REPORT FOR THE CULLEN COMMISSION ON PRIVACY LAWS AND INFORMATION SHARING

Barbara McIsaac Law

https://mcisaaclaw.com/

barbara@mcisaaclaw.com

613-797-1897

November 17, 2020

Introduction

I have been asked by the Commission of Inquiry into Money Laundering in British Columbia (Cullen Commission) to prepare a report on the privacy and other laws impacting the flow of information, particularly personal information, between various private and public sector entities that either have a role in combatting money laundering in Canada or that may have information relevant to combatting money laundering activity in British Columbia specifically.

In doing so, I have looked at the privacy regimes in the Province of British Columbia and at the federal level that may impact the sharing of personal information by both private sector and public entities. Specifically, I have reviewed the following:

- British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA);
- British Columbia *Personal Information Protection Act* (PIPA);
- British Columbia *Privacy Act*;
- Federal *Privacy Act*;
- Federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

I have also reviewed the sectoral regulatory schemes that might impact the sharing of information generally, including personal information, for the following sectors:

- Banks regulated by the *Bank Act*
- Cooperative credit societies, savings and credit unions, both provincially and federally regulated
- Trust and loan companies both provincially and federally regulated
- Securities dealers
- Securities Commission
- Land Title and Survey Authority
- Money Services businesses, including, foreign exchange dealers, businesses engaged in remitting funds or transmitting funds, businesses engaged in issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments; and businesses dealing in virtual currencies;
- Dealers in precious metals
- Casinos, Lotteries, Gaming and Horseracing;
- Lawyers
- Chartered accountants
- BC Notaries
- Real estate agents
- Mortgage brokers
- Motor vehicle dealers

For the purposes of this report, I have adopted the definition of money laundering as set out on the website of the Financial Transactions and Reports Analysis Centre (FINTRAC).[1]

> Under Canadian Law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means most serious offences under the *Criminal Code* or any other federal Act. It includes, but is not limited to those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement.

The term "combatting money laundering" as used in this report, refers to the detecting, preventing and deterring of money laundering as well as facilitating investigations and prosecutions of money laundering activity. Again, referring to the FINTRAC website, this involves the collection, analysis and disclosure of information which will assist in the combatting of money laundering.

Limitation of this Report

By way of this introduction, a caution must be added regarding the scope of this Report. This Report is only intended to be a general canvassing of the legislative and common law restrictions that may constrain the ability of the entities discussed to disclose personal or other information, the disclosure of which might aid authorities in the combatting money laundering. It must be understood that, just because there is no legal impediment to information, personal or otherwise, being disclosed, particularly to law enforcement authorities, does not guarantee it will be admissible in court. The standard of admissibility in court for the purposes of a criminal proceeding has been set by the Supreme Court of Canada in cases such as *R v Spencer*[2], *R v Cole*[3], *R. v Jones*[4] and *R. v. Marakahf.*[5]

[1] https://www.fintrac-canafe.gc.ca/guidance-directives/overview-apercu/Guide1/1-eng#s2-3. This report does not focus on terrorist financing as a separate activity from money laundering, but my observations and conclusions are likely to apply to terrorist financing activity as well.
[2] [2014] 2 SCR 212.
[3] [2012] 3 SCR 34.
[4] [2017] 2 SCR 696.
[5] [2017] 2 SCR 608.

See *R. v. James*[6] for a case which addresses this issue in the context of information used in the investigation of money laundering and the interaction with the *Personal Information Protection and Electronic Documents Act.*[7]

A review of the constraints that may be placed on law enforcement authorities in the use of information for the purposes of investigating or prosecuting an alleged money laundering offence is beyond the scope of this Report.

Overview

While there may be an assumption among some that privacy laws in Canada act to deter the disclosure of personal information related to combatting money laundering, it is my view that, properly understood, they do not prohibit such activity. These laws have specific provisions outlining how such disclosures can be done lawfully while respecting individuals' personal privacy, thus providing a guide and assurance for would-be information sharers and users alike.

On the other hand, since their focus is privacy and the protection of personal information, none of the privacy regimes that I have examined encourage the sharing of personal information in any circumstance, including sharing for the purpose of combatting money laundering. Generally the provisions that allow for the sharing of personal information are discretionary, not mandatory. Accordingly, the principal way in which Canadian privacy laws may be detrimental to combatting money laundering is in their perception. Without clear guidance as to when information sharing is permitted, potential information sharers will be more likely to err on the side of caution and default to the position of non-disclosure. In this sense, in order to better combat money laundering in Canada, public bodies and private organizations need to have a better understanding of the current laws and clearer direction from regulators as to when information sharing for the purposes of combatting money laundering will be acceptable. If the relevant public and private organizations which are likely to have information related to money laundering better understand their options under these legislative regimes, they may be more likely to cooperate in the sharing of personal information, particularly the voluntary sharing of such information.

---

[6] 2013 ONSC 5085.
[7] See the discussion below regarding this legislation, particularly in connection with paragraph 7 (3) (d).

The sort of "safe harbour" provisions which are discussed in this report, and which have been recommended by the Canadian Bankers' Association, among others, may act to provide both public bodies and private organizations with more confidence that they will be protected from liability or censure by a regulator if they act in good faith when they share information, including personal information, for the purposes of combatting money laundering. Such provisions would likely be a welcome addition to both the public and private sector privacy regimes. It may also be worthwhile considering whether sectoral legislative regimes would benefit from similar provisions and clarification as to when non-personal information can be shared for the purpose of combatting money laundering.

Privacy Legislation

Introduction

Generally speaking, privacy legislation, whether it is applicable to the public sector or to private sector entities, and whether in Canada or international, is aimed at regulating the collection, use, disclosure and ultimate retention/destruction of personal information.

What is Personal Information?

Generally, Personal Information is defined as information about an identifiable individual. It may include information about:

- Race, national or ethnic origin;
- Age, marital status;
- Gender, sexual orientation;
- Medical, DNA profile;
- Education, employment history;
- Financial information;
- Identifying numbers such as drivers' licence, social insurance number, health card number;
- Views and opinions of others about you;
- Your views and opinions if expressed in a personal capacity.

The information may be recorded in some form or not. Each legislative initiative tends to have a slightly different definition of personal information, but the essentials are as described above. For the purposes of this Report, financial information about an identifiable individual is considered Personal Information under most definitions. Financial information about a corporate

entity or partnership is generally not considered to be personal information unless the relationship between that entity and the individuals who operate it is so closely intertwined that the information of that entity would be considered the personal information of those individuals. This is a determination that would have to be made on a case by case basis.

Information that is publicly available, such as that found in land registry records, court documents and records of administrative tribunals is generally excluded from the ambit of privacy legislation. Again, the precise definition of what constitutes publicly available information will vary from one legislative scheme to the other.

Fair Information Principles

While privacy legislation in Canada takes slightly differing approaches to regulating the collection, use, disclosure and retention/destruction of personal information, the underlying theme of these legislative provisions is generally based on what are known as the "Ten Privacy Principles of Fair Information Practices". These principles are:

1. Be accountable - An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
2. Identify the purpose - The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
3. Obtain consent - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. Limit collection - The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
5. Limit use, disclosure and retention - Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
6. Be accurate - Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
7. Use appropriate safeguards - Personal information must be protected by appropriate security relative to the sensitivity of the information.
8. Be open - An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
9. Give individuals access - Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and 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.

10. Provide Recourse - An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.[8]

The legislated privacy regimes reviewed for the purposes of this Report are based on these ten fair information practices. When it comes to the issue of information sharing, the most important and relevant aspects of these 10 principles or practices are related to the restrictions that privacy legislation places on the disclosure of personal information that may have been collected by both public and private sector organizations.

In each case, the legislative requirement is that personal information not be disclosed for any purpose other than that for which it was collected, with the exception of situations in which there is a legal requirement to do so or, in a limited number of legislated exceptions which, by and large, give an organization the discretionary ability to disclose the information in specific and limited circumstances. The typical/general legislated requirement to limit the disclosure or sharing of personal information may impede the sharing of personal information between various private and public entities that have a role in anti-money laundering regimes in Canada. On the other hand, some of the legislated exceptions may operate to allow some sharing of personal information between these entities.

Focus of this Report

This Report will examine the legislative regimes identified above and the restrictions and exceptions to those restrictions that may impact the sharing of personal information.

[8] Government of British Columbia, "Ten Principles of Privacy Collection" *gov.bc.ca*, online: < www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles#limit-collection>; See also the International Association of Privacy Professionals (IAPP), "Fair Information Practice Principles" *IAPP*, online: <iapp.org/resources/article/fair-information-practices/>; Office of the Privacy Commissioner, "PIPEDA fair information principles" (May 2019), *Office of the Privacy Commissioner of Canada*, online: <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/>; and Pam Dixon, "A Brief introduction to Fair Information Practices" (December 19 2007), *World Privacy Forum*, online: <www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>.

The review of the BC *Freedom of Information and Protection of Privacy Act* and the federal *Privacy Act* will examine the ability of government entities to share information with other government entities and with the private sector. The review of the BC *Personal Information Protection Act* and the *Personal Information Protection and Electronic Documents Act* will examine the ability of non-government entities to share information with other non-government entities and with government entities.

