to get the sample.[838]
- Types of sampling allowed for forensic DNA testing are:
- plucking hairs from the person;
- swabbing the lips, tongue and inside of the cheeks of the mouth to collect cells; and
- taking blood by pricking the skin surface with a sterilized lancet.[839]

The police must also take reasonable steps to ensure that the sampling is done in such a way that the suspect's privacy is, if at all possible, respected.[840] The judge issuing the warrant may also include instructions that the sampling be done by a qualified medical professional.

Because collecting a sample under this type of warrant requires that the person be detained, the *Charter of Rights and Freedoms*[841] requires that this person must be informed of his right to have a lawyer and be given a reasonable opportunity to contact one.[842] If you do not have or do not know a lawyer whom you could call, the police must supply you with a phone book or a phone list of lawyers, including any information on the availability of legal aid should you feel you cannot afford a lawyer.[843] In Alberta if you are detained, there is a 24 hour number you can call to speak with a lawyer. You must be given privacy when phoning and talking to a lawyer.[844]

Why should a law-abiding citizen, with nothing to hide, be concerned about whether or not the police are allowed to keep DNA samples or DNA information on their files forever?

Without very clear and strong rules, there is enormous potential for the abuse of this kind of information. For example, if a member of a law enforcement agency feels that someone is a seedy character who may have committed a crime, even if she is not convicted of any listed offense for which the law allows DNA samples to be collected, the police may one day be able to collect a

[838] *Criminal Code*, section 487.07.
[839] *Criminal Code*, section 487.06.
[840] *Criminal Code*, section 487.07(3).
[841] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act* 1982, being Schedule B of the *Canada Act* 1982 (UK), 1982, c 11, section 10(a) and (b).
[842] *R. v. Bartle*, [1994] 3 Supreme Court Reports 173 (SCC).
[843] *R. v. Brydges* (1987), 84 Alberta Reports 259 (ABCA); reversed [1990] 1 S.C.R.190 (SCC).
[844] See *R. v. Playford* (1987), 63 Ontario Reports (2d) 289 (ONHC).

sample from her anyway. There are also concerns about who will legally have access to genetic information and the overall security of computerized databases. With samples that have already been collected and analyzed, there is the potential for them to be used for drawing up offender profiles. Some people who do not commit crimes may match these profiles and therefore be under continual suspicion. Even if a DNA data bank might make the street safer, will the improvements be substantial enough to justify these types of risks?[845] There are many other means of confirming a person's identity—such as fingerprints, eyewitnesses and surveillance cameras. If law enforcement authorities have reason to suspect an individual is involved in a particular crime, they can and should be made to justify obtaining a forensic DNA warrant each time. To allow the police to automatically gather, retain and re-use samples and information is to empower police officers, rather than judges, to force people to produce evidence that contains their most intimate secrets as well as those of their blood relatives.

6.1.2 Genetic Testing by the Government in Other Situations

Does privacy legislation apply to genetic testing by the government?

Provincial and federal privacy laws may apply to genetic testing by the government (provincial or federal). Once genetic samples are taken from a person and labeled as belonging to the individual, they fall into the definition of 'personal information' under these laws. Because of the genetic testing uncovers extremely sensitive personal information, the federal Privacy Commissioner believes that the law must provide specific authority for the collection of most genetic testing information. Also, since privacy laws require that the government take all reasonable steps to ensure the accuracy and completeness of the information, both the technical part of genetic testing must be accurate (qualified technicians are used, there is no contamination of the samples, no accidental switching of samples, no recording errors, etc.) and that the interpretation of the test results must also be accurate based on the scientific knowledge at that time.[846] Privacy laws require the government to keep the information for an appropriate period of time after it has been used to allow the person a reasonable chance to obtain access to it. This applies to both the genetic sample and the analysis.[847] If the information was not used, there is no requirement for the government to keep it. A

[845] "Bill C-3, the DNA Identification Act."
[846] *Genetic Testing and Privacy*, at 64.
[847] *Genetic Testing and Privacy*, at 62.

government institution, however, might keep genetic information and the samples indefinitely, for destruction is not mandatory.[848]

For information on the rules and duties imposed on government institutions gathering personal information, see Chapter 1: Privacy Protection and the Government.

Does the Charter apply to genetic testing by the government?

The *Charter* adds some additional protection against government bodies intruding on a person's privacy. While specific laws authorizing a specific program to collect personal information may in fact override the standards set out in privacy laws, they cannot violate the *Charter*, which is the supreme law of Canada.[849] The *Charter* protects the right to be free from unreasonable search and seizure, and the right to life, liberty and security of the person. If the government program infringes on these rights and the infringement cannot be justified according to a well-defined test,[850] the law authorizing the program will be invalid.

I have already given the government lots of information on me. If they need more what's the harm in giving it to them?

Unfortunately, government departments do not always use information in ways that were originally promised. For example, the Social Insurance Number card's use has expanded beyond government purposes to banking, credit history and may even be requested as identification for some membership cards. Restricting the collection of personal information is the most obvious but often most understated protection against violations of privacy by government.[851] It is common sense that government institutions, or those who can break into their files, are less likely to violate a person's privacy if they do not collect information about that person in the first place.

6.2 GENETIC TESTING IN THE PRIVATE SECTOR

The regulation of one's genetic information in the private sector has not developed as far as the regulation of it in the federal or provincial governments. The *Personal Information Protection and Electronic Documents Act,* or PIPED Act (or other provincial privacy laws)regulates how private sector organizations collect, use and disclose personal information in the course of business

[848] *Genetic Testing and Privacy*, at 62.
[849] *Genetic Testing and Privacy*, at 56.
[850] *R v Oakes,* [1986] 1 Supreme Court Reports 103 (SCC).
[851] *Genetic Testing and Privacy*, at 57.

activities. In May 2017 the *Genetic Non-Discrimination Act*[852] received Royal Assent creating stricter and more specific laws for genetic testing in the private sector. The *Genetic Non-Discrimination Act* prohibits any person from requiring an individual to undergo genetic test or to disclose existing results of previous tests. Further, companies who collect genetic information are prohibited for disclosing it to other organizations without the individuals written consent. Other federal and provincial privacy laws do not apply to the private sector; nor does the *Charter*. There are some other laws that are applicable to the private sector, which would apply to genetic testing. For example, certain professionals, like health care workers and lawyers, must also keep the information they receive from their clients in confidence.[853] Also, in some cases, health information legislation and legislation dealing with data collection by the private sector might apply to the collection, use and disclosure of genetic testing information. **For further information on privacy and the private sector, see Chapter 2: Privacy and Canada's Private Sector.**

The private sector may be largely made up of good citizens, but people can be vulnerable to fear, prejudice, irrationality and the drive for efficiency. Society must protect its citizens from the stigmatization of its individuals by the private sector's unregulated collection, use and disclosure of one's uniquely personal information likely to be obtained from genetic testing.[854] One author believes that active regulation of genetic testing in the private sector is necessary to prohibit the increasing use of genetic testing in questionable areas.[855]

---

[852] *Genetic Non-Discrimination Act,* Statute of Canada 2017, c 3.
[853] *Genetic Testing and Privacy* at 79.
[854] *Genetic Testing and Privacy*, at 80.
[855] Michael Burgess "Whither Morality in Genetic Tests?" (2001) 9(3) Health Law Review 3-9.

6.2.1 EMPLOYMENT

Why would an employer want to use genetic testing?

Employers see many economic benefits to knowing which of their workers and job applicants are likely to remain healthy.[856] For example:

- fewer employees taking sick leaves means more production in the workplace,
- having healthier workers means the company may qualify for a less expensive life insurance program,
- the longer an employee lasts, the less time and money an employer needs to spend on training new employees,
- genetic testing information which identifies individuals who have above average genetic resistance to workplace contaminants makes for longer employment terms.

What may happen if I provide a genetic sample at work?

The thought of using genetic testing in the workplace creates or perpetuates many economic concerns for all employees.[857] For example, genetic testing information which shows that a job applicant may develop future heart disease may make the applicant unattractive to an employer, and the applicant may not be hired. Such genetic discrimination, however, overlooks the basic need for adequate sick leave policies, insurance coverage and reasonable sick leave accommodation for all the employees who have temporary or permanent disabilities for whatever reasons.[858] Using genetic test results as a screening technique in workplaces may create an entire group of "unemployable" people.[859] Discrimination against individuals without a particularly hardy genetic disposition also harms all workers by allowing attention to be diverted from the need to improve or eliminate workplace conditions that contribute to the ill health for all the workers.[860]

At present, Canadian employers appear to conduct little genetic testing.[861] If they did, arguing that genetic testing is justified because it makes a more productive workforce would have serious human

---

[856] *Position Paper on Genetic Discrimination*.
[857] Shaw, Westwood and Wodell, at 146.
[858] *Position Paper on Genetic Discrimination*.
[859] Cavoukian and Tapscott, at 111.
[860] *Position Paper on Genetic Discrimination*.
[861] *Genetic Testing And Privacy*, at 16.

rights implications.[862] Discrimination in the workplace on the basis of genetic testing ignores the present abilities and health of workers. It substitutes tentative predictions about the possible future development of diseases with questionable stereotypes about one's future job performance. With the Assent of the *Genetic Non-Discrimination Act* employers are now completely prohibited from requiring genetic testing of either current or future employees. Any genetic testing must be voluntary.

During a casual conversation with my employee, she happened to mention that she has a genetic trait that increases her risk of developing heart disease. Can I put this information in her file?

If your workplace is a federal government workplace, you must comply with the federal *Privacy Act*. The Act limits the collection of volunteered information.[863] Volunteered information should not be recorded, unless it passes the same "relevance" test as personal information that is allowed to be collected without a person's consent such as through a mandatory testing program. Since the PIPEDA (or similar provincial legislation) now applies to the private sector, the knowledge and consent of an individual is required (except for the enumerated exceptions under the Act) not only for the collection of personal information, but also for the subsequent use or disclosure of this information. In this regard, you may need to obtain the employee's consent before using the employee's volunteered information in her file.

6.2.3 GENETIC TESTING FOR ACCESS TO INSURANCE OR OTHER BENEFITS

Why would an insurance company perform genetic testing?

Although insurance companies do not currently require that a person who is applying for insurance have genetic testing, they do insist, but cannot require,[864] that people disclose any information they may have about any genetic test they may have taken.[865] If this information is not disclosed, the insurance policy may be void. Experts in the insurance industry argue that it is not only useful to use genetic test results in the underwriting process (the process of determining if the company will

[862] Shaw, and Westwood and Wodell, at 146.
[863] *Privacy Act*, Revised Statutes of Canada, 1985, chapter P-21, section 4; see also *Genetic Testing and Privacy*, at 58.
[864] *Genetic Non-Discrimination Act*, s 4(1).
[865] *Genetic Testing and Insurance*.

insure you and how much it will cost), but that it is essential for them to have access to this information. Some of the reasons they often give are:[866]

- Anti-selection: Insurers need to assess the risk of someone's health failing so they can calculate what would be the appropriate premium for the person to pay. Genetic testing can help identify those people who are likely to die soon. Those applicants who have somehow discovered that they have an increased risk of death or disablement have a greater incentive to buy insurance. In not telling the insurance company about this genetic information they may be insured for risks the company did not want or be in a position to cover.
- Equity: By not using genetic testing results to help identify those clients with higher risks, all policy holders end up paying more to help subsidize the unhealthy policy holders' insurance. These higher rates are not fair to those insurance holders who are healthy.
- Usual Underwriting Practices: Insurance agencies argue that using the information from genetic testing is just a natural extension of the current process of requesting information on an applicant's family history.