British Columbia

British Columbia has three statutes which govern privacy. Two govern the collection, use and disclosure of personal information, in the public sector and in the private sector, while the third provides an avenue for recourse if personal information is misused ie. if there has been an "invasion of privacy".

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165

Application

The BC Freedom of Information and Protection of Privacy Act (FIPPA) has as one of its purposes, "preventing the unauthorized collection, use or disclosure of personal information by public bodies" [subsection 2 (d)]. "Personal information" is defined as, "recorded information about an identifiable individual other than contact information".

A "public body" is defined as:

(a) a ministry of the government of British Columbia,
(b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2,[9] or
(c) a local public body

but does not include

(d) the office of a person who is a member or officer of the Legislative Assembly, or
(e) the Court of Appeal, Supreme Court or Provincial Court.

A "local public body is defined as:

(a) a local government body,
(b) a health care body,
(b.1) a social services body,
(c) an educational body, or

[9] See Appendix A for a list of entities listed in Schedule 2 that may have information, including personal information, that would be relevant to combating money laundering.

(d) a governing body of a profession or occupation, if the governing body is designated in, or added by regulation to, Schedule 3.[10]

A local government body is defined as, *inter alia*, a municipal police board established under section 23 of the *Police Act.*[11] A municipal police board must "establish a municipal police department and appoint a chief constable and other constables and employees the municipal police board considers necessary to provide policing and law enforcement in the municipality" [s.26(1)].

General

FIPPA is enforced by the Office of the Information and Privacy Commissioner of BC.[12] The role and duties of the Commissioner are set out in section 42 and include:

- Conducting investigations and audits to ensure compliance with any provision of this Act or the regulations,
- Receiving comments from the public about the administration of this Act
- Public education
- Commenting on the implications for access to information or for protection of privacy of proposed legislative schemes or programs or activities of public bodies,
- Commenting on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information,
- Commenting on the implications for protection of privacy of using or disclosing personal information for data linking,[13]
- Authorizing the collection of personal information from sources other than the individual the information is about

Complaints may include an allegation that personal information has been collected, used or disclosed in contravention of Part 3 by (i) a public body or an employee, officer or director of a public body, or (ii) an employee or associate of a service provider.[14]

---

[10] See Appendix B for a list of entities listed in Schedule 3 that may have information, including personal information, that would be relevant to combating money laundering.
[11] *Police Act*, RSBC 1996, c 367.
[12] Information about the Commissioner's Office and its roles and responsibilities can be found on its website: <https://www.oipc.bc.ca/>.
[13] A detailed discussion of the concept of data-linking is beyond the scope of this Report, however, Schedule 1 defines "data-linking" and "data-linking initiative" as essentially the combining of information from one database with that in another if the purpose of the combining is different from the purpose for which the information was initially collected.
[14] A "service provider" is defined in Schedule 1 as "a person retained under contract to perform services for a public body".

Part 3 deals generally with the Collection, Protection, Retention, Use and Disclosure of Personal Information by Public Bodies and Data-linking Initiatives, which are discussed below in the context of the restrictions that FIPPA places on the sharing of personal information by public bodies.

The Commissioner has extensive powers to investigate complaints regarding the collection, use or disclosure of personal information, including the power to require a public body or service provider to stop collecting, using or disclosing personal information in contravention of the Act, confirm a decision of a public body or service provider to collect, use or disclose personal information or require the head of a public body to destroy personal information collected in contravention of the Act.

A public body has a duty to comply with an order of the Commissioner and failure to comply can result in a certified copy of the order being filed with the superior court, at which time the order becomes enforceable as if it were an order of that Court.

Restrictions on the Sharing of Personal Information

Restrictions on the sharing of personal information are found in PART 3 of FIPPA and must be read in the context of restrictions on the collection, use and retention of personal information. Restrictions on the collection and retention of personal information are found in Division 1 of Part 3. These restrictions will impact the ability of public bodies that are subject to FIPPA to share and to receive personal information that may be relevant to combatting money laundering.

A public body may only collect personal information for specific purposes that are described in section 26 of the legislation. Obviously this restriction informs not only what information a public body may have in its possession for the purposes of sharing with a third party, but if the third party is also subject to FIPPA, its ability to collect information by way of information sharing from another body will be restricted.

26. A public body may collect personal information only if
(a) the collection of the information is expressly authorized under an Act,

(b) the information is collected for the purposes of law enforcement,

(c) the information relates directly to and is necessary for a program or activity of the public body,

(d) with respect to personal information collected for a prescribed purpose,
(i) the individual the information is about has consented in the prescribed manner to that collection, and
(ii) a reasonable person would consider that collection appropriate in the circumstances,

(e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

(f) the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur,

(g) the information is collected by observation at a presentation, ceremony, performance, sports meet or similar event
(i) at which the individual voluntarily appears, and
(ii) that is open to the public, or

(h) the information is personal identity information that is collected by
(i) a provincial identity information services provider and the collection of the information is necessary to enable the provincial identity information services provider to provide services under section 69.2, or
(ii)a public body from a provincial identity information services provider and the collection of the information is necessary to enable
(A) the public body to identify an individual for the purpose of providing a service to the individual, or
(B) the provincial identity information services provider to provide services under section 69.2.

In addition, there are restrictions in section 27 as to how personal information may be collected. Generally, it must be collected directly from the individual involved, unless one of a number of limited exceptions applies. Again, whether personal information can be collected, other than directly from the individual involved, will inform the ability of a public body to receive personal information from another public body or from another entity.

A public body must ensure that an individual from whom it collects personal information is told the purpose for collecting it, the legal authority for collecting it, and the title, business address

and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection. [subsection 26 (2)].

The British Columbia government has published a FIPPA Policies and Procedures Manual (FIPPA Manual) which provides helpful guidance on the collection, use and disclosure of personal information.[15]

The use and disclosure of personal information is governed by Division 2 of Part 3.

Generally speaking, personal information can only be used or disclosed by an entity if one of the criteria in Division 2 is met. The FIPPA manual also emphasises that, if a public body discloses personal information in accordance with one of the provisions in Division 2, it should disclose only the minimum personal information necessary.

Section 32 sets out the limited circumstances for the use of personal information:

32. A public body may only use personal information under its custody and control

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose, [16]

(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

If personal information was originally collected by a public body for the purpose of combatting money laundering, it may be used or disclosed for that purpose. However, if it was collected for some other purpose, as in most cases it will have been, it may only be disclosed by the public body within the confines of Division 2. For the purposes of this report, the following provisions of Division 2 may operate to allow the sharing of personal information by entities subject to FIPPA. Note that, with the exception of disclosure in response to a subpoena, warrant or court order, disclosure is not mandated, but it is permitted. The disclosure could be made in response to a request from another entity for the information or proactively by the public body. The

[15] Government of B.C., "FOIPPA Policy & Procedures Manual", *gov.bc.ca*, online: <www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual>.

[16] A consistent purpose is one that has a reasonable and direct connection to the original purpose and is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information [section 34].

disclosure provisions which are likely to be most relevant in the context of the sharing of information by public bodies for the purposes of combating money laundering are:

- For the purpose consistent with the purpose for which the information was collected, obtained or compiled – [s. 32 (a) & 33.2 (1) (a)];
- The disclosure reveals financial and other details of a contract to supply goods or services to a public body [s. 33 (1) (a1) referencing s.22 (4) (f)];
- In accordance with an enactment of British Columbia, other than FIPPA, or Canada that authorizes or requires disclosure – [s. 33.1 (1) (c)];
- In accordance with a provision of a treaty, arrangement or written agreement that
    - Authorizes or requires disclosure, and
    - Is made under an enactment of BC, other than FIPPA, or Canada – (s.33.1 (1) (d)];
- For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies or professions and occupations – [s. 33.1 (1) (l)];
- To comply with a subpoena, a warrant or an order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information – [s. 33.1 (1) (t)].

In addition, if the entity is a law enforcement agency[17] it may disclose personal information to

- Another law enforcement agency in Canada, or
- A law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority – [s. 33.1 (2) (a)].

The following disclosure(s) may only be made within Canada:

- To a public body or law enforcement agency in Canada to assist in a specific investigation
    - Undertaken with a view to a law enforcement proceeding, or
    - From which a law enforcement proceeding is likely to result [s. 33.2 (i)].

Disclosure Inside or Outside Canada

For the purpose consistent with the purpose for which the information was collected, obtained or compiled – [s. 32 (a) & 33.2 (1) (a)]

Section 34 defines a consistent purpose as "one that has a reasonable and direct connection to the original purpose and is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information" (emphasis added).

[17] FIPPA definition: "law enforcement" means (a) policing, including criminal intelligence operations, b) investigations that lead or could lead to a penalty or sanction being imposed, or c) proceedings that lead or could lead to a penalty or sanction being imposed (Schedule 1).

The definition has two parts, both of which must be met in order to be considered a consistent purpose. The FIPPA Manual describes the first part of the test; "[t]he consistent use must have a logical and plausible link to the original purpose. It must flow or be derived directly from the original use or be a logical outgrowth of the original use. There is no strict rule on what constitutes a consistent use. However, one guideline to consider is whether the person concerned would expect the personal information to be used in the proposed way."

The second part of the test refers to necessity. Again, the FIPPA Manual states that "[n]ecessary for performing the statutory duties' means the personal information is needed to perform duties or obligations required by legislation."

See *Coast Mountain Bus Co. v. C.O.P.E., Local 378,*[18] which adopts the above guideline. In that case a union wanted documents which had been compiled by the employer to be disclosed but the employer refused, citing the FIPPA as preventing them from doing so. The employer was ultimately directed to disclose the information because the disclosure was found to be permitted under s. 33.2(a), as the information which the union sought, (personal information contained in job applications, resumes and interview responses) and their use of the information for the purpose of assessing the employer's hiring decision, was consistent with the purpose for which the information was obtained, that is, seeking a suitable candidate for a job with the employer.

See also *Greater Vancouver (Regional District) v. G.V.R.D.E.U.:*[19]

> "In order to be consistent with that purpose it must have a "reasonable and direct connection". This has been described by the Information and Privacy Commissioner, who is charged with the administration of FIPPA, in a variety of ways: "logical and plausible link", "flow or be directly derived from" and "logical outgrowth".

In applying these criteria in this case, the Commissioner also appears to accept the concept of the "expectation" of the subject or provider of the information.

That case revolved around a workplace discharge where the causes relied on by the employer included allegations of fraud and otherwise inappropriate conduct in the making of a Workers' Compensation claim. The employer applied for an order pursuant to s. 95(1.1)(c) of the *Workers'*

[18] 2005 BCCA 604, at paras 58-60.
[19] [2006] BCCAAA No. 160, at paras 50-51.

Compensation Act , R.S.B.C. 1996, c. 492 which would permit it to use the Workers' Compensation Board's disclosure file for its case, which the Board allowed, leading to the settlement of the grievance. The disclosure was found to be permitted under s. 33.2(a) because the intended use of the information by the employer was, in the circumstances of the case, consistent with the purpose for which it was obtained. In particular, the employer's use, the discharge case, was a "logical outgrowth" of the original purpose of addressing the legitimacy of the WCB claim.

The disclosure reveals financial and other details of a contract to supply goods or services to a public body [s. 33 (1) (a1) referencing s.22 (4) (f)]

Assuming that information described in this paragraph and held by a public body that would assist in the combating of money laundering is discovered, disclosure may be permitted under this provision. An example of information falling within this provision can be found in *Ministry of Health (Re)*,[20] which refers to a schedule to a contract outlining the services a contractor will supply to the Ministry.

In accordance with an enactment of British Columbia, other than FIPPA, or Canada that authorizes or requires disclosure – (s. 33.1 (1) (c))

Specifically, this provision allows for disclosure of personal information to anybody where that disclosure is permitted by legislation. For instance, section 12 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[21] requires reporting to FINTRAC when certain monetary instruments are imported or exported. Assuming that a public body subject to FIPPA were to be required under this provision to make a report containing personal information, this provision would operate as a complementary provision allowing the report to be made.

An example of permissible disclosure under this provision can be found in *British Columbia (Finance) (Re)*[22] in which multiple people complained to the Office of the Information and Privacy Commissioner (OIPC) regarding the Ministry of Finance's authority to collect, use and disclose the name, address, SIN, date of birth and email address of property owners. The Ministry

[20] 2014 BCIPC 48.
[21] For a discussion of this legislation see below.
[22] 2019 BCIPC 41.

required the information to be provided in a declaration form under the *Speculation and Vacancy Tax Act* (SVTA).[23] Although the information at issue was clearly personal information under FIPPA, the Ministry was found to be authorized to collect the personal information under s. 26(c) of FIPPA as the information related directly to and was necessary for a program of the public body. It was also held that the Ministry was using the information at issue for the purpose for which it was obtained and was therefore authorized to use the personal information under s. 32(a). Regarding disclosure, the Commission found that the Ministry of Finance had entered into a memorandum of understanding with the Canada Revenue Agency under section 121 of the *Speculation and Vacancy Tax Act.*[24]Because the Ministry was authorized under s. 120 of that Act to disclose information to the CRA in accordance with that memorandum, this in turn authorized the Ministry under s. 33.1(1)(c) of FIPPA to disclose the information.

See also *British Columbia Hydro and Power Authority*, Re,[25] where it was acknowledged that Section 19.2 of the *Safety Standards Act*[26] provides authority for BC Hydro to disclose consumption information to municipalities who request residential electricity information within their jurisdictional boundaries. Section 33.1(1)(c) authorizes BC Hydro to make such a disclosure.

In accordance with a provision of a treaty, arrangement or written agreement [s. 33.1 (1) (d)]

The FIPPA manual makes it clear that the "treaty, arrangement or agreement" must specifically authorize or compel the disclosure of the personal information that is released under section 33.1(1)(d). The fact that a disclosure would assist in a program's operation is insufficient. It also states that if a "treaty, arrangement or agreement" is used to release personal information under section 33.1(d), the authority to enter into the "treaty, arrangement or agreement" must be clearly established in an enactment for this provision to apply.

[23] SBC 2018, c 46.
[24] SBC 2018, c 46.
[25] 2011 BCIPC 43.
[26] SBC 2003, c 39.

Only a "treaty, arrangement, or written agreement" made by the government of British Columbia or the government of Canada may authorize a disclosure under this provision. This provision does not authorize public bodies to disclose personal information under the legislation of other provinces or other countries.

An example of permissible disclosure under this provision can be found in *British Columbia (Finance) (Re)* referenced above. Because the Commissioner found that section 33.1 (1) (c) applies, it was unnecessary to consider section 33.1 (d), but that section would also have been applicable in light of the agreement between the two levels of government and the statutory authorization for the agreement.

For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies or professions and occupations – [s. 33.1 (1) (l)]

The FIPPA manual gives the purpose of this provision as follows:

> "The exchange of personal information between licensing bodies in different jurisdictions prevents a professional involved in criminal or unethical behaviour from moving to a new jurisdiction and repeating the same practice."

Accordingly, this provision might be available to disclose information about a professional who has been disciplined or had his or her licence revoked for activities relating to money laundering.

To comply with a subpoena, a warrant or an order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information [s. 33.1 (1) (t)]

While this provision is couched in the general terms of section 33.1 that permits the disclosure of personal information, clearly, in light of a valid subpoena, warrant or order, a public body would be required to produce the information requested unless it were to challenge the subpoena, warrant or order. See *Svangtun v Pacific National Exhibition*.[27]

Disclosure by a law enforcement agency [s. 33.1 (2) (a)]

[27] 2019 BCSC 121.

Disclosure by a law enforcement agency is permitted to another law enforcement agency in Canada, or, if there is an arrangement, written agreement, treaty or provincial or federal legislative authority, to another law enforcement agency in a foreign country. Note that the foreign law enforcement agency must meet the same definition under FIPPA that applies to a domestic law enforcement agency i.e. policing, including criminal intelligence operations, investigations that lead or could lead to a penalty or sanction being imposed, or proceedings that lead or could lead to a penalty or sanction being imposed.

The FIPPA manual reiterates that, "Public bodies that have some law enforcement responsibilities, but whose primary function is not law enforcement, are not law enforcement agencies for the purposes of section 33.1(2). They are, however, authorized under section 33.2(i) to disclose personal information within Canada to assist in a specific law enforcement investigation". This provision is discussed below.

The FIPPA manual goes on to identify examples of public bodies with law enforcement responsibilities that do not come within the definition of a "law enforcement agency" in section 33.1(2):

- Conservation branches, Ministry of Environment
- Office of the Fire Commissioner, Ministry of Public Safety and Solicitor General
- BC Financial Services Authority (BCFSA)
- Municipal bylaw enforcement officers
- Other regulatory bodies responsible for enforcing compliance with a law.

While this provision may seem quite broad, it is to be interpreted carefully. The FIPPA Manual notes that,

> "Public bodies have the discretion not to disclose personal information to other public bodies or law enforcement agencies if the request relates to an investigation that is not focused and where personal information is sought on suspicion, surmise or guesses."

On Ministerial Authority section 33.1 (3)

This section provides that:

> (3) The minister responsible for this Act may, by order, allow disclosure outside Canada under a provision of section 33.2 in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable. The FIPPA manual confirms that a summary of any order made under this section will be made public and that disclosures under this section are to be made on a case by case basis.

Disclosure Inside Canada Only

To a public body or law enforcement agency in Canada to assist in a specific investigation [s. 33.2 (i)]

This provision applies to disclosures within Canada only and relates to two circumstances in which personal information may be disclosed by a public body. The disclosure must be to another public body or a law enforcement agency in Canada. The disclosure must be for the purposes of assisting in a specific investigation that is being undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result. The public body to which disclosure is made must be an entity that meets the definition in FIPPA. The law enforcement agency need not be located in British Columbia, but it must meet the definition of a law enforcement agency as it appears in FIPPA.