Consumer groups, on the other hand, strongly oppose using genetic testing information in the underwriting process. Some of the concerns they have are:[867]

- Avoidance: The very people who could benefit medically from the early detection of a genetic risk may not get tested because they are afraid of being denied services like insurance because of this same information.
- Goal of Insurance: The goal of insurance is to provide families who experience a death or disability with some economic security. Underwriting practices that identify and insure only the very healthiest individuals undermine the objective of insurance, which is to spread the cost of a payout across a broad pool of people.
- Discrimination: No one has control over her genetic makeup. Using the information from genetic testing in a way that negatively impacts on the individual, like making her pay much higher premiums, is arguably discrimination based on an inborn disability.

[866] Lombardi.
[867] Lombardi.

- Limited Predictability: As already discussed, genes are often only one factor in determining whether or not individuals will get diseases. Other important factors like the environment and behaviors must still be assessed using the old underwriting technique.
- Increased Costs: The use of genetic testing and the storage of this information will introduce additional costs for the insurance company. This cost increase is not necessary because insurance companies use life-expectancy tables that have already taken into account that some people have genetic based diseases. Insurance companies have always insured people at risk for genetic conditions, and there is no new epidemic of genetic conditions.[868] These additional and unnecessary costs of genetic testing are likely to be passed on to the customer.
- Privacy: With the collection, use and storage of such sensitive information like genetic test results, there is always the added risk of this information being accessed by unauthorized individuals or agencies. The best way to avoid this type of misuse is not to collect the unnecessary information in the first place.

Currently, the relatively high cost of genetic testing keeps insurance companies from using it in their underwriting process.[869] However, as the cost of genetic testing decreases, interest in its use will no doubt increase. Overall, there is no reason for insurers to begin to use this new predictive information merely because it is available. It could lead to creating a class of uninsurable people based on the limited success of future predictions. The information from genetic testing is largely redundant to the insurance industry's business. Considering the sensitivity of genetic information, which reaches into the unknown secrets of an individual and his biological relatives, the privacy concerns surrounding genetic testing should be dealt with now before genetic testing becomes more economically available.

[868] *Position Paper on Genetic Discrimination*.
[869] Lombardi.

The union where I work says I have to have regular genetic tests done to make sure I am not getting sick from the stuff I work with. If they find something, could the company cut me off of the company insurance/health benefits package I have now?

A union that has negotiated a workplace contract for its employees does so keeping in mind what is best for the majority of the workers in that particular workplace. If the union agreed to include genetic testing in the workplace agreement (also called a collective agreement), then it probably bargained with the employer what the information from these tests could be used for and how it could or could not affect a person's benefits or length of employment. But due to new laws requiring genetic testing, even as negotiated through a collective agreement is prohibited. It is important to ask your union this question so they can tell you how the new regulations will be dealt with in your particular workplace agreement.

The genetic test I had at work showed that I have a gene that is supposed to cause a serious illness. Do I have to tell my private insurance company?

With this new genetic information, some insurance companies may continue to insure you at your present rate, others may increase your rate to cover the additional risk, while still others may not want to insure this type of risk at all. To know whether or not you must disclose this new information to your insurance company, you must check the exact wording of your present life insurance policy or contract. If you signed a policy that states or implies that you will update the insurance company about this new type of information, then you probably have to in order to fulfill your half of the contract and to keep your policy valid. If you are supposed to inform your insurance company but do not, then they do not have to pay out any claims made against the policy because you did not hold up your end of the agreement. Because contracts can be difficult to understand and the consequences could be severe, it would be a good idea to consult a lawyer to help interpret the specific insurance deal you have.

6.2.4 GENETIC TESTING IN MEDICAL CARE/HEALTH CARE FACILITIES

What are the laws and policies on the disclosure of genetic information?

Genetic information is often seen as being part of a person's medical information and, therefore, should be treated with the same rules of secrecy.[870] Some argue that genetic information is even more sensitive than medical information for at least two reasons:

[870] Cavoukian and Tapscott, at 109.

- it can reveal information about a patient's future health, which can be a heavy emotional and financial weight on patients who are suddenly aware of a serious or fatal medical condition that will now affect them for the rest of their lives, and
- it can also reveal information that is of real interest to biological relatives.[871]

Medical professionals are in a difficult position when faced with the question of whether they should, or even can, disclose their patient's genetic information to the patient's biological relatives. The health of biological relatives is the most compelling reason for disclosing genetic information as this information can often provide them with important information for their own health care decisions. On the other hand, the medical professionals will probably not be held at fault for not disclosing this information, as the "duty to warn" cases involve immediate and life threatening risks to others, which is usually not the case with most genetic disorders.

The current laws governing the use and disclosure of health information are set out in Chapter 1: Privacy Protection and the Government; and those governing medical information are set out in Chapter 2: Privacy and Canada's Private Sector.

6.3 GENETIC TESTING IN HUMAN REPRODUCTION

What is the role of genetic testing in human reproduction?

Information from genetic testing can help people make decisions about having children. This particular use of genetic testing is known as genetic counselling and is one of the most common

---

[871] W. F. Flanagan, "Genetic Data and Medical Confidentiality" (1995) 3 Health Law Journal 269 at 269 (hereinafter Flanagan). In 1983, a Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioral Research recommended that genetic information should be disclosed to biological relatives without the patient's consent, only if:

- reasonable attempts to get the patient's consent for disclosure were unsuccessful,
- there is a high probability of serious (meaning irreversible or fatal) harm to an identifiable relative,
- there is reason to believe that disclosure of the information will prevent harm to the relative, and
- the disclosure is limited to the information necessary for diagnosis or treatment of the relative. (Flanagan, at 280-287).

In other words, to justify disclosing a patient's genetic information without his consent, the information should be both significant and useful to the biological relative. Genetic information will be most significant when it shows that the relative is at a substantially higher risk of suffering from a serious genetic disorder than the normal population. Genetic information will be most useful when it informs someone that they should get treatment or avoid the triggers of diseases they probably have the genes for. While these guidelines suggest that disclosure might be justified under certain circumstances, they do not make it clear as to whether disclosure is necessary in these same situations.

A 1989 study showed that a majority of the geneticists surveyed would, in some cases, disclose genetic data to biological relatives even if a patient expressly refused to consent to such disclosure, and even if the genetic condition was untreatable and fatal. It appears that many physicians practicing in the field of genetics believe that they can breach a patient's medical confidentiality in order to share some genetic information with biological relatives. These views are, at the very least, legally questionable.

uses of genetic testing.[872] Genetic testing can be used at three different stages of genetic counselling[873]:

1) **Pre-conception**: Before a couple tries to get pregnant, the parents can undergo genetic testing to see if they could produce a child with genetic disorders, such as Tay-Sachs or sickle-cell anemia.

2) **Prenatal**: During the pregnancy, genetic testing of the fluid around the fetus helps guide difficult decisions about possible medical treatments or abortion of the fetus.

3) **Neonatal**: All provinces and territories screen newborns for phenylketonuria, (where a person lacks a necessary enzyme and unless they are placed on a special diet early in life may experience effects like retardation and seizures), and hypothyroidism (where too little thyroid hormone is produced and if not treated can lead to effects like mental retardation, growth failure, deafness and neurologic abnormalities.) Although routinely done, these tests are not mandatory and parents can refuse to have them done.

With the help of technology like genetic testing, which unlocks information about one's future health, medicine continues to move from diagnosing and treating patients to preventing individuals from becoming patients.[874] At first glance, preventing a disease appears better than having one. But will this kind of information lead us to select our mates only after we are sure their genes are compatible with our own? Will we one day be able to design our children to match our particular tastes? Will there be increasing pressures to reject all but the most genetically desirable offspring? Will there be no more resources to help individuals with genetically related disorders because they could have been pre-determined and eliminated prior to birth? Who will draw the line and decide what will be acceptable and non-acceptable genetic traits? Will the line be drawn at Down Syndrome? Diabetes? Allergies? Homosexuality?[875] As helpful as genetic testing information may be, it can also be used in many undesirable ways against not only ourselves but future generations.

---

[872] *Genetic Testing And Privacy*, at 19.
[873] *Genetic Testing And Privacy*, at 19.
[874] B. M. Knoppers, "Professional Norms: Towards a Canadian Consensus?" (1995) 3 Health Law J.1 at 1.
[875] Cavoukian and Tapscott, at 112.

Does my "significant other" have a right to know my genetic information if we want to have a child?

As already discussed, your genetic information may be of interest to your reproductive partner as this information can be useful in making more informed reproductive decisions. However, while there may be some allowance for medical professionals to release significant and useful genetic information to biologically related individuals, it is likely that a court would excuse your physician breaching your confidentiality by giving your partner this information without your consent.[876] In this situation, your genetic information cannot be used to prevent any risk of serious and imminent harm to another living person. Any genetic disorders you may have are not contagious to your reproductive partner. Presently, it appears that it is up to you whether or not you want to share some or all of your genetic information with your partner. If you are considering having a child with your partner, sharing any information that may affect reproduction with that partner will enable you to make informed decisions together.

6.4 CONCLUSION TO GENETIC TESTING

Our genetic information can help us develop a greater understanding of our bodies and our health.[877] On the other hand, genetic technology can also provide us with the ability to pre-select for genes in order to produce someone's idea of "better" human beings. In the future, we may be able to use the knowledge about genes to tell us who will be smart, antisocial, hardworking, athletic, beautiful, predisposed to acts of crime or who will die young.[878] Genetic testing is no longer just a medical aid.; it is also a way of creating social categories.[879] As genetic tests become simpler to do and their use more common, discrimination will likely increase.[880] Genes for traits that some find undesirable will follow people like scarlet letters that are handed down from generation to generation.[881] Genetic information is being processed more quickly than our legal and social service systems have responded.[882] Individuals must be and are allowed to control if and when they will learn and share this extremely personal and potentially very sensitive information about their genetic potential.[883]

---

[876] Flanagan, at 285 - 286.
[877] "Bill C-3, the DNA Identification Act."
[878] *Genetic Testing and Privacy*, at 2.
[879] *Position Paper on Genetic Discrimination*.
[880] *Position Paper on Genetic Discrimination*.
[881] Cavoukian and Tapscott, at 111.
[882] *Position Paper on Genetic Discrimination*.
[883] *Genetic Testing and Privacy*, at 4.

6.5 Case Studies

6.5.1 Genetic Testing in Employment

John Doe v Canada (Attorney General), [2004] FCJ No 555

A former employee of the RCMP applied for a judicial review of a decision of the Veteran's Review and Appeal Board of Canada ("Board") regarding a pension claim he made due to some work related medical conditions. He was employed by the RCMP for 26 years and had on two different occasions successfully sought judicial review of the Board's decision.