The terms used in this section are not defined in the statute, but the FIPPA manual provides the following definitions:

> "investigation" – A methodical process of examination, inquiry and observation including examining a crime scene, interviewing witnesses and reviewing documents.
> "proceeding" - The form and manner of conducting juridical business [business having to do with the administration of justice] before a court or judicial officer. Thus a "law enforcement proceeding" is a juridical process undertaken for law enforcement reasons with a view to imposing penalties or sanctions (as opposed to simply gathering information for intelligence purposes).
>
> "*likely to result*" - For a public body to disclose personal information under this paragraph there must be a reasonable probability that a law enforcement proceeding will result.
>
> "*with a view to*" - The purpose of the investigation must be to institute law enforcement proceedings, even if, for lack of evidence, such proceedings do not actually take place.

As with disclosure under s. 33.1 (2) (a), disclosure is discretionary. The public body is in the best position to determine if disclosure is appropriate in any given circumstance. This principle is evidenced by *Inquiry Re: A request by the British Columbia College of Teachers*, in which the College requested a statement by a former student from the Vancouver Police Department, but the police refused, citing section 3(1)(h) of FIPPA, since the statement related to a prosecution that was still before the courts. The College disagreed and requested a review of the decision by the Information and Privacy Commissioner. Although the Commissioner commented that "it does not make sense in these circumstances, for one law enforcement agency to refuse to

cooperate with another public agency engaging in a law enforcement activity," he regretted that he had no choice but to conclude that it was the responsibility of the public body, in this case the Vancouver Police Department, to decide whether disclosure was appropriate under section 33 of the Act.[28]

Public Interest Override

In addition to the specific provisions permitting disclosure without the consent of the individual involved, information, including personal information, must be disclosed if it would be in the public interest to do so. Section 25 of FIPPA provides as follows:

> 25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information
>
> (a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
>
> (b) the disclosure of which is, for any other reason, clearly in the public interest.
>
> (2) Subsection (1) applies despite any other provision of this Act.
>
> (3) Before disclosing information under subsection (1), the head of a public body must, if practicable, notify
>
> (a) any third party to whom the information relates, and
>
> (b) the commissioner.
>
> (4) If it is not practicable to comply with subsection (3), the head of the public body must mail a notice of disclosure in the prescribed form
>
> (a) to the last known address of the third party, and
>
> (b) to the commissioner.

Section 25 applies to all information, including personal information. Note that, while the section is mandatory, it is within the discretion of the head of the public body to make the initial determination if a disclosure is required by this section, even if that information is subject to an exception to disclosure within Part 2 or would be restricted from disclosure under Part 3. As the FIPPA Manual states, this is a significant override of the otherwise restrictive provisions in the legislation and, "[t]he broad override that section 25 provides necessitates a high threshold for

[28] Inquiry Re: A request by the British Columbia College of Teachers for a statement in the custody or under the control of the Vancouver Police Department, Order No. 256-1998 August 13, 1998.

disclosure. The use of this section should require sufficient gravity in that it overrides all other provisions of the Act, and therefore its use should be considered exceptional."

It may be that this provision could come into play if a public body has significant information in its possession that relates to money laundering activities, the disclosure of which could meet the "clearly in the public interest" test. Note however, that both the party to whom the information relates and the Commissioner would have to be notified of the disclosure beforehand, if at all possible. This requirement may mean that disclosure pursuant to this provision, even if it could be justified, would not be practical.

Disincentive to disclosures under Division 2 of Part 3

While section 73 of FIPPA protects public bodies, the head of a public body and the employees of a public body from civil liability if they disclose personal information in good faith, there are a number of provisions in the legislation that act as disincentives to disclose personal information, even if it would be permitted by the legislation.

If a public body discloses personal information in a manner not permitted by the legislation, the Commissioner has the power under section 58 (3) (e) and (f) to,

> (e) require a public body or service provider to stop collecting, using or disclosing personal information in contravention of this Act, or confirm a decision of a public body or service provider to collect, use or disclose personal information;
> (f) require the head of a public body to destroy personal information collected in contravention of this Act.

In light of these provisions, there is unlikely to be any incentive to "push the envelope" in interpreting the sections allowing for discretionary disclosure of personal information when there is the possibility of an adverse finding and order from the Commissioner.

In addition, there is the potential for criminal liability if personal information is disclosed contrary to the provisions of the legislation.

> **Unauthorized disclosure prohibited**
> 30.4 An employee, officer or director of a public body or an employee or associate of a service provider who has access, whether authorized or unauthorized, to personal

information in the custody or control of a public body, must not disclose that information except as authorized under this Act.

And, section 74.1 provides, *inter alia*:

> **Privacy protection offences**
> 74.1 (1) A person who contravenes section 30.4 (unauthorized disclosure) or 30.5 (notification of unauthorized disclosure) commits an offence.
>
> - - - - -
> (3) If an employee or associate of a service provider
> (d) contravenes section 30.4 (unauthorized disclosure), or
> (e) Contravenes section 30.5 (notification of unauthorized disclosure),
>
> in relation to personal information that is held because of the service provider's status as a service provider, the service provider commits an offence.
>
> (4) If a corporation commits an offence under this section, an officer, director or agent of the corporation who authorizes, permits or acquiesces in the commission of the offence also commits an offence, whether or not the corporation is prosecuted for the offence.
>
> (5) A person who commits an offence under this section is liable
> (a) in the case of an individual, other than an individual who is a service provider, to a fine of up to $2 000,
> (b) in the case of a partnership that is or individual who is a service provider, to a fine of up to $25 000, and
> (c) in the case of a corporation, to a fine of up to $500 000.

While subsection (8) provides that, "In a prosecution for an offence under this section, it is a defence for the person charged to prove that the person exercised due diligence to avoid the commission of the offence" these offence provisions would also operate as a disincentive to disclose personal information unless it is clear that the disclosure will abide by the provisions permitting disclosure.

Damages are not available under FIPPA, but may be available, under some circumstances, by way of the BC *Privacy Act*.[29]

[29] For a discussion on this issue, see: Naomi J Kruege, *Public Sector Privacy Breaches: Should British Columbians have a Cause of Action for Damages Under the Freedom of Information and protection of Privacy Act?* (2018) 23 Appeal 149.

Personal Information Protection Act, SBC 2003, c 63

Application

The purpose of the BC *Personal Information Protection Act* (PIPA) is set out in section 2:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect 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.

Personal information is defined as, "information about an identifiable individual and includes employee personal information but does not include, (a) contact information, or (b) work product information". Note that, unlike FIPPA, the personal information does not have to be recorded in order to qualify for protection under PIPA.

An "organization is defined as:

> "organization" includes a person, an unincorporated association, a trade union, a trust or a not for profit organization, but does not include
> (a) an individual acting in a personal or domestic capacity or acting as an employee,
> (b) a public body,
> (c) the Provincial Court, the Supreme Court or the Court of Appeal,
> (d) the Nisga'a Government, as defined in the Nisga'a Final Agreement, or
> (e) a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settlor

Section 3 sets out a number of categories of personal information that are not subject to the legislation. This includes personal information to which another act applies, personal information collected, used or disclosed for purely domestic or journalistic, literary or artistic purposes and some court documents.

Generally, PIPA follows the fair information principles set out above. Part 2, specifically sections 4 and 5 set out General Rules Respecting Protection of Personal Information by Organizations.

> ***Compliance with Act***
> 4 (1) In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.

(2) An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.

(3) An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the duty conferred by that designation.

(5) An organization must make available to the public
(a) the position name or title of each individual designated under subsection (3) or delegated under subsection (4), and
(b) contact information for each individual referred to in paragraph (a).

Policies and practices
5 An organization must
(a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
(b) develop a process to respond to complaints that may arise respecting the application of this Act, and
(c) make information available on request about
(i) the policies and practices referred to in paragraph (a), and
(ii) the complaint process referred to in paragraph (b).

Consent is a lynchpin of the legislation and organizations must have consent from an individual for the collection, use or disclosure of personal information [s. 6]. The rules surrounding the disclosure of personal information without consent are set out in Part 6.

The BC Information and Privacy Commissioner has general authority with respect to the enforcement of the legislation. The general powers of that office are set out in section 36 and include:

- The power to initiate investigations and audits to ensure compliance with any provision of this Act, if the commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with the Act;
- The power to make an order described in section 52 (3), whether or not a review is requested, which includes the power to:
  (a) confirm that a duty imposed under the Act has been performed or require that a duty imposed under the Act be performed;
  (b) confirm or reduce the extension of a time limit under section 31;
  (c) confirm, excuse or reduce a fee, or order a refund, in the appropriate circumstances;
  (d) confirm a decision not to correct personal information or specify how personal information is to be corrected;

(e) require an organization to stop collecting, using or disclosing personal information in contravention of the Act, or confirm a decision of an organization to collect, use or disclose personal information;
(f) require an organization to destroy personal information collected in contravention of the Act.

- The power to comment on the implications for protection of personal information of programs proposed by organizations, of automated systems for the protection of personal information; and of the use or disclosure of personal information held by organizations for document linkage;
- The power to authorize the collection of personal information by an organization from sources other than the individual to whom the personal information relates;
- The power to bring to the attention of an organization any failure of the organization to meet the obligations established by this Act;
- The power to exchange information with any person who, under legislation of another province or of Canada, has powers and duties similar to those of the commissioner;
- The power to enter into information-sharing agreements for the purposes of paragraph (k) and into other agreements with the persons referred to in that paragraph for the purpose of coordinating their activities and providing for mechanisms for handling complaints.

Orders made by the Commissioner under s. 52 (3) are binding on the organization against which they are made. As discussed below, it is an offence under s. 56 (1) (f) to fail to comply with an order made by the Commissioner.

Jurisdiction

For constitutional reasons, the PIPA can only apply to the collection, use and disclosure by organizations located in BC of personal information of any individual inside or outside of BC or to organizations located outside of BC which collect, use, or disclose the personal information of individuals in BC. There is somewhat of an overlap with the federal *Personal Information and Protection of Privacy Act*, which is discussed below. The Federal Privacy Commissioner has published a document entitled "Questions and Answers Regarding the application of PIPEDA, Alberta and British Columbia's *Personal Information Protection Acts*".[30] This document provides some useful guidance to help organizations decide if they are subject to provincial legislation or to the federal legislation.

[30] Office of the Privacy Commissioner of Canada, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts," (November 2004) *Office of the Privacy Commissioner of Canada*, online: www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/ [OPCC].

Organizations that are not considered to be Federal Works or Undertakings[31] within the meaning of the *Personal Information Protection and Electronic Documents Act*, but which engage in commercial activities that involve inter-provincial or international personal information flows, would have to comply with the federal legislation for those transactions. The Federal Privacy Commissioner gives the example of an import and export business or credit bureau which would have to comply with the *Personal Information Protection and Electronic Documents Act* regarding cross-border personal information collection, use or disclosure. Organizations that operate wholly with the province of BC would have to comply with PIPA.

Restrictions on the Sharing of Personal Information

As with FIPPA, disclosure is closely tied to collection and use and a receiving organization must be able to demonstrate that it is entitled, under whichever legislative regime applies to it, to receive the personal information. According to the BC Information and Privacy Commissioner,

> Disclosing personal information means showing, sending or giving some other organization, government or individual the personal information in question. To continue the example above, providing the customer's name and address when lawfully requested by the Canada Revenue Agency would be a valid disclosure of personal information.[32]

The circumstances under which disclosure of personal information is permitted are dealt with in Part 6. Section 17 provides that any disclosure must, be "only for purposes that a reasonable person would consider are appropriate in the circumstances and that

- fulfill the purposes that the organization discloses under section 10 (1),
- for information collected before this Act comes into force, fulfill the purposes for which it was collected, or
- are otherwise permitted under this Act.

Section 18 sets out the circumstances in which personal information may be disclosed without the consent of the person to whom the information relates. Note that, with the exception of

[31] The application of PIPEDA is discussed more fully below, but general speaking, Federal Works and Undertakings would include, Banks, Radio and television stations, Inter-provincial trucking companies, Airports and airlines, navigation and shipping by water, Telecommunication companies such as internet service providers, phone (cellular or land line companies), cable companies and Railways, canals, pipelines, ferries, etc. that cross borders.

[32]Office of the Information and Privacy Commissioner, *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations* (Vancouver: OIPC, 2015) [OIPC] at page 22.

disclosure in response to a subpoena, warrant or court order, disclosure is not mandated, but is permitted. The disclosure could be made in response to a request from another entity for the information or proactively by the organization. The following provisions are most likely to be relevant to the disclosure, without consent, of personal information for the purposes of combatting money laundering:

- it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding [s. 18 (1) (c)]
- the personal information is disclosed in accordance with a provision of a treaty that
    - authorizes or requires its disclosure, and
    - is made under an enactment of British Columbia or Canada [s. 18 (1) (h)]
- the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information [s. 18 (1) (i)]
- the disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation,
    - to determine whether the offence has taken place, or
    - to prepare for the laying of a charge or the prosecution of the offence [s. 18 (1) (j)]
- the disclosure is required or authorized by law [s. 18 (1) (o)]

It is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding [s. 18 (1) (c)]

The term “investigation” is defined in PIPA:

> "investigation" means an investigation related to
>
> (a) a breach of an agreement,
>
> (b) a contravention of an enactment of Canada or a province,
>
> (c) a circumstance or conduct that may result in a remedy or relief being available under an enactment, under the common law or in equity,
>
> (d) the prevention of fraud, or
>
> (e) trading in a security as defined in section 1 of the *Securities Act* if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying out investigations of trading in securities,
>
> if it is reasonable to believe that the breach, contravention, circumstance, conduct, fraud or improper trading practice in question may occur or may have occurred;

“An overarching requirement throughout this provision is that, in order for an investigation to be reasonable and therefore constitute an investigation for the purpose

> of PIPA, a cause to investigate in the circumstances of the particular case must first exist. An organization must have a reasonable belief that the individual who is the subject of the investigation contravened a law, or that he or she may do so."[33]

The term "proceeding" is defined as:

> "proceeding" means a civil, a criminal or an administrative proceeding that is related to the allegation of
>
> (a) a breach of an agreement,
>
> (b) a contravention of an enactment of Canada or a province, or
>
> (c) a wrong or a breach of a duty for which a remedy is claimed under an enactment, under the common law or in equity

In the labour context, a Union's investigation of a potential violation of a breach of s. 68 of the *Labour Relations Code*[34] has been found to be an investigation. Use of a private investigator to film inside a store and behind a picket line was reasonable and subsequent disclosure of that information in arbitration proceedings was in compliance with paragraph (c).[35]

The personal information is disclosed in accordance with a provision of a treaty that, authorizes or requires its disclosure, and is made under an enactment of British Columbia or Canada [s. 18 (1) (h)]

As with section 33.1 (1) (d) of FIPPA, this section only refers to treaties made under an enactment of British Columbia or Canada. It does not permit disclosure if the treaty was made under an enactment of another province. An Extradition Treaty would be an example of the sort of treaty contemplated by this section.

The disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information [s. 18 (1) (i)]

While this provision is couched in the general terms of section 33.1 that permits the disclosure of personal information, in light of a valid subpoena, warrant or order, a public body would be required to produce the information requested unless it were to challenge the subpoena, warrant or order.

---

[33] *Surrey Creep Catcher (Re)*, 2017 BCIPC 38.
[34] RSBC 1996, c 244.
[35] *Ikea Canada Limited Partnership v Teamsters Local Union No 213*, 2013 CanLII 42658 (BC LRB).

The disclosure is to a public body or a law enforcement agency in Canada, concerning an offence under the laws of Canada or a province, to assist in an investigation, or in the making of a decision to undertake an investigation, to determine whether the offence has taken place, or to prepare for the laying of a charge or the prosecution of the offence [s. 18 (j)]

The term "law enforcement agency" is not defined in PIPA, but the term "public body" is and refers back to the definition of public body in FIPPA. The term "prosecution" as used in paragraph (j) means the state pursuing legal action for a criminal or quasi-criminal offence.[36] See the discussion under paragraph (c) regarding the definition of an "investigation". An investigation by the police would fall within the ambit of paragraph (j) as would an investigation by Workplace BC of a workplace accident.[37] The difference between an investigation as contemplated by paragraph (c) and that contemplated by paragraph (j) is that the state need not be involved in a paragraph (c) investigation. An investigation by an insurer into a potential fraudulent insurance claim would fall within the ambit of paragraph (c).[38]

The disclosure is required or authorized by law [s. 18 (o)]

PIPA does not define the term "law." However, the *Interpretation Act*[39] defines an "enactment" as including a "regulation". "Regulation" is defined as including a "rule…enacted…in execution of a power conferred under an Act." For a discussion on this point see *Mary- Helen Wright Law Corporation (Pacific Law Group) (Re)*[40] where the Commissioner found that the British Columbia Human Rights Tribunal Rules of Practice and Procedure requiring the production of information constituted a "law" for the purposes of this section.

Another example of a law requiring and authorizing disclosure would be section 36 of the *Strata Property Act*[41] which obliges a strata corporation to make documents specified in section 35 available for inspection by an owner, tenant or person authorized by the owner to inspect the documents.[42]The law need not be a law of the Province of British Columbia. It could be a law

[36] *Mary- Helen Wright Law Corporation (Pacific Law Group) (Re)*, 2020 BCIPC 21 (CanLII).
[37] OIPC, *supra* note 32 at 23.
[38] *Ibid* at 18.
[39] RSBC 1996, c 238.
[40] 2020 BCIPC 21 (CanLII).
[41] SBC 1998, c 43.
[42] *Mason v. The Owners, Strata Plan* BCS 4338, 2017 BCCRT 47 (CanLII).

of another province or a law of Canada, such as the reporting requirements mandated by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[43]

Disincentive to disclosures

As noted above, it is an offence under s. 56 for a person or organization to, *inter alia* fail to comply with an order made by the Commissioner [para (f)]. Therefore, if the Commissioner makes an order against an organization under s. 52 (3) (e) to stop disclosing personal information in a manner that contravenes PIPA, and the organization fails to comply with that order, it could be prosecuted for an offence. A successful prosecution could lead to a fine of up to $100,000.00. More importantly, section 57 provides as follows:

> ***Damages for breach of Act***
> 57 (1) If the commissioner has made an order under this Act against an organization and the order has become final as a result of there being no further right of appeal, an individual affected by the order has a cause of action against the organization for damages for actual harm that the individual has suffered as a result of the breach by the organization of obligations under this Act.
>
> (2) If an organization has been convicted of an offence under this Act and the conviction has become final as a result of there being no further right of appeal, a person affected by the conduct that gave rise to the offence has a cause of action against the organization convicted of the offence for damages for actual harm that the person has suffered as a result of the conduct.