The former employee was seconded to another unit for a special assignment for a period of nine months. He became extremely upset to learn on coming back, that the nine months spent at the special unit would not be included in his annual assessment. He was also upset because the assessment would be done by someone with whom he had previous conflicts. According to a medical expert, this convinced the employee that he would not be getting the progress and recognition he has hoped for in his work.

The former employee suffered four medical conditions as a result of this final conflict. The first condition was a serious autoimmune condition, which the employee developed a few months after the administrative conflict. The second condition developed of viral origin leading to a third condition of malignancy. Finally, he developed a fourth condition which medical literature described as having a psychosomatic origin or being linked to stress. Two medical experts had indicated that the evolution of the former employee's disease favored the possibility that he had a genetic predisposition to develop cancer, but later genetic testing did not show such genetic predisposition to cancer. The Board awarded him two-fifths of a pension for the first medical condition and decided that the other three conditions were not attributable to service. However, the medical experts' opinions supported the employee's evidence that all four of his medical conditions resulted from the administrative conflicts and the working situation with his employer. The court ruled that the Board made a patently unreasonable error in failing to consider the uncontradicted evidence of the medical experts and directed the Board to hold another hearing before an entirely new panel that had not participated in either of the first two hearings. The court also ruled that the evidence of former employee's stress in his workplace and its link to the employee's medical condition were clearly established and compensable. The court awarded the employee the cost of retaining the medical experts.

Re Cognitive Impairment due to Exposure to Aluminum, 1996 (Workers' Compensation Appeals Tribunal)[884]:

A claim supported by the worker's genetic disposition to easily absorb aluminum.

An electrician who had worked with many aluminum products for over 24 years developed a neurological disability affecting his memory and concentration. Over time, these problems became bad enough that the worker felt he had to stop working. The worker made an application for disability benefits to the Workers' Compensation Board claiming that his disability was brought on by aluminum toxicity at work. The Workers' Compensation Board denied the worker's claim, so the worker appealed to the Worker's Compensation Appeal Tribunal. Two neuropsychologists each gave evidence that the worker's brain dysfunction was consistent with that associated with aluminum neurotoxicity. The worker showed that he had contact with aluminum in the workplace in several different ways, some of which were: using an aluminum powder in "cadwelding"; welding aluminum pipes; cutting and stripping cable that contained aluminum; cutting and grinding aluminum parts; using aluminum oxide sandpaper; and spraying aluminum paint. The worker testified that he seldom used a mask, that he often placed aluminum parts into his mouth as he worked, that his hands were frequently black from the aluminum, and that he not only did not use gloves but often licked his fingers before beginning work requiring finger dexterity. The aluminum at the workplace would have gotten into the workers' body through his skin assisted by the moisture from the various solvents he handled, and the build up of aluminum to a toxic level can occur in a body because the kidneys are not removing aluminum from the blood. Further evidence was introduced to show that the only source of aluminum dust in the worker's life was his workplace. Genetic evidence was also introduced to show that this worker, like the peoples of Guam and Java, appear to have a genetic susceptibility to aluminum absorption, which in turn made this worker more susceptible to aluminum toxicity than most people. The worker was successful in persuading the Appeal Panel that his neurological disability was a workplace accident and was, therefore, entitled to disability benefits.

[884] *Re Cognitive Impairment Due to Exposure to Aluminum,* Workers' Compensation Appeals Tribunal October 30, 1996, Decision No. 249/96.

6.5.2 Genetic Testing For Access to Services

Uppal v Canada (Minister of Citizenship and Immigration)
(2009)(Federal Court of Canada - T.D.)[885]
Genetic testing of permanent residence applicants.

Mr. Uppal and his wife Ms. Kaur were citizens of India, but applied for permanent residence for themselves and their three children. They were being sponsored by Amandeep Singh Kaur, who was also represented as the biological child of the principal applicant, Mr. Uppal and his wife Ms. Kaur. Mr. Uppal indicated in the application form that he had not been married prior to his marriage to Ms. Kaur. During their interview in India, the immigration officer asked Ms. Kaur why there was a substantial age difference between Amandeep and the other children, and she explained that she had a medical problem after the birth of Amandeep and had to stop giving birth, but later had the other three children after resolving her problem with medication. Unsatisfied that the three children were the dependent children to Mr. Uppal and his wife, the immigration officer requested for genetic testing. Before the DNA testing, Amandeep wrote a letter to immigration advising them that Mr. Uppal is his real father, his wife is his step-mother and the youngest children his step-brothers.

The DNA testing established that Mr. Uppal was the biological father of all four children and the wife the biological mother of only the two youngest children. Mr. Uppal argued that he did not mention the fact that his children had two different mothers because he did not think that it was relevant. Ms. Kaur did not provide any explanation. Mr. Uppal subsequently submitted a death certificate for his first wife, and a marriage certificate for the marriage between him and Ms. Uppal, but these documents were rejected by the immigration officer on the ground that they were self-serving having been issued after the request of the immigration office. The officer also considered that no photographs were submitted despite being specifically requested, noting the fact that weddings are highly festive events in India, and photograph of such events are usually kept for decades.

As a result of the inconsistencies identified, the officer refused Mr. Uppal's application for permanent residence on the ground of misrepresentation. Mr. Uppal and his wife Ms. Kaur argued

[885] *Uppal v Canada (Minister of Citizenship and Immigration),* [2009] FCJ No 557.

that the officer erred in finding that they had misrepresented a material fact given that the situation was clarified prior to the actual decision on their application for permanent residence. The court ruled that disclosing their misrepresentation prior to the final decision being taken did not assist them, as their misrepresentations were made in the context of the applications for permanent residence considered by the office. The court also found that it was not unreasonable for the immigration officer to reject the certificates provided as they were issued after the request from immigration authorities and no other supporting evidence of their marriage was offered. Mr. Uppal's application was dismissed.

6.5.3 Genetic Testing and Medical/Health Care

Zhang v Kan
[2003] BCJ No 164[886]:

A case showing the importance of a patient being given relevant genetic information in order to make informed medical treatment choices.

The plaintiff, Zhang, became pregnant at 37 years while living in Hong Kong. She consulted with her Hong Kong doctor and learned that she was at risk of having a child with Down syndrome because of her age. Her doctor advised her to undergo amniocentesis. Zhang arranged an amniocentesis with her Hong Kong doctor, but the procedure was later postponed due to a later vaginal bleeding. Since Zhang had obtained a Canadian landed immigrant status and had planned with her ex-husband Fung to have the child in Canada, she and Fung flew from Hong Kong to Vancouver to consult Dr. Kan about the pregnancy.

During the meeting, Zhang requested an amniocentesis test and any other necessary examination but Dr. Kan advised that it would be too late for amniocentesis. After she informed Dr. Kan that she was at a high risk of having a baby with Down syndrome because of her age, Dr. Kan advised that the risk was not that high, but rather less than one in 1000. She requested that Dr. Kan hasten the procedure to which he explained that he would have to call up and arrange for an appointment and that before he was able to get an appointment, it would be too late. Dr. Kan later advised that since neither Zhang nor Fung had any health problems that the possibility of their having a baby with Down Syndrome would be even less. Zhang left Dr. Kan office feeling very questionable about his advice compared to all that she had read from Brochures and heard from her Hong Kong Doctor. She spoke to Fung, who was waiting outside about her doubts, but he told her to believe in the doctor.

Zhang and Fung subsequently had a daughter who was diagnosed with Down Syndrome. Following their divorce, Fung took on the care of the child with his second wife in California. The parties sought damages against Dr. Khan to compensate for the consequences of the child's condition and for Fung's expenditures incurred in California with respect to the Down syndrome. Dr. Kan argued against the claim on the basis that there were substantial agency resources in California which would provide the child with all the necessary medical services. The court ruled that Kan's failure to arrange for the amniocentesis for Zhang fell below the accepted standard of care and that he

[886] *Zhang v Kan*, 2003 BCSC 5. *RH v Hunter* (1996), 32 Canadian Cases on the Law of Torts (2d) 44 (ONGD).

could have arranged an amniocentesis on an expedited basis that would have disclosed the Down syndrome and would have enabled Zhang to terminate the pregnancy. The court also ruled that Zhang and Fung were 50 per cent negligent because they had a lot of information on the issue and knew that there might be a problem if the amniocentesis was not done, but made no effort to take the test. Zhang was awarded $10,000 and Fung $5,000 for his non monetary loss. Fung was further awarded $5,000 for the claim of past compensation and $171,926 (US Dollars) for future care. Given that the child was not a US Citizen and will not qualify for state benefits, Fung was awarded additional $21, 845 in that respect.

Raina v Shaw, [2006] BCJ No 1219

Mr. and Ms. Raina (the Rainas), the plaintiffs, brought an action against Dr. Shaw, the defendant, seeking damages for medical malpractice. The Rainas are parents to a son with Down Syndrome. They alleged that Dr. Shaw, Ms. Raina's family physician, failed to provide genetic counselling to Ms. Raina during her pregnancy, contrary to the standard of care required of British Columbia Physicians towards pregnant women of her age. They claimed that if the standard of care had been met, they would have obtained tests and made a decision to terminate the pregnancy.

Ms. Raina suspected that she was pregnant and went to see Dr. Shaw. During that visit, Dr. Shaw ran a simple urine test and confirmed the pregnancy. An appointment was then made for Ms. Raina for her first pre-natal visit. During the pre-natal visit, Dr. Shaw conducted a physical examination, took the family history and asked Ms. Raina questions regarding smoking, heart disease and high blood pressure. Ms. Raina claimed that genetic counselling did not come up at the meeting except that she was given a requisition form to take to a lab for blood sample purposes. Ms. Raina later cancelled some appointments and traveled to India. She testified in court that she asked Dr. Shaw if it was alright to travel, and obtained Dr. Shaw's permission.

Dr. Shaw, on the other hand, testified that her office would have provided Ms. Raina with a large blue folder as it is the office's usual practice. Dr. Shaw said that the blue folder would contain material from the Health District and a signed form that would entitle the patient to obtain a booklet titled Baby's Best Chance *from the Health District office, which contained information about pre-natal genetic testing. Dr. Shaw also testified that she informs her patients about three genetic tests; triple marker screening, amniocentesis and CVS. Dr. Shaw also took the position that she told Ms. Raina about the high risk for Down Syndrome and Chromosome Damage and asked that Ms. Raina should let her know what tests she chose. She testified that she was shocked to learn that Ms. Raina was overseas and had informed her assistant after Ms. Raina had missed three pre-natal visits that she needed to see Ms. Raina as soon as possible. Dr. Shaw testified that when Ms. Raina finally showed up, she asked if she had seen a doctor in India and she had indicated that she had not, and by that time, it was already too late to order the amniocentesis. The court ruled that the Rainas failed to establish any breach of standard of care, and that Dr. Shaw provided Ms. Raina genetic counselling at her first antenatal visit, and that the genetic counselling would have continued at the second visit if Ms. Raina had attended. The Rainas' claim was dismissed.*

6.5.4 Genetic Testing and Human Reproduction

MD v LL, [2008] OJ No 907

Surrogacy, genetic parents and the recognition of parentage.