Because, with the exception of a subpoena or court order, or other legal compulsion, an organization is not obliged to disclose personal information, there is little incentive for an organization to do so and potentially face the risk of an adverse finding by the Commissioner and a subsequent action for damages if actual harm can be demonstrated. It is to be expected that organizations will err on the side of caution and not disclose personal information unless they are required to do so.

On the other hand, this section requires the demonstration of actual harm before damages can be awarded. That may be difficult to do in many cases. Also note that the right to seek recourse is

[43] SC 2000, c 17.

dependent on there being an order against the organization by the Commissioner or a conviction.[44]

Privacy Act, RSBC 1996, c 373

Introduction

The BC *Privacy Act* creates a statutory tort of breach of privacy, which allows an individual to sue for breach of privacy [s.1 (1)]. By way of this legislation, the legislature created a cause of action for which no common law tort existed anywhere in Canada until 2012, which is when the Ontario Court of Appeal decided *Jones v. Tsige*.[45] In that decision, the Court recognized the tort of "intrusion upon seclusion". The key elements of the tort are:

- the defendant's conduct must be intentional, which would include recklessness;
- the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and
- a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.[46]

In order to be compensated for damages, the plaintiff need not provide proof of harm to a recognized economic interest. However, where there is no tangible economic loss, damages will be modest and the court is to take the following factors into account in assessing quantum:

> (a) the nature, incidence and occasion of the act, conduct or publication constituting the violation of privacy of that person;
> (b) the effect of the violation of privacy on the health, welfare, social, business or financial position of that person or his family;
> (c) any relationship, whether domestic or otherwise, between the parties to the action;
> (d) any distress, annoyance or embarrassment suffered by that person or his family arising from the violation of privacy; and
> (e) the conduct of that person and the defendant, both before and after the commission of the violation of privacy, including any apology or offer of amends made by the defendant.[47]

---

[44] For cases discussing the limitations of this section see *Zellstoff Celgar Limited Partnership v Public and Private Workers of Canada, Local 1*, 2019 CanLII 104310 (BC LA); *McIvor v. MLK Pharmacies Ltd.*, 2016 BCSC 2249 (CanLII) and *Facilities Subsector Bargaining Association v. British Columbia Nurses' Union*, 2009 BCSC 1562 (CanLII).
[45] *Jones v Tsige*, OCA [2012] OJ No. 148, 2012 ONCA 32.
[46] *Ibid* at para 71.
[47] *Ibid* at para 81.

The British Columbia Supreme Court has repeatedly declined to adopt *Jones*, recently and most notably in *Demcak v. Vo*.[48] As such no common law action for breach of privacy exists in B.C., leaving the *Privacy Act* as the sole vehicle for a cause of action for invasion of privacy.

The *Privacy Act* has two main effects. First, it may act as a disincentive for an organization or an individual to take a liberal approach to other privacy legislation and disclose personal information they are not required to. As discussed above, most privacy legislation permits disclosure, but rarely requires it. With the possibility of liability for the wrongful disclosure of personal information that the *Privacy Act* creates, it is unlikely that anyone will be unnecessarily forthcoming with personal information.

That said, the second effect may mitigate the first. The Act contains an exceptions section, which details a number of situations where no cause of action exists. In so doing the legislation appears to be attempting to balance protecting individual privacy with protecting those who act in good faith.

Legislation

The BC Privacy Act is a short document containing just 5 sections, only the first 2 of which are potentially relevant to money laundering. They are:

> **Violation of privacy actionable**
> 1 (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.
>
> (2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.
>
> (3) In determining whether the act or conduct of a person is a violation of another's privacy, regard must be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.
>
> (4)Without limiting subsections (1) to (3), privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass.
>
> **Exceptions**
> 2 (1) In this section:

[48] *Demcak v Vo*, 2013 BCSC 899.

"court" includes a person authorized by law to administer an oath for taking evidence when acting for the purpose for which the person is authorized to take evidence;
"crime" includes an offence against a law of British Columbia.

(2) An act or conduct is not a violation of privacy if any of the following applies:
(a) it is consented to by some person entitled to consent;
(b) the act or conduct was incidental to the exercise of a lawful right of defence of person or property;
(c) the act or conduct was authorized or required under a law in force in British Columbia, by a court or by any process of a court;
(d) the act or conduct was that of
(i) a peace officer acting in the course of his or her duty to prevent, discover or investigate crime or to discover or apprehend the perpetrators of a crime, or
(ii) a public officer engaged in an investigation in the course of his or her duty under a law in force in British Columbia,
and was neither disproportionate to the gravity of the crime or matter subject to investigation nor committed in the course of a trespass.

(3) A publication of a matter is not a violation of privacy if
(a) the matter published was of public interest or was fair comment on a matter of public interest, or
(b) the publication was privileged in accordance with the rules of law relating to defamation.

(4) Subsection (3) does not extend to any other act or conduct by which the matter published was obtained if that other act or conduct was itself a violation of privacy."

Application

What is a violation of privacy?

As Justice Sharpe noted in *Jones v. Tsige*, despite four common law provinces having a statutorily created tort of invasion of privacy, (British Columbia, *Privacy Act*, R.S.B.C. 1996 c. 373; Manitoba, *Privacy Act*, R.S.M. 1987 c.P125; Saskatchewan, *Privacy Act*, R.S.S. 1978, c. P-24; and Newfoundland, *Privacy Act*, R.S.N. 1990, c.P-22) no provincial legislation provides a precise definition of what constitutes an invasion of privacy.[49] The courts in provinces with a statutory tort are thus left with more or less the same task as courts in provinces without such statutes, that is, to define the contours of the right to privacy.

[49] The Manitoba and Saskatchewan Acts provide some guidance by listing a non-exhaustive list of activities that may be a violation of privacy in s. 3. The Newfoundland and Labrador Act has a similar list in s. 4.

Although what amounts to invasion of privacy will undoubtedly vary significantly with the circumstances, all four provincial *Privacy Acts* are similar. They establish a limited right of action, whereby liability will only be found if the defendant acts wilfully (not a requirement in Manitoba) and without a claim of right. Moreover, the nature and degree of the plaintiff's privacy entitlement is circumscribed by what is "reasonable in the circumstances".[50]

The British Columbia courts have not provided a strict test of the elements of an invasion of privacy in any case law. Instead, they have been applying the same elements that are found in the common law doctrine: (1) the defendant's conduct must be intentional, which includes reckless; (2) the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and (3) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. Note that proof of harm to a recognized economic interest is not an element of the cause of action.[51]

The lack of a precise definition for the breach of privacy in BC notwithstanding, the case law provides a working understanding of the term. The first case to be heard under the Act, *Davis v. McArthur*, at both the trial and appeal level, interpreted "privacy" to be equivalent to U.S. judicial definitions of the word as meaning a "right to be let alone, and to be "free from unwarranted publicity" and "a right to withhold oneself from public scrutiny if one chooses."[52] With this understanding of what privacy is, the cases hold that two questions must be answered in every case in which a violation of privacy under the Act is alleged:[53]

1. Was the plaintiff entitled to privacy?
2. If so, did the defendant violate the plaintiff's privacy?

Entitlement to privacy is not automatic. As per section 1(2), it exists only if a reasonable person would have an expectation of privacy under the circumstances of the case in light of the lawful interests of others, and only to the extent of that expectation.

---

[50] *Jones v Tsige*, *supra* note 45 at paras 52-54.
[51] Memorandum of Law from Taran Virtual Associates (1 May 2019), *What are the elements of the tort of invasion or breach of privacy in British Columbia?*, CARS2MEMO-BCM 10646.
[52] 10 DLR (3d) 250 at 254 (BCSC); 17 DLR (3d) 760 at 763 (BCCA).
[53] *Getejanc v. Brentwood College*, (2001), 6 CCLT (3d) 261 at para 16; *Milner v. Manufacturers Life Insurance Company*, [2005] ILR I-4479 [*Getejanc*] at para 74.