M.D. and J.D. were married and could not bear children for medical reasons. M.D. and J.D. sought help from their family friends, L.L. and I.L. , a married couple who could bear children. The Parties entered into a Gestational Carriage Agreement. Under the agreement, L.L. agreed to act as a gestational carrier for M.D.'s Ova, which was fertilized with J.D.'s sperm. L.L. and M.D. would be the genetic parents of any child born as a result of this procedure.

L.L. gave birth to a child, E.D., in the summer of 2007 and was required to complete and file a Statement of Live Birth (the Statement) with the Registrar. The Statement required that L.L. place her name on the form as the mother of E.D., notwithstanding the agreement nor the fact that M.D. and J.D. were E.D.'s genetic parents. Consequently, M.D. and J.D. sought an order declaring them to be the mother and father of E.D., and L.L. and I.L. <u>not</u> the mother and father of E.D. They also sought an order directing the Deputy Registrar for the Province of Ontario to amend E.D.'s birth registration to reflect M.D. and J.D. as the parents.

L.L. and I.L did not oppose the Motion sought. The court ruled that M.D. and J.D. were the parents of the child. The court recognized them as the genetic parents of the child and no DNA testing was sought. The court also ruled that Section 4 of the Children's Law Reform Act gave the court jurisdiction to declare parentage. L.L. and I.L. were declared <u>not</u> to be the parents of the child. Although L.L. gave birth to the child, the court had jurisdiction to issued declaration of non-parentage based on section 4 of the Children's Law Reform Act.

N (K) v M (K.), 1989 (Supreme Court of Canada)[887]:

A case illustrating the increasing importance of genetic information in deciding custody cases.

Before emigrating to Canada with her family in 1962, Miss N had had a relationship with a young man that her parents did not approve of. When she arrived in Canada she was two months pregnant. In her Vietnamese culture and Catholic faith an unmarried pregnant woman was forever after unmarriageable. With the biological father presumed dead in the war, Miss N's family would have been burdened with her and her child's future maintenance. As pregnancy outside of marriage was disgraceful and dishonorable in

[887] *N (K) v M (KM)* (1989), 97 Alberta Reports 38 (ABQB) (1989) 100 Alberta Reports 1 (ABCA).

Miss N's culture, Miss N's family felt that their family's reputation could only be salvaged if the young mother's pregnancy was concealed from the Vietnamese community and the child placed for adoption outside of that community. A private adoption was arranged and the newborn immediately went to live with a two parent non-Vietnamese family. Four weeks after the baby was born, grieving for her baby and fortified by the news that the biological father was alive and waiting for medical clearance to be re-united with Miss N and their baby, Miss N contacted a lawyer to regain her child.

In determining what was best for the baby, to stay with the non-Vietnamese adoptive parents or be returned to the natural Vietnamese mother, the court found that both families presented an optimal environment in which to meet the baby's physical, spiritual and emotional needs. The deciding factor in this case turned out to be what was in the best interests of the baby's long-term psychological well being. Relying heavily on the testimony of a trained social worker and a child psychologist, the court was persuaded that cultural, racial and genetic factors would be of great importance to the baby's healthy psychological development, especially during adolescent identity development. The adoptive parents appealed this court's decision claiming that the lower court placed too much weight on cultural and genetic factors and too little on the two years of bonding between the child and the adoptive parents. Both the Court of Appeal and the Supreme Court of Canada stated that the first court used the correct test, considered all the information presented to it and, therefore, had not made any mistakes in coming to the decision to have the child returned to the biological, Vietnamese mother.

6.5.5 Genetic Testing in Criminal Cases

R v Ali, [2008] BCJ No 980

A case illustrating the court's discretion not to order a DNA sample.

The accused was born in Fiji and came to study in Canada in 1996. At the end of his studies, he obtained a diploma in Business Management and returned to Fiji. Thereafter, the accused re-entered Canada illegally. He saw a lawyer a day after his illegal immigration and reported himself to immigration authorities with the lawyer's assistance. He also maintained a biweekly report to the immigration authorities. The accused's father died in Fiji. The loss, and the fact that Fiji was unstable at the time, resulted in the accused's decision to leave and not to return to live in Fiji. The accused could not be an employee due to his immigration status so he ran his own business of repairing and selling automobiles, where he employed three people.

The accused subsequently became engaged in a dial-a-dope operation, with a co-accused who is also an addict. The operation involved accepting cocaine orders by phone and delivering the order by rental cars. Following their apprehension, the accused was found guilty of trafficking in cocaine, and for possession of cocaine for the purpose of trafficking. The Crown, among other things, sought an order for DNA sample and nine months imprisonment. The defense opposed the DNA order sought by the Crown, and asked the court for a conditional sentence. The defense also posited that the accused could be under electronic monitoring. The defense argued that the DNA sample might disclose the accused's condition as a diabetic to immigration official or uncover other medical problems and thus impact on his privacy and his chances of becoming a permanent resident.

The court accepted the Crown's submission that a term of imprisonment is more appropriate than a conditional sentence for the accused and sentenced him to six months imprisonment and 10-year weapons prohibition. The court, on the other hand, agreed with the defense that the DNA sample could represent a serious issue of privacy to the accused and impact on his chances of becoming a permanent resident. In reaching this decision, the court considered the facts that the accused had no criminal record, was a respected business and hardworking man, and the sole financial support for his wife, mother, four children and two step children as mitigating factors. As there was no indication that the accused used drug or was addicted to drugs, the court found greed to be the motivation for the crime.

***R v Rodgers*,** [2006] SCJ No 15

A case on the legality of the collection of DNA sample(s) for inclusion at the DNA databank. *The accused was sentenced to 4 years in prison for a sexual assault he committed while on probation from a conviction for sexual interference. He was not ordered to provide a DNA sample because his conviction took place before the* DNA Identification Act *was in force. However, before the expiration of the accused's sentence, the Crown applied to a judge for authorization ex parte (for a decision without requiring all of the parties involved being present), to take the accused's DNA samples for inclusion in the databank. The accused applied to the Ontario Court of Appeal for a declaration that the* Criminal Code *sections authorizing a DNA sample (s. 487.055) infringes his section 7, 8, and 11 rights under the* Canadian Charter of Rights and Freedoms*. In the alternative, he argued that the authorizing judge lost jurisdiction by proceeding ex parte. The Ontario Court of Appeal upheld the constitutional validity of the section but ruled that the lower court judge committed an error by hearing the application without the presence of the accused. The authorization was set aside. The Crown appealed to the Supreme Court where the accused also cross appealed on the constitutionality of the section.*

The majority of the Supreme Court ruled that the authorizing judge did not commit any error by proceeding without hearing the accused, and that the Ontario Court of Appeal was wrong in deciding that both parties should be heard. The Supreme Court also ruled that the Criminal Code *section did not infringe s. 7 or 8 of the* Charter. *The Court pointed out that while the taking of bodily samples for DNA analysis without consent constitutes a seizure under the* Charter*, that the collection of DNA samples for data bank purposes from designated classes of convicted offenders is reasonable. The Court differentiated the fact that the samples may only be used in order to create profiles in the DNA databank, and do not target suspected offenders nor particular offences, from the investigative DNA warrants, and considered the process similar manner to fingerprinting and other identification measures. The Court found that the accused had no reasonable expectation of privacy in respect of his identity and that since his identity as a multiple sex offender had become a matter of state interest, he had lost any reasonable expectation of privacy in the identifying information derived from DNA sampling. The data bank provisions were found to strike an appropriate balance between the public interest in the effective identification of persons convicted of serious offences and the rights of individuals to physical integrity and privacy.*

R v Good, 1995, (British Columbia Supreme Court)[888]:

The first criminal case to make use of forensic DNA legislation forcing a suspect to provide a blood sample.

In mid September of 1992, a man found his roommate dead in their apartment. He had been killed by being stabbed many times. The only clue left at the scene of the crime was some blood on the deceased's jeans, which did not belong to the deceased. For a long time the police were not able to make much progress in this case, because they had no suspect. Finally in mid 1994 police received some information from friends of Mr. Good that Mr. Good may have been involved in the stabbing. Wanting a sample from Mr. Good that would allow them to do DNA matching tests with the additional blood found on the victim's jeans, plain clothes officers set up a phony consumer products testing booth in a mall. They got Mr. Good to chew gum and discard it into a cup. This material was analyzed and although it pointed towards Mr. Good as being the source of some of the blood on the victim's clothing, the 1 in 41,000 match was thought to be relatively low in DNA testing standards.

In mid 1995, Bill C-104 was passed and allowed the police to apply for a special warrant to collect samples from suspects for DNA analysis. The police got such a warrant to collect a blood sample from Mr. Good and the analysis showed a one in several billion match rate with the other blood found on the victim's jeans which in scientific standards is a very high statistical result showing that Mr. Good was at the murder scene. Mr. Good claimed that the warrant for his blood sample was not valid because the law authorizing it came into being after the murder. The court, however, said that new laws about new procedures could be used on old cases.

[888] *R v Good,* [1995] BCJ No.2853 (QL) (BCSC).

Reference Re Milgaard, 1992 (Supreme Court of Canada)[889]

A case showing how forensic DNA testing can be used to exonerate a suspect.

Following a jury trial in 1970, David Milgaard was sentenced to life in prison for the death of Gail Miller, a nurse's aid who had been robbed, sexually assaulted and murdered in 1969. Mr. Milgaard appealed this conviction, but the Court of Appeal for Saskatchewan dismissed the appeal and the Supreme Court of Canada would not hear an appeal. Mr. Milgaard always professed that he did not kill Ms. Miller. In 1991, a second application for mercy was made to the Minister of Justice. This, along with the growing concern that there may have been a miscarriage of justice in the conviction of Mr. Milgaard, prompted the Governor in Council to refer the matter to the Supreme Court of Canada. In 1992, the Supreme Court of Canada reviewed the original trial proceedings and new evidence in the case against Mr. Milgaard. Although the Supreme Court of Canada was not satisfied beyond a reasonable doubt that Mr. Milgaard was innocent of the murder, they were satisfied that the new evidence could have affected the verdict if it had been known and presented at trial. A significant piece of information appeared to be evidence of sexual assaults committed by another person who confessed in 1970. The Court recommended that the Minister of Justice set aside the conviction and direct that a new trial be held. Once this was done, the Attorney General of Saskatchewan chose to suspend Mr. Milgaard's new trial. So Although Mr. Milgaard was released from prison in 1992, he was still not exonerated for Gail Miller's death. Finally in July of 1997, DNA testing revealed that the semen on the clothes that Ms. Miller was wearing at the time of her death was not Mr. Milgaard's. Mr. Milgaard negotiated a damage settlement with the Saskatchewan Justice Minister for his wrongful conviction and for spending 23 years in prison for a crime he did not commit. Another suspect has been charged for the death of Ms. Miller.

Had forensic DNA testing been available or been done earlier, Mr. Milgaard may not have spent as many, if any, years in prison for a crime that genetic science shows he did not commit.