If a reasonable expectation of privacy did exist, the court must then consider whether the conduct in question violated that right to privacy, with consideration for the criteria mentioned in section 1(3), being the nature, incidence, and occasion on which the conduct occurred, and any relationship between the parties.[54]

Examples

With these considerations in mind, a list of decisions is illustrative. British Columbia courts have held the following to be violations of privacy:

- Publishing details of a sexual assault in violation of a publication ban. The jury awarded $18, 000 in damages for the breach[55]
- A landlord videotaping an undressed female tenant; compensatory damages of $15,000 and punitive damages of $35,000[56]
- Releasing the plaintiff's financial information to third parties while also suggesting that the plaintiff was acting fraudulently; no award aside from party costs[57]
- A teacher invading the plaintiff's home in their absence while looking for another missing student; $2,500 assessed in damages[58]
- Asking personal questions at the plaintiff's workplace about the plaintiff's income, character and drinking habits without any lawful interest in seeking the information; $1, 000 awarded[59]
- Intercepting, recording and disclosing a neighbour's mobile phone conversations in violation of section 9 of the Radio Communications Act[60] and sections 184.5(1) and 193.1(1) of the Criminal Code; the plaintiff was awarded general damages of $30,000, out of pocket expenses of $1,000, and punitive damages of $5,000.[61]

Additionally, it is worth noting that corporations may have the right to sue for invasion or breach of privacy under the *Privacy Act*.[62]

---

[54] British Columbia Law Institute, "Report on The Privacy Act of British Columbia", Legislation Report on *The Privacy Act* [RSBC 1996] c 373, BCLI report no. 49, February 2008.
[55] *F.(J.M.) v. Chappell* (1998), 45 BCLR (3d) 64 (CA).
[56] *Malcolm v. Fleming*, [2000] BCJ No. 2400 (SC).
[57] *B.M.P. Global Distribution Inc. v. Bank of Nova Scotia* (2005), 8 BLR (4th) 247 (SC).
[58] *Getejanc*, *supra* note 53.
[59] *I.C.B.C. v. Somosh (*1983), 51 BCLR 344 (SC).
[60] R.S.C. 1985, c. R-2.
[61] *Watts v. Klaemt* (2007), 71 BCLR (4th) 362 (SC).
[62] *Madco Investments Ltd. v. Western Tank & Lining Ltd.*, 2017 BCSC 219 (B.C. S.C.), where, on a motion to strike a counterclaim, the judge noted the following at para 69: "The claims for breach of privacy are grounded, at least in part, in the Privacy Act, RSBC 1996, c 373 ("Privacy Act"). Section 1(1) of the Privacy Act provides that "it is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another". The word "person" is not defined in the *Act*. However, according to s. 29 of British Columbia's Interpretation Act, RSBC 1996, c 238, when an enactment uses the word "person" without express

The following have been held not to be violations of privacy:

- a plaintiff's wife using a private investigator to follow the plaintiff's car and plant a tracking device on it because she suspected the plaintiff of adultery[63]
- filming an altercation involving the plaintiff on the plaintiff's parking lot[64]
- showing a third party a partially nude photo of the plaintiff which the plaintiff had carelessly left in the defendant's possession.[65][66]

Exceptions

Section 2 (2) (c) may have the greatest impact in relation to money laundering. It has been interpreted to mean that "an act or conduct is not a violation of privacy if the act or conduct was authorized or required under a law in force in British Columbia, by a court or by any process of a court. The effect of this provision is to exclude from the operation of the Privacy Act any act taken in a judicial proceeding that was authorized by a law in force in British Columbia or any process of a court."[67] For example, in *British Columbia (Public Service Employee Relations Commission) v. B.C.G.E.U* it was held that a wiretap did not violate the Privacy Act since it was authorized by the *Criminal Code*.[68]

Section 2 (2) (d) is also of obvious potential connection to the investigation of money laundering. The plain language of the text excepts actions of breach of privacy against officers who are acting lawfully in the course of their duty. *Bracken v. Vancouver Police Board* illustrates how officers acting in accordance with the Police Act will be exempt from lawsuit under this section.

Interaction with other Legislation

As noted above, the British Columbia courts have repeatedly denied a common law cause of action for violation of privacy because the province's legislative privacy protection scheme

---

qualification, it includes a "corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law": see also *St. Pierre v. Pacific newspaper Group Inc*., 2006 BCSC 241, at para 41."

[63] *Davis v. Mcarthur, supra*, note 52.

[64] *Silber v. BCTV* (1986), 69 BCLR 34 (SC).

[65] *Milton v. Savinkoff* [1993] BCJ No. 2396 (SC).

[66] List found at British Columbia Law Institute, *supra* note 54.

[67] *Duncan v. Lessing*, 2018 CarswellBC 16, 2018 BCCA 9 at paras 63-64. See also *Turkson v. TD Direct* 2016 BCSC 732 for example of 2(c)(c) allowing evidence to be admitted that would otherwise violate section 1.

[68] *British Columbia (Public Service Employee Relations Commission) v. B.C.G.E.U.*, 63 CLAS, 3 LAC (4th) 325. The case also demonstrates that the officers were acting according to FOIPPA, and thus would also be immune under section 2(2)(c).

supersedes any common law rights. But there are other important interactions between the Privacy Act and other legislation that are worth discussing.

First, how do FIPPA and the *Privacy Act* interact? This is not clear, but see the discussions noted above.

Second, how does PIPA interact with the *Privacy Act*? Since there is already a remedy under section 57 of PIPA, can a claimant also seek a remedy under the Privacy Act? As per *Facilities Subsector Bargaining Assn. v. B.C.N.U.*[69] the answer appears to be no, at least not until the Privacy Commissioner has made an order under s. 57. In that case defendants brought a motion to strike claims for a breach of privacy rights. The Court granted the motion, finding that BC's PIPA legislation provided an exclusive scheme for investigating and remedying privacy violations. Because the legislature had considered and provided a process for seeking damages under the *Act*, an individual should only be allowed to advance a claim for damages after the Commissioner has made an order, in accordance with s. 57 of *PIPA*.[70]

Regarding the overlap of PIPA and PIPEDA, British Columbia's PIPA applies in the same way to all organizations that are subject to it, but when British Columbia organizations subject to PIPA engage in commercial trans-border personal information flows, they also have to follow PIPEDA for those specific transactions.[71] While it is not clear, one may assume that a breach of PIPEDA would have to be dealt with under that statute and that, following the reasoning in *Facilities Subsector Bargaining Assn. v. B.C.N.U.*, it is likely that remedies would have to be sought under PIPEDA.

Conclusion

In sum, the BC *Privacy Act* makes a breach of privacy actionable, and may deter the sharing of personal information. Nevertheless, a lawful investigation or any act that was authorized or required under a law in force in British Columbia, by a court or by any process of a court, is not in violation of the act. As such, the Privacy Act serves as a disincentive to the sharing of information, but not a total ban. Similar to the conclusion reached above in the PIPA discussion,

[69] *Facilities Subsector Bargaining Assn. v. B.C.N.U.*, 2009 BCSC 1562.
[70] *Ibid* at para 78.
[71] OPCC *supra* note 30.

this Act may act as an impediment to the investigation of money laundering, as organizations are may be less than willing to expose themselves to a potential lawsuit for breach of privacy by disclosing personal information if there is no obligation to do so.

Federal

Privacy Act, RSC 1985, c P-21

Application

Unlike British Columbia, which combines both public sector access to information legislation and privacy legislation in one statute (FIPPA), at the federal level there are separate statutes for access (the *Access to Information Act*[72]) and for privacy (the *Privacy Act*).

The purpose of the federal *Privacy Act* is "to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information." [s.2]

A Government institution means;

- any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and
- any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*;

Essentially all federal government departments and agencies are subject to the federal *Privacy Act*.

The definition of personal information for the purposes of this legislation is quite detailed:

> *personal information* means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

[72] RSC 1985, c A-1.

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26[73] and section 19[74] of the *Access to Information Act*, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,

(ii) the title, business address and telephone number of the individual,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(v) the personal opinions or views of the individual given in the course of employment,

[73] Section 7 refers to the use to which personal information may be put, section 8 deals with disclosure of personal information without consent and 26 refers to an exemption for the personal information of an individual other than the person who has requested his or her personal information.

[74] Section 19 is an exemption under the *Access to Information Act* for personal information.

> (j.1) the fact that an individual is or was a *ministerial adviser* or a member of a *ministerial staff*, as those terms are defined in subsection 2(1) of the *Conflict of Interest Act*, as well as the individual's name and title,
>
> (k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,
>
> (l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
>
> (m) information about an individual who has been dead for more than twenty years.

The legislation is overseen by the federal Privacy Commissioner. This is a separate office from that of the Access to Information Commissioner. The Commissioner does not have order making powers. He or she receives complaints from individuals who claim to have been denied access to their personal information [s. 29 (1) (b)]. The Commissioner may investigate and make a recommendation as to whether the information was properly withheld or not [s. 35]. Either way, if the complainant is not satisfied, he or she can take the matter before the Federal Court for a binding ruling [s. 44 – 52].

The Commissioner can also receive complaints that personal information has been used or disclosed contrary to the legislation [s. 29 (1) (a)]. In addition, the Commissioner can, on his or her own initiative, review compliance with the legislation, including whether personal information has been disclosed contrary to the provisions of section 8, as discussed below. Again, the Commissioner can only make a recommendation as to whether the disclosure was authorized by the legislation. The Federal Court has also decided that it does not have the power to review allegations of improper use or disclosure of personal information.[75]

Nevertheless, the Commissioner must, if he or she finds non-compliance with the disclosure provisions of section 8, "provide the head of the institution with a report containing the findings of the investigation and any recommendations that the Commissioner considers appropriate"

[75] *Gauthier v. Canada* (1993), 58 FTR 161.