[889] *Reference Re Milgaard* (1992), 135 National Reports 81; [1992] 3 Western Weekly Reporter 385 (SCC).

Appendix

PROVINCIAL PRIVACY LEGISLATION ACROSS CANADA

Every province and territory in Canada has some form of access to information and protection of privacy legislation. The legislation varies from province to province, but the rules regarding personal information are very similar in several. One significant difference is the role of the Commissioner. In some provinces and territories, the Commissioner has the authority to make decisions about access to information and privacy issues that government departments have to follow. In other provinces, he or she can only make recommendations that the government may or may not follow. The federal jurisdiction is an example where the Commissioner can only make recommendations to the appropriate government department. The access to information system in Alberta is an example of a province where the Commissioner can make decisions that the government has to follow.

ALBERTA

How is privacy protected in Alberta?

Access to information and protection of privacy in Alberta are governed by the *Freedom of Information and Protection of Privacy Act* [*FOIPP*][890], the *Health Information Act*[891], and the *Personal Information Protection Act* [*PIPA*].[892]

Who is covered by the FOIPP Act?

This legislation applies to the information (including employee information) collected by government bodies in Alberta. These include: departments, branches or offices of the Government of Alberta; educational bodies, such as universities and school boards; health care bodies, such as hospitals, some nursing homes, and other regional health authorities; law enforcement bodies, such as city police departments; and local government bodies, such as cities and municipalities.[893] Municipalities (e.g., cities), schools, universities, police departments and health care bodies have been under the *FOIPP Act* for only a few years. Each organization has its own special privacy issues and procedures. For example, in schools, one key issue is access to, collection of, disclosure of, and

---

[890] *Freedom of Information and Protection of Privacy Act* [*FOIPP*], RSA 2000, c F-25.
[891] *Health Information Act*, RSA 2000, c H-5.
[892] *Personal Information Protection Act* [*PIPA*], SA 2003, c P-6.5.
[893] *Freedom of Information and Protection of Privacy Act* [*FOIPP*], RSA 2000, c F-25, at sections 2.

correction of student records. Alberta Learning and various school boards have developed policies and procedures dealing with privacy issues.

Who is protected by PIPA?

This legislation applies to information collected by organizations/business in the private sector. This includes information collected from consumers and employees. *PIPA* protects individual privacy including the privacy of employees, by requiring private sector organizations/employers to obtain consent for the collection, use and disclosure of personal information, and providing individuals with a right to access their own information. *PIPA* has been deemed substantially similar to *PIPEDA* by the Federal Government. This means that *PIPA,* and not *PIPEDA,* will apply to all consumer information collected in Alberta.

BRITISH COLUMBIA

How is privacy protected in British Colombia?

Access to information and protection of privacy in British Colombia are governed by the *Freedom of Information and Protection of Privacy Act* [*FIPPA*],[894] the *Personal Information Protection Act* [*PIPA*],[895] the *Privacy Act*,[896] and the *E-Health* (*Personal Health Information Access and Protection of Privacy*) *Act* [*E-Health*].[897]

Who is protected by FIPPA and who is protected by PIPA?

In B.C. the privacy of persons employed by public bodies such as the Legislature, is protected by the *Freedom of Information and Protection of Privacy Act.* The privacy of person employed by the private sector is protected by the *Personal Information Protection Act*.

How does B.C.'s Privacy Act work?

The *Privacy Act* in B.C. creates a tort [cause of action] that allows someone to sue for a violation of their privacy.[898] No proof of damage is required. The *Act* specifically mentions the unauthorized use of, "name or portrait of another," defines privacy as that which is reasonable in the circumstances, and does not specifically outline available defenses.[899] The tort may be used by

[894] *Freedom of Information and Protection of Privacy Act* [*FOIPP*] RSBC 1996, c 165
[895] *Personal Information Protection Act* [*PIPA*], SBC 2003, c63.
[896] *Privacy Act*, RSBC 1996, c 373.
[897] *E-Health* (*Personal Health Information Access and Protection of Privacy*) *Act* [*E-Health*], SBC 2008, c 38.
[898] *Privacy Act*, RSB. 1996, c 373 at section 1(1).
[899] *Privacy Act*, RSBC 1996, c 373 at sections 1(1), 1(2), and 3(2).

someone who feels their privacy has been violated, including those that have been the victim of eavesdropping or surveillance regardless if trespass has taken place.[900]

SASKATCHEWAN

How is privacy protected in Saskatchewan?

In Saskatchewan, access to information and privacy protection are governed by the *Freedom of Information and Protection of Privacy Act* [*FIPPA*],[901] the *Local Authority Freedom of Information and Protection of Privacy Act,*[902] the *Health Information Protection Act*[903] and the *Privacy Act.*[904]

Who is protected under FIPPA and the Local Authority Act?

The *Freedom of Information and Protection of Privacy Act* [*FIPPA*] applies to provincial government institutions in Saskatchewan. It outlines what constitutes personal information, when this type of information can be collected and how it should be collected. *FIPPA* also outlines how private citizens can access information about themselves held by government institutions.[905] The *Local Authority Freedom of Information and Protection of Privacy Act* applies to records that are held by local authorities. It allows citizens to access records in the possession of local authorities including a municipality, any Board or Commission under the *Municipalities Act*, the Board of the Public Library, Regional Colleges, the University of Regina, any board or commission that receives more than 50% of its budget from the Government of Saskatchewan, etc.[906]

How does Saskatchewan's Privacy Act work?

The *Privacy Act* creates a civil action for the violation of an individual's privacy by another. The action does not need proof of damage, just proof of the violation.[907] The *Act* includes examples of privacy violations as well as applicable defenses and remedies.[908]

MANITOBA

How is privacy protected in Manitoba?

---

[900] *Privacy Act*, RSBC 1996, c 373 at section 1(4).
[901] *Freedom of Information and Protection of Privacy Act* [*FIPPA*], SS, 1990-91, c F-22.01.
[902] *Local Authority Freedom of Information and Protection of Privacy Act,* SS, 1990-91, c L-27.1.
[903] *Health Information Protection Act,* SS, 1999, c H-0.021.
[904] *Privacy Act,* RSS 1978, c P-24.
[905] *Freedom of Information and Protection of Privacy Act* [*FIPPA*], SS, 1990-91, c F-22.01, at sections 5-9.
[906] *Local Authority Freedom of Information and Protection of Privacy Act,* SS, 1990-91, c L-27.1, at section 2(f).
[907] *Privacy Act,* RSS 1978, c P-24 at section 2.
[908] *Privacy Act,* RSS 1978, c P-24, at sections 3, 4, and 7.

In Manitoba, access to information and protection of privacy are governed by the *Freedom of Information and Protection of Privacy Act* [*FIPPA*],[909] the *Personal Health Information Act*[910] and the *Privacy Act.*[911]

Who is protected by FIPPA?

FIPPA provides a legal right of access to records held by Manitoba public bodies and also provides for the protection of personal information collected, stored, used and disclosed by public bodies.[912]

How does Manitoba's Privacy Act work?

The *Privacy Act* creates a tort (a civil wrong) that is actionable in a court of law. This means that anyone in Manitoba that "substantially, unreasonably, and without claim of right, violates the privacy of another person commits a [wrong] against that person" and can be held accountable.[913] No proof of damage is required to bring the action; just proof that an individual's privacy has been violated. The *Privacy Act* outlines examples of what constitutes a violation of privacy and provides for a limited number of defenses.[914]

ONTARIO

How is privacy protected in Ontario?

In Ontario, privacy and access to information is governed by the *Freedom of Information and Protection of Privacy Act,*[915] the *Personal Health Information Protection Act,*[916] and the *Municipal Freedom of Information and Protection of Privacy Act.*[917]

Who is protected by Ontario privacy legislation?

Privacy legislation in Ontario protects information collected by public bodies. Each *Act* outlines when a public body is allowed to collect, use and disclose private information collected from citizens. This would include any private information collected from employees of public bodies.

---

[909] *Freedom of Information and Protection of Privacy Act* [*FIPPA*], SM 1997, c 50.
[910] *Personal Health Information Act,* SM 1997, c 51.
[911] *Privacy Act,* CCSM, c P125.
[912] Ombudsman Manitoba, Principles of Access and Privacy Legislation, https://www.ombudsman.mb.ca/info/access-and-privacy-division.html
[913] *Privacy Act,* CCSM, c P125, at section 2(1).
[914] *Privacy Act,* CCSM, c P125, at sections 3 and 5.
[915] *Freedom of Information and Protection of Privacy Act,* RSO 1990, c F. 31.
[916] *Personal Health Information Protection Act,* SO 2004, c 3, Sch A.
[917] *Municipal Freedom of Information and Protection of Privacy Act,* RSO 1990, c M. 56.

Ontario privacy legislation does not cover employee information collected by employers that are not considered public bodies.

QUEBEC

How is privacy protected in Quebec?

In Quebec, privacy and access to information is governed by *An Act Respecting the Protection of Personal Information in the Private Sector,*[918] and by *An Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information.*[919]

Who and what is covered by Quebec privacy legislation?

Quebec has legislation that covers the public sector and the private sector. The manner in which all personal information from citizens and employees is collected, used and disclosed is outlined in Quebec legislation. Each *Act* ensures confidentiality and allows individuals to access information about themselves held by public and private bodies. All employers must follow either the private sector *Act* or the public sector *Act* depending on the type of employer.

NEW BRUNSWICK

How is privacy protected in New Brunswick?

In New Brunswick, privacy and access to information is governed by the *Personal Health Information Privacy and Access Act.*[920] The *Personal Health Information Privacy and Access Act* applies to the information collected and managed by public bodies. The *Act* allows individuals to access information held by public bodies as well as information about themselves held by public bodies.

NEWFOUNDLAND & LABRADOR

How is privacy protected in Newfoundland & Labrador?

---

[918] *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1.
[919] *An Act Respecting Access to Documents held by Public Bodies and the Protection of Personal Information*, RSQ, c A-2.1.
[920] *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05.

In Newfoundland & Labrador, privacy and access to information is governed by the *Access to Information and Protection of Privacy Act, 2015,*[921] the *Privacy Act,*[922] and the *Personal Health Information Act*.[923]

How does Newfoundland & Labrador's Privacy Act work?

The *Privacy Act* creates a civil action for the violation of an individual's privacy by another. The action does not need proof of damage, just proof of the violation. The *Act* includes examples of privacy violations as well as applicable defenses and remedies.[924]

NOVA SCOTIA

How is privacy protected in Nova Scotia?

In Nova Scotia, privacy and access to information is governed by the Nova Scotia *Freedom of Information and Protection of Privacy Act.*[925] The *Freedom of Information and Protection of Privacy Act* applies to public bodies in Nova Scotia. The *Act* ensures that citizens can access personal information about them, prevents the unauthorized collection, use and disclosure of personal information by public bodies, and ensures that public bodies are directly accountable to the public.

PRINCE EDWARD ISLAND

How is privacy protected in P.E.I.?

In P.E.I., privacy and access to information is governed by the P.E.I. *Freedom of Information and Protection of Privacy Act*.[926] The purpose of the *Freedom of Information and Protection of Privacy Act* is to allow any person access to records held by a public body, to control how public bodies collect information from citizens, how the information is used and how it is disclosed. It also allows individuals to access information about themselves held by a public body.

---

[921] *Access to Information and Protection of Privacy Act, 2015* SNL 2015, c A-1.2.
[922] *Privacy Act,* RSN 1990, c.P-22.
[923] *Personal Health Information Act*, S. 2008, c P-7.01.
[924] *Freedom of Information and Protection of Privacy Act,* SNS 1993, c 5 at sections 4, 5, 6, and 7.
[925] *Freedom of Information and Protection of Privacy Act,* SNS 1993, c 5.
[926] *Freedom of Information and Protection of Privacy Act,* RSPEI 1988, c F-15.01.

NORTH WEST TERRITORIES, YUKON, NUNAVUT

How is privacy protected in the N.W.T., the Yukon and in Nunavut?

Each of the territories has enacted a similar *Access to Information and Protection of Privacy Act.*[927] Each *Act* applies to public bodies within the respective territory and protects individual privacy by giving the public the right to access public records, preventing the unauthorized collection, use or disclosure of information by a public body and giving individuals the right to access information about themselves held by a public body.

---

[927] *Access to Information and Protection of Privacy Act,* SNWT 1994, c 20; RSY 2002, c 1; SWNT (Nu) 1994 c 20.

GLOSSARY

Affidavit - A written or printed declaration or statement of facts, made voluntarily, and confirmed by the oath or affirmation of the party making it, taken before a person having authority to administer such oath or affirmation.

Arbitrator – A neutral third party who decides disputes on the basis of evidence which the parties to the dispute provide. In contrast with a Mediator, an arbitrator's decisions can sometimes be binding; that is, have the force of law.

Basket Clause – Clause intended to ensure that the document covers a larger number of persons or instances than are actually specified in the document.

Blood Warrants – These warrants are only available if there is a driving offence in which alcohol has been involved. With a blood warrant, a blood sample is collected and analyzed to determine the level of alcohol in an individual's bloodstream.

Breach – Encroachment of a right. Can also be called Infringement.

Breathalyzer – An instrument to measure alcohol content in the blood by analysis of a breath sample.

Burden of Proof – The level of proof required by one party to prove their case to a judge. In criminal law, the accuser (always the government) must prove their case "beyond a reasonable doubt". This is a very high level of proof which is in place to protect the innocent from conviction. In civil law (see Torts) the accuser (anyone) need only prove that they are right on "a balance of probabilities". This means that it is simply more likely than not that the accuser is correct and the other party is wrong.

Canadian Charter of Rights and Freedoms – The "Charter" was passed into law in 1982 and is part of the Constitution of Canada. The Charter sets out the fundamental rights and values of Canadians. As part of the Constitution, the Charter is a portion of the highest law in Canada.

Canadian Security Intelligence Service (CSIS) – CSIS is the government department that is responsible for Canada's national security. CSIS is not a law enforcement body, but a security and surveillance organization that delivers information to law enforcement agencies.

Case Law – The decisions of judges relating to particular matters in contrast to statute law. Case law is a source of law and forms legal precedents and is known as Common Law.

Coercion – Compelling by force or threats.

Collective Agreement – An agreement in writing between an employer or an employer's organization acting on behalf of employers, and a bargaining agent of employees acting on behalf of a unit of employees containing provisions respecting terms and conditions of employment and related matters.

Common Law – Law which relies for its authority on the decisions of the courts and is recorded in the law reports as decisions of judges along with the reasons for their decisions. See also, Case Law.

Conscriptive Evidence – Evidence that someone can be compelled to give e.g. a breath sample or a DNA sample.

Consent – Freely given agreement.

Contraband - In general, any property which is unlawful to produce or possess. Goods exported from or imported into a country against its laws. Articles, the importation or exportation of which is prohibited by law. Smuggled goods.

Contract - An agreement between two or more persons which creates an obligation to do or not to do a particular thing.

Criminal Code - Canada's list of laws that declare particular acts to be crimes and sets out punishments for those crimes.

Defamation - To defame is to attack the reputation or good name of someone. Can be written (libel) or spoken (slander) although written defamation is more serious.

Detention – Mandatory restraint.

Dial or Digital Recorders – The recording of the date, time, and length of telephone calls. The telephone number being called from and the number being called are also being recorded. Police must obtain a warrant for this type of surveillance if there is a reasonable expectation of privacy.

DNA – DNA stands for Deoxyribonucleic Acid. This is the basic building block of people. Every cell of the human body contains 46 chromosomes (23 from each parent) and each chromosome contains a long string of DNA. Different combinations of DNA create genes that determine many facets of the human body from hair and eye colour to height and any inherited diseases.

Disability – The absence of legal ability to do certain acts or enjoy certain benefits; The incapacity of a minor or of a person who is mentally incompetent; Any previous or existing mental or physical disability and include disfigurement and previous or existing dependence on alcohol or a drug.

Discrimination - Unfair treatment of a person or group, usually due to prejudice about that person's race, ethnic group, gender, religion, sexual orientation, or other characteristic.

Equality Before the Law – The principle by which the law must be applied to everyone equally and every member of society must be treated the same way before the law.

Evidence – Every means (testimony, writings, material objects, or other things presented to the senses) that are offered to prove the existence or nonexistence of a fact.

Ex Parte - A judicial proceeding, order, injunction, etc., is said to be ex parte when it is taken or granted at the instance and for the benefit of one party only, and without notice to, or contestation by, any person adversely interested.

Federal Court of Canada – This is where most litigation involving the Federal government (e.g. Revenue Canada and Federal Privacy Legislation) takes place. There are trial and appeal levels of the Federal Court.

Freedom of Information and Protection of Privacy Act – The Alberta "FOIP" act which applies to all provincial government bodies. The FOIP act controls, regulates access to and protects information held by the government.

Genetic Testing – Genetic testing covers a large range of procedures, including genetic screening (used to detect diseases or conditions which are inherited) genetic monitoring (used to detect genetic changes brought on by exposure to things such as chemicals or radiation) and forensic DNA analysis (used in criminal cases to determine if a sample left at crime scene matches with a sample collected by police).

Indictable Offence – One of two types of offence under the Criminal Code (the other being Summary Conviction). These are the more serious offences in the Criminal Code and are usually tried by provincial superior courts. Sentences usually include jail time. These offences are equivalent to Felonies in the United States.

Legal Aid – Legal advice and services made available or furnished under a legal aid act. Legal aid is usually available to those who cannot afford to hire a lawyer of their choice.

Legislation – The creation of law by government (federal, provincial or municipal); a collection of statutes, regulations, by-laws.

Liability – Where someone is actually or potentially subject to an obligation. When we drive, we are sometimes liable for accidents because we have an obligation to drive carefully. Not to be confused with libel (see Defamation).

Mass Surveillance – Monitoring large groups of people.

Mediator – A neutral third party who resolves and reconciles disputes. Unlike an Arbitrator, a mediator's recommendations can sometimes be taken as suggestions only, and are not always binding.

National Parole Board – A federal body with exclusive authority and final discretion to grant a temporary absence with no escort or parole under the Penitentiary Act, to terminate or revoke day parole for inmates in federal institutions and inmates in provincial institutions in the Atlantic and Prairie provinces.

Notwithstanding Clause – This is section 33 of the Charter which allows provinces to override sections of the Charter with legislation that would normally be of no force or effect. Governments do this when they enact legislation that is in force "notwithstanding" a certain section of the Charter, such as language laws in Quebec.

Oakes Test – Section 1 Analysis – The legal test created in the case *R. v. Oakes,* [1986] 1 S.C.R. 103, where the Supreme Court set out what constitutes a "reasonable limit" on a right, or a limit which can be "demonstrably justified in a free and democratic society". The test is a complex, three step process the Court uses to determine if a right can be infringed by the government.

Personal Surveillance – Monitoring one individual.

Privacy Commissioner of Canada – The federal official who investigates complaints of government failure to comply with rights to personal information provided by the Privacy Act.

Private Sector – Businesses and corporations. The private sector can also be that which is not the government, or the Public Sector.

Publication Ban – An order that a judge can make to protect sensitive information as well as protect the identity of a witness or a party in a case. The media is never allowed to publish the names of persons under the age of 18.

Public Sector – The government and its departments, ministries and agencies.

Recidivism – Habitual relapse into crime.

Remedy – The means by which one redresses, prevents or compensates the violation of a right. Can be monetary, but can also include actions such as "striking down" a law, "severing" the offending portion of a law from the healthy portion, "reading in" new language to expand the law or "reading down" the law to make it comply with the Charter.

Residual Management Rights – Gives management (employers) the right to manage those areas which have not been addressed in an employment contract or an agreement between the workers and the employer (such as a collective agreement). Employers often rely on their Residual Management Rights for authority to use surveillance.

Resort to Clause – This clause is found in a warrant applied for by CSIS to receive permission to intercept the communications of a specific person both at a place named in the warrant and also at places to which the person is believed to have gone or will go.

Right(s) – A "right" can be an entitlement, freedom or privilege to do something (right to privacy, freedom of speech or the right to vote for example). A right can also be a freedom from something as well (a right to be free from unreasonable search and seizure).

Search – Search under section 8 of the Canadian Charter of Rights and Freedoms should be given a broad meaning to include a search of a person, a place or vehicle. It should include searches not only by the direct act of a police officer, say on executing

a search warrant, but also by interception of private oral communications by electronic devices under Part IV.I of the Code.

Search Warrant – An order in writing which a justice issues under statutory powers to authorize a named person to enter a certain place to search for and seize any property that will provide evidence of the intended or actual commission of a crime.

Statute – A law or act that expresses the will of Parliament (the federal government) or a legislature (provincial government).

Strict Liability Offence – Imposed in tort law when a lawful activity exposes others to extraordinary risks even though no fault is involved on the part of the "wrongdoer." For example, transporting dangerous chemicals or explosives exposes a person to strict liability, as any accident could endanger a great deal of people.
Subpoena - A subpoena is a command to appear at a certain time and place to give testimony upon a certain matter.

Summary Conviction Offence – One of two types of offence under the Criminal Code (the other being Indictable offence). Summary Conviction offences are usually less serious than Indictable offences, are usually tried by lower level courts and sentences may not include jail time. These offences are equivalent to Misdemeanors in the United States.

Supreme Court of Canada – Located in Ottawa, this is the general court of appeal for all of Canada, the final interpreter of all Canadian law, whatever its source. The Court is made up of nine judges or "justices".

Surveillance - Police investigative technique involving visual or electronic observation or listening directed at a person or place. Its objective is to gather evidence of a crime or merely to accumulate intelligence about suspected criminal activity.

Tracking Devices – Devices which have been installed to monitor movement are an invasion of one's reasonable expectation of privacy. The police can apply for a warrant allowing them to use this technique.

Torts – A "civil wrong" (as opposed to a criminal offence). A tort usually allows a person to collect damages (usually money) for a perceived injury (to property or person).