[s.37 (3)] and may include the findings in an Annual or Special Report to Parliament made pursuant to section 38 or 39.

In addition, as will be discussed below, disclosure of personal information by a government institution, in breach of the restrictions in section 8, could give rise to a civil cause of action by the individual affected, for invasion of privacy.

Restrictions on the Sharing of Personal Information

As with the British Columbia legislative regimes, the federal *Privacy* Act, ties the disclosure of personal information to the purposes for which it was collected in the first place and the circumstances under which it can be used. Section 4 provides that, "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."

Section 7 sets out limitation on the use of personal information.

> **Use of personal information**
> 7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except
> (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
>
> (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2)

Section 8 provides that personal information is not to be disclosed without the consent of the individual except in the limited circumstances set out in subsection 8 (2). As with the BC legislative provisions discussed above, disclosure under s. 8 is permitted, but, with the exception of a subpoena or court order, it is not required.

The provisions of section 8 (2) that are likely to be relevant to combating money laundering are as follows

> (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
> (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or any of its institutions and the government of a province, the council of the Westbank First Nation, the *council of a participating First Nation* as defined in subsection 2(1) of the *First Nations Jurisdiction over Education in British Columbia Act*, the council of a *participating First Nation* as defined in section 2 of the *Anishinabek Nation Education Agreement Act*, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(m) for any purpose where, in the opinion of the head of the institution,
(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure

Subsection 8 (4) requires an institution to keep copies of requests under paragraph (e) and a record of any information disclosed pursuant to the request. On a request by the Privacy Commissioner, copies of requests and records must be made available to the Privacy Commissioner.

Subsection 8 (5) requires the head of an institution to notify the Privacy Commissioner in writing of any disclosure under paragraph (2) (m) prior to the disclosure. Where it is not practical to notify before disclosure, notification must take place as soon as reasonably practicable or in any other case forthwith on the disclosure. The Privacy Commissioner may, if deemed appropriate, notify the individual to whom the information relates of the disclosure.

Section 9 requires that a record be kept of uses and disclosures that have not been previously identified:

> 9 (1) The head of a government institution shall retain a record of any use by the institution of personal information contained in a personal information bank or any use or purpose for which that information is disclosed by the institution where the use or purpose is not included in the statements of uses and purposes set forth pursuant to subparagraph 11(1)(a)(iv) and subsection 11(2) in the index referred to in section 11, and shall attach the record to the personal information.
>
> **Limitation**
> (2) Subsection (1) does not apply in respect of information disclosed pursuant to paragraph 8(2) (e).
>
> **Record forms part of personal information**
> (3) For the purposes of this Act, a record retained under subsection (1) shall be deemed to form part of the personal information to which it is attached.
>
> **Consistent uses**
> (4) Where personal information in a personal information bank under the control of a government institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not included in the statement of consistent uses set forth pursuant to subparagraph 11(1)(a)(iv) in the index referred to in section 11, the head of the government institution shall
>
> (a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and
>
> (b) ensure that the use is included in the next statement of consistent uses set forth in the index.

A very useful discussion of these provisions, in the context of information sharing for the purposes of national security, can be found in *Interjurisdictional Information Sharing and National Security: A Constitutional and Legislative Analysis.*[76]

For the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose [8 (2) (a)]

[76] Jacques Shore, Brian A Crane and John D Wilson," Interjurisdictional Information Sharing and National Security: A Constitutional and Legislative Analysis" (2017) 62:1 *McGill Law Journal* 207.

In *Bernard v. Canada (Attorney General)*[77] the Supreme Court of Canada found that an employer was not in breach of the *Privacy Act* when it released employee names and contact information to a Union so that it could contact those employees. The Court stated:

> "A use need not be identical to the purpose for which information was obtained in order to fall under s. 8 (2) (a) of the *Privacy Act*; it must only be consistent with that purpose. There need only be a sufficiently direct connection between the purpose and the proposed use, such that an employee would reasonably expect that the information could be used in the manner proposed. The union needed employee home contact information to represent the interests of employees, a use consistent with the purpose for which the government employer collected the information, namely, to contact employees about the terms and conditions of their employment. The information collected by the employer was for the appropriate administration of the employment relationship. This purpose is consistent with the union's intended use of the contact information."

However, disclosure of personal information regarding suspected money laundering which the RCMP has received from FINTRAC to a private lawyer, for use in a civil action is not a "consistent use".[78]

For any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure [8 (2) (b)]

In Re: Privacy Act (Can.)[79] the question before the Federal Court of Appeal was;

> "Is the disclosure of "personal information" by the Department of National Revenue to the Canada Employment Insurance Commission pursuant to the Ancillary Memorandum of Understanding for data capture and release of customs information on travellers authorized by section 8 of the *Privacy Act* and section 108 of the *Customs Act*?

Section 108 (1) of the *Customs* Act[80] provided that:

> An officer may communicate or allow to be communicated information obtained under this Act or the *Customs Tariff*, or allow inspection of or access to any book, record, writing or other document obtained by or on behalf of the Minister for the purposes of this Act or the *Customs Tariff*, to or by
>
> (a) any officer or any person employed in the Department of National Revenue;
> (b) any person, or any persons within a class of person, that the Minister may authorize, subject to such conditions as the Minister may specify;
> (c) or any person otherwise legally entitled thereto.

[77] [2014] 1 SCR 227.
[78] *Massa v. Sualim*, 2014 ONSC 5171 (CanLII), but see *Massa v. Sualim and Others*, 2014 ONSC 2103 (CanLII).
[79] [2000] 3 FC 82.
[80] RSC 1985, c 1 (2nd Supp).

The Court of Appeal found that, paragraph 8(2)(*b*) of the *Privacy Act* has a fairly wide meaning and that paragraph 108(1)(*b*) of the *Customs Act* gave the Minister of National Revenue the discretionary power to authorize the arrangement at issue with the Canadian Employment Insurance Commission. In very short reasons, the Supreme court of Canada confirmed the decision of the Federal Court of Appeal.[81]

For the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information [8 (2) (c)]

As with the BC legislation discussed above, this provision, although couched in the general terms of a permissive disclosure, by use of the word 'may" is in fact a disclosure that will in most cases be required. For a discussion of the scope of this section see *Law Society of Upper Canada v. Canada (Attorney General)*.[82]

To the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada [8 (2) d)]

This provision allows for the disclosure of personal information to the Attorney General to either commence legal proceedings or defend legal proceedings. The personal information may be about an individual directly involved in the proceedings of about an individual whose personal information is in some way relevant to the defence or prosecution of the proceeding.

To an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed [8 (2) (e)]

For the purposes of a disclosure pursuant to this provision, the investigative body must:

- be specified in the regulations[83] under the *Privacy Act*;
- make a written request for the information;
- require the information for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation; and

[81] [2001] 3 SCR 905.
[82] 89 OR (3d) 209.
[83] Privacy Regulations, SOR/83-508, Schedule II; see Appendix C for a list of investigative bodies specified in the regulations.

- specify the information that it requires.

This provision is not meant to allow for a fishing expedition. The federal Treasury Board Secretariat has published a document entitled, *Interim Directive on Privacy Practices*[84] which contains a set of detailed requirements relating to paragraph 8 (2) (c) in Appendix C.

Note that records of such requests for disclosure and copies of the information disclosed must be kept and provided to the Privacy commissioner on request. These records must be kept for 2 years.[85]

Under an agreement or arrangement between the Government of Canada or any of its institutions and the government of a province, the council of the Westbank First Nation, the *council of a participating First Nation* as defined in subsection 2(1) of the *First Nations Jurisdiction over Education in British Columbia Act,* the council of a *participating First Nation* as defined in section 2 of the *Anishinabek Nation Education Agreement Act,* the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation [8 (2) (f)]

The test for disclosure under this provision is:

- there must be an agreement or arrangement between the Government of Canada or the institution disclosing the information and the entity requesting the information;
- the requesting institution must be of the kind listed in the provision. For the purposes of combating money laundering, such institutions would typically be law enforcement agencies of provinces or municipalities, foreign governments or international organizations; and
- the purpose of the request must be to administer or enforce a law or carry out a lawful investigation.

Note that the test under paragraph (f) includes the administering or a law while the test under paragraph (e) is limited to enforcing a law or carrying out a lawful investigation. There is no list or definition of what constitutes institutions of provincial or foreign governments or an international organization of states or an international organization. Presumably organizations like a provincial police force or INTERPOL or a similar international organization would qualify, assuming the appropriate agreement is in place.

[84] Government of Canada, ”Interim Directive on Privacy Practices” (18 June 2020), *Canada.ca*, online: <www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309>.
[85] Privacy Regulations, SOR/83-508, s. 7.

For a discussion of this provision, as it relates to the sharing of information between the RCMP and the Director of Civil Forfeiture in British Columbia, see *Director of Civil Forfeiture v. Angel Acres Recreation and Festival Property Ltd.*[86] In that case, the agreement was between the Government of Canada and the government of British Columbia, but was deemed sufficient