Video Surveillance – If a person has a reasonable expectation of privacy, then any unauthorized surreptitious video surveillance of them is considered a search that breach Section 8 of the *Charter* even if the person under surveillance is doing an illegal act. The police can apply for a warrant under the *Criminal Code* to use video surveillance.

Visitor Clause – This type of clause is found in an application by the CSIS for a warrant that would give CSIS investigators a warrant for surveillance of a class of persons merely described by CSIS investigators by their nationality, as a visitor to Canada, those identified in CSIS data banks as being known intelligence officers, and/or those for whom there were reasonable grounds to believe they would engage in espionage or other threat related activity while they were in Canada. These types of warrants are unlikely to be granted.

Windfall Evidence – Communications being legally wiretapped that turn up information of other crimes that are not listed. This evidence could also be used to prosecute the additional offence.

Wiretapping - A form of electronic eavesdropping where, upon court order, enforcement officials secretly listen to phone calls.

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 fulfill 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 the Limiting Collection principle (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.

OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities

16. **Video surveillance should only be deployed to address a real, pressing and substantial problem.**

    The problem to be addressed by video surveillance must be pressing and substantial, of sufficient importance to warrant overriding the right of innocent individuals to be free from surveillance in a public place. Accordingly, concrete evidence of the problem to be addressed is needed. This should include real evidence of risks, dangers, crime rates, etc. Specific and verifiable reports of incidents of crime, public safety concerns or other compelling circumstances are needed, not just anecdotal evidence or speculation.

17. **Video surveillance should be viewed as an exceptional step, only to be taken in the absence of a less privacy-invasive alternative.**

Less privacy-invasive alternative ways of addressing the identified problem should be chosen unless they are not feasible or significantly less effective.

18. **The impact of the proposed video surveillance on privacy should be assessed before it is undertaken.**

    A Privacy Impact Assessment of the proposed video surveillance should be conducted to determine the actual or potential kind and degree of interference with privacy that will result, and the ways in which adverse effects will be mitigated.

19. **Public consultation should precede any decision to introduce video surveillance.**

    Public consultation should be conducted with relevant stakeholders, including representatives of communities that will be affected. "Community" should be understood broadly; it should be recognized that a particular geographic area may have several distinct communities, and one community should not be presumed to speak for the others.

20. **The video surveillance must be consistent with applicable laws.**

    Video surveillance must be conducted in accordance with all applicable laws, including overarching laws such as the *Canadian Charter of Rights and Freedoms* and Quebec's *Charter of Human Rights and Freedoms*.

21. **The video surveillance system should be tailored to minimize the impact on privacy.**

    The surveillance system should be designed and operated so that the privacy intrusion it creates is no greater than absolutely necessary to achieve the system's goals. For example, limited use of video surveillance (e.g., for limited periods of day, public festivals, peak periods) should be preferred to always-on surveillance if it will achieve substantially the same result.

22. **The public should be advised that they will be under surveillance.**

    The public should be informed with clearly written signs at the perimeter of surveillance areas, which advise that the area is or may be under surveillance, and indicate who is responsible for the surveillance, including who is responsible for compliance with privacy principles, and who can be contacted to answer questions or provide information about the system.

23. **Fair information practices should be respected in collection, use, disclosure, retention and destruction of personal information.**

    The information collected through video surveillance should be minimal; its use should be restricted, its disclosure controlled, its retention limited, and its destruction assured. If a camera is manned, the recording function should only be turned on in the event of an observed or suspected infraction. If a camera records continuously, the recordings should be conserved for a limited time only, according to a retention schedule, unless they have captured a suspected infraction or are relevant to a criminal act that has been reported to the

police. Information collected through video surveillance should not be used for any purpose other than the purpose that the police force or public authority has explicitly stated in the policy referred to in 14 below. Any release or disclosure of recordings should be documented.

24. **Excessive or unnecessary intrusions on privacy should be discouraged.**

    Surveillance cameras should not be aimed at or into areas where people have a heightened expectation of privacy: for example, windows of buildings, showers, washrooms, change rooms, etc. If cameras are adjustable by an operator, reasonable steps should be taken to ensure that they cannot be adjusted or manipulated to capture images in areas that are not intended to be under surveillance.

25. **System operators should be privacy-sensitive.**

    The operators of surveillance systems, including operators hired on contract, should be fully aware of the purposes of the system, and fully trained in rules protecting privacy.

26. **Security of the equipment and images should be assured.**

    Access to the system's controls and reception equipment, and to the images it captures, should be limited to persons authorized in writing under the policy referred to in 14 below. Recordings should be securely held, and access within the organization limited to a need-to-know basis.

27. **The right of individuals to have access to their personal information should be respected.**

    People whose images are recorded should be able to request access to their recorded personal information. Under many privacy statutes, they have a right of access. Severing the personal information in a recording (including technological blurring or blocking of the identities of others) may be necessary to allow individual access. Policies and procedures should be designed to accommodate these requests.

28. **The video surveillance system should be subject to independent audit and evaluation.**

    The system's operations should be subject to frequent audit, and its effectiveness should be evaluated regularly to identify unintended negative effects. Audit and evaluation should be conducted by persons or organizations independent of the management and direction of the video surveillance system. Audits should ensure compliance with the policy governing the system, including ensuring that only pertinent information is collected, that the system is used only for its intended purpose, and that privacy protections in the system are respected. Evaluation should take special note of the reasons for undertaking surveillance in the first place, as determined in the initial statement of the problem and the public consultation, and determine whether video surveillance has in fact addressed the problems identified at those stages. Evaluation may indicate that a video surveillance system should be terminated, either because the problem that justified it in the first place is no longer significant, or because the surveillance has proven ineffective in addressing the problem. Evaluation should take into

account the views of different groups in the community (or different communities) affected by the surveillance. Results of audits and evaluations should be made publicly available.

29. **The use of video surveillance should be governed by an explicit policy.**

    A comprehensive written policy governing the use of the surveillance equipment should be developed. The policy should clearly set out:

    - the rationale and purpose of the system
    - the location and field of vision of equipment
    - the rationale and purpose of the specific locations of equipment and fields of vision selected
    - which personnel are authorized to operate the system
    - the times when surveillance will be in effect
    - whether and when recording will take place
    - the place where signals from the equipment will be received and monitored, and
    - the fair information principles applying to recordings, including
        - security
        - use
        - disclosure
        - retention and destruction
        - rights of individual access to personal information captured, and
        - rights to challenge compliance

    The policy should identify a person accountable for privacy compliance and privacy rights associated with the system. The policy should require officers, employees and contractors to adhere to it, and provide sanctions if they do not. It should provide a process to be followed in the event of inadvertent privacy and security breaches. Finally, it should provide procedures for individuals to challenge compliance with the policy.

30. **The public should have a right to know about the video surveillance system that has been adopted.**

    Police forces and public authorities should recognize that individuals will want information about video surveillance systems. They may seek to know, for example, who has authorized the recording, whether and why their images have been recorded, what the images are used for, who has access to them, and how long they are retained. Police forces and public authorities should be prepared to provide this information."

NON-GOVERNMENTAL PRIVACY WEBSITES and RESOURCES

CANADIAN SITES:

BRITISH COLUMBIA FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION (FIPA): www.fipa.bc.ca

FIPA provides public legal education, public assistance, legal and policy research, and law reform on freedom of information and privacy issues. In the process of being built.

ALBERTA CIVIL LIBERTIES RESEARCH CENTRE
www.aclrc.com
A non-profit, non-governmental organization that deals with issues of fundamental civil liberties and human rights across Canada.

CANADIAN ACCESS AND PRIVACY ASSOCIATION: www.capa.ca
The CAPA website contains links and information concerning CAPA's conferences. Good Canadian resource.

CANADIAN CIVIL LIBERTIES ASSOCIATION
www.ccla.org
A non-profit, non-governmental organization that deals with issues of fundamental civil liberties and human rights across Canada.

CANADIAN PRIVACY LAW
http://www.privacyinfo.ca/ Professor Michael Geist plus law students maintain a site that contains summaries of Canadian Privacy Commissioner's decisions, fully searchable by keywords, statute section number, industrial sector or outcome. Site also contains links to statute, regulations, and legislative history, together with other resources.

ELECTRONIC FRONTIERS: www.efc.ca
Electronic Frontier Canada (EFC) was founded to ensure that the principles embodied in the Canadian Charter of Rights and Freedoms remain protected as new computing, communications, and information technologies are introduced into Canadian society. This is a great Canadian site containing good information and links.

MEDIA AWARENESS NETWORK: http://www.media-awareness.ca/

This is a great Canadian site pertaining to privacy issues. The site contains links and information on a wide variety of privacy issues, not just those concerning the media.
INTERNATIONAL SITES:

CENTER FOR DEMOCRACY AND TECHNOLOGY:www.cdt.org
CDT is an information resource and an advocate for change concerning privacy issues related to technology.

ELECTRONIC FRONTIER FOUNDATION: www.eff.org

The EFF is a San Francisco based rights advocate and educator. They lobby for privacy concerns to be included in legislation worldwide. The site contains great links as well as good coverage of issues and concerns.

ELECTRONIC PRIVACY INFORMATION CENTRE: www.epic.org/crypto
EPIC is a database of news and opinion on information and privacy issues.
Relating mainly to the United States, there is some international content.

HEALTH PRIVACY PROJECT: www.healthprivacy.org
The Health privacy Project is an initiative of Georgetown University. The site contains information and links concerning health issues and privacy concerns surrounding emergent technology**.**

ON-LINE PRIVACY ALLIANCE: www.privacyalliance.org
The On-Line Privacy Alliance is a group of businesses that have come together to advocate for changes to privacy laws. They also provide education on current issues. A good source for business oriented information.

PRIVACY EXCHANGE: www.privacyexchange.org
The Privacy exchange touts itself as an "online global exchange of resources" and it does this very well. The site contains information and links concerning a huge range of global privacy issues.

PRIVACY INTERNATIONAL: www.privacyinternational.org
Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI has conducted campaigns throughout the world on issues ranging from wiretapping and national security activities, to police information systems, and medical privacy.

PRIVACY JOURNAL: http://www.privacyjournal.net/
Privacy Journal is a monthly newsletter reporting on new technology and its impact on personal privacy. A Washington D.C. lawyer who specializes in privacy issues publishes the Journal, and this site contains great links and a wide variety of information.

PRIVACY RIGHTS CLEARING HOUSE: www.privacyrights.org
The Privacy Rights Clearinghouse is a non-profit consumer education, research, and advocacy program based in San Diego. This is an excellent site with information and links concerning a wide variety of subjects.

Canadian Government Websites

Offices of the privacy commissioner or ombudsman responsible for privacy in:
Canada: http://www.priv.gc.ca/

Alberta: http://www.oipc.ab.ca

British Columbia: http://www.oipc.bc.ca/

Manitoba: http://www.ombudsman.mb.ca/access.htm

New Brunswick: http://www.info-priv-nb.ca/

Newfoundland and Labrador: http://www.oipc.nl.ca/

Nova Scotia: http://foipop.ns.ca//

Ontario: http://www.ipc.on.ca/english/Home-Page/

Prince Edward Island:
http://www.gov.pe.ca/attorneygeneral/index.php3?number=1024336&lang=E

Quebec (English): http://www.cai.gouv.qc.ca/index-en.html

Saskatchewan: http://www.oipc.sk.ca/

Nunavut: http://www.info-privacy.nu.ca/en/home

Yukon: http://www.ombudsman.yk.ca/

SELECTED BIBLIOGRAPHY

Privacy Generally

Austin, L., "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006), 56 *University of Toronto Law Journal*, 181.

B.C. Civil Liberties Association *Privacy: Why it's Important, and How to Protect it (Web only)*, BC Civil Liberties Association, http://www.bccla.org/privacy/privacymain.html .

Brown, R., "Privacy Law Rethinking Privacy: Exclusivity, Private Relation and Tort Law" (2006), 43 *Alberta Law Review*, 589 – 614.

Bruyer, R., "Privacy: A Review and Critique of the Literature" (2006), 43 *Alberta Law Review*, 553 – 588.

Fraser, D., *The Canadian Privacy Law Blog: Developments in privacy law and writings of a Canadian privacy lawyer, containing information related to the Personal Information Protection and Electronic Documents Act (aka PIPEDA) and other Canadian and international laws*: http://blog.privacylawyer.ca/ .

Gotell, L., "Privacy Law When Privacy is Not Enough: Sexual Assault Complainants, Sexual History Evidence and the Disclosure of Personal Records" (2006), 43 *Alberta Law Review*, 743 – 778.

Levin, A., and Nicholson, M., "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground" (2005), 2:2 *University of Ottawa Law and Technology Journal*, 357.

McIssac, B., Shields, R., and Klein, K., *The Law of Privacy in Canada*, Canada: Carswell, 2004.

Office of the Information and Privacy Commissioner, *Public-sector Outsourcing and Risks to Privacy*
Alberta (2006): http://www.assembly.ab.ca/lao/library/egovdocs/2006/alipc/153159.pdf

Office of the Information and Privacy Commissioner, ***Health Information - A Personal Matter: A Practical Guide to the Health Information Act Alberta***: https://www.oipc.ab.ca/media/383665/practical_guide_to_hia_aug2010.pdf

Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2009 – Report on the Personal Information Protection and Electronic Documents Act*, (2010): https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/200910/2009_pipeda/ .

Office of the Privacy Commissioner of Canada*, 2010-2011 - Report on Plans and Priorities,* (2010): http://www.tbs-sct.gc.ca/rpp/2010-2011/inst/nd6/nd600-eng.asp .

Office of the Privacy Commissioner of Canada, Your *guide to PIPEDA: The Personal Information Protection and Electronic Documents Act*. Office of the Privacy Commissioner of Canada, *Leading*

By Example: Key Developments in the first Seven years of the Personal Information Protection and Electronic Documents Act (PIPEDA), (2008).

Paton-Simpson, E., "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000), 50 *University of Toronto Law Journal* 305.

Renke, W. N., and Racicot, M., "Privacy Law Introduction" (2006), 43 *Alberta Law Review*, 549 – 551.

Roy, B., "A Case Against Biometric National Identification Systems (NIDS): 'Trading-Off' Privacy Without Getting Security" (2005), 19 *Windsor Review of Legal and Social Issues*, 45.

Rozenberg, J., *Privacy and the Press* New York: Oxford University Press, 2004.

Service Alberta and the Office of the Information and Privacy Commissioner Alberta*, A Guide for Businesses and Organizations on the Personal Information Protection Act,* Alberta, (2008): https://www.oipc.ab.ca/resources/guide-for-businesses-and-organizations-on-the-personal-information-protection-act-guide.aspx .

Warren, S. D. and Brandeis, L.D., "The Right to Privacy" (1890) *Harvard Law Review* 193.

Wood, C., "Do You Know Who's Watching You?" (February 19, 2001) 114(8) Maclean's 20.

Reasonable Expectation of Privacy

Jochelson, R., "Trashcans and Constitutional Custodians: The Liminal Spaces of Privacy in the Wake of Patrick" (2009), 72 *Saskatchewan Law Review*, 199 – 222.

Luther, G., "Consent Search and Reasonable Expectation of Privacy: Twin Barriers to the Reasonable Protection of Privacy in Canada" (2008), 41 *University of British Columbia Law Review* 1 – 29.

Mackinnon, W., "Tessling, Brown, and A.M.: Towards a Principled Approach to Section 8" (2007), 45 *Alberta Law Review* 79 – 116.

Privacy and Anti-Terrorism

Danlies, R., Macklem, P., and Roach, K., eds. *The Security of Freedom: Essays in Canada's Anti-Terrorism Bill* Toronto: University of Toronto Press, 2001.

Davies, A., "Invading the Mind: The Right to Privacy and the Definition of Terrorism in Canada" (2006), 3:1 *University of Ottawa Law and Technology Journal* 249.

Hughes, Dr. P., "Putting the Anti-Terrorist Legislation into Perspective" (2002), 8(1) Centrepiece 1.

Renke, W., "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy" (2006), 43 *Alberta Law Review* 779 – 823.

Swaigen, J., "Anti-Terrorism Initiatives Erode Privacy" September 2002, 3(1) Ontario Bar Association Personally Yours 5.

Privacy in the Education Context

Brown, A., and Zuker, M., *Education Law*, 2d ed. Scarborough: Carswell, 1998.

Monahan, T. (Ed), *Schools Under Surveillance: Cultures of Control in Public Education*. New Jersey: Rutgers University Press, 2010.

Rowen, K., "The Supreme Court of Canada Rules on the Use of Drug-Sniffing Dogs in Schools" (2008), 18 *Education and Law Journal* 83.

Steeves, V., "It's Not Child's Play: The Online Invasion of Children's Privacy" (2006), 3 *University of Ottawa Law and Technology Journal* 169.

Privacy in the Health/Medical Context

Baliey, T., and Penney, S., "Healing, not Squealing: Recent Amendments to Alberta's Health Information Act" (2007), 15 *Health Law Journal No. 2*, 3 – 14.

Bokenfohr, B., "Police Experience with the Health Information Act: The Edmonton Police Service's Submissions to the Select Special Health Information Act Review Committee" (2005), 14 *Health Law Review Rev. No. 1*, 9 – 11.

Florencio, P., and Ramanathan, E., "Secret Code: The Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination
Based on Genetic and Health Information" (2001), 39 *Osgoode Hall Law Journal* 77 – 116.

Gerlach, N., *The Genetic Imaginary: DNA in the Canadian Criminal Justice System* Toronto: University of Toronto Press, 2004.
Gibson, E., "Health Law in the 21st Century Is There a Privacy Interest in Anonymized Personal Health Information?" (2003), *Health Law Journal* 97 – 112.

Gibson, E., "Jewel in the Crown? The Romanow Commission Proposal to Develop a National Electronic Health Record System" (2003), 66 *Saskatchewan Law Review* 647 – 665.

Kosseim, P., and Brady M., "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes" (2008), 2 *McGill Journal of Law and Health* 5-45.

Kosseim, P., "The Landscape of Rules Governing Access to Personal Information for Health Research: A View from Afar" (2003), 11 *Health Law Journal* 199 – 216.

Parfett, J., "Canada's DNA Databank: Public Safety and Private Costs" (2002), 29 *Manitoba Law Journal* 33 – 80.

Ries, N., "Patient Privacy in a Wired (and Wireless) World: Approaches to Consent in the Context of Electronic Health Records" (2006), 43 *Alberta Law Review* 681 – 712.

Von Tigerstrom, B., Nugent, P., and Cosco, V., "Alberta's Health Information Act and the Charter: A Discussion Paper" (2000), 9 *Health Law Review No. 2*, 3-2.

Privacy and Surveillance

Cockfield, A., "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies" (2007), 40 *University of British Columbia Law Review,* 41 – 67.

Cockfield, A., "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance" (2003), 29 *Queen's Law Journal*, 364 – 407.

Forster, N., "Electronic Surveillance, Criminal Investigations, and the Erosion of Constitutional Rights in Canada: Regressive U-Turn or a Mere Bump in the Road Towards Charter Justice?" (2010), 73 *Saskatchewan Law Review*, 23 – 73.

Lai, D., "Public Video Surveillance by the State: Policy, Privacy Legislation, and the Charter" (2007), 45 Alberta Law Review 43 – 77.

Minuk, L., "Why Privacy Still Matters: The Case Against Prophylactic Video Surveillance in For-Profit Long-Term Care Homes" (2006), 32 *Queen's Law Journal*, 224 – 277.

Monahan, T. (Ed), *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Taylor and Francis Group LLC, 2006.

Privacy International, *Leading surveillance societies in the EU and the World 2007: The 2007 International Privacy Ranking* (2007), http://observatoriodeseguranca.org/files/phrcomp_sort.pdf .

Privacy and Technology

Alberta Civil Liberties Research Centre, *Techno-tonomy: Privacy, Autonomy and Technology in a Networked World,* Alberta Civil Liberties Research Centre, 2007.

Dubrovsky, D., "Protecting Online Privacy in the Private Sector: Is There a 'Better' Model?" (2005), 18 *Review Quebecois de Droit International no 2* 171 – 186.

Ford, W., and Baum, M.S., *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption* New Jersey: Prentice Hall, 2001.

Goldie, J., "Virtual Communities and the Social Dimension of Privacy" (2006), 3:1 *University of Ottawa Law and Technology Journal* 133.

Leuprecht, P., "Brave New Digital World? Reflections on the World Summit on the Information Society" (2005) 18 *Review Quebecois de Droit International* no. 1, 41 – 56.

MacDonnell, J., "Exporting Trust: Does E-Commerce Need A Canadian Privacy Seal of Approval?" (2001), 39 Alberta Law Review 346 – 440.

Scassa, T., Chiasson, T., Deturbide, M., and Uteck, A., "Consumer Privacy and Radio Frequency Identification Technology" (2005-2006), 37 *University of Ottawa Law Review* 215-248.

Solove, D., *Information Privacy Law* Aspen Publishing, 3rd ed. 2009.

Solove, D., *The Digital Person: Technology and Privacy in the Information Age* New York: New York University Press, 2004.
Solove, D., *Understanding Privacy* Harvard University Press, 2008.

Privacy at the Workplace

Anderson, S., "Privacy Law Alberta's Statutory Privacy Regime and its Impact on the Workplace" (2006), 43 *Alberta Law Review* 647 – 680.

Debeer, J., "Employee Privacy: The Need for Comprehensive Protection" (2003), 66 *Saskatchewan Law Review* 383 – 418.

Makela, F., "The Drug Testing Virus" (2009), 43 *Revue Juridique Themis*, 651 – 706.

Moulton, D., "Workplace Email Raises Liability, Privacy Concerns" (2001), Volume 20 Number 39 *The Lawyers Weekly* 11.
Pearce, C., "Balancing Employer Policies and Employee Rights: The Role of Legislation in Addressing Workplace Alcohol and Drug Testing Programs" (2008), 46 *Alberta Law Review* 141 – 172.

Poirier, M., "Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?" (2002), 60 *University of Toronto Faculty of Law Review* No. 2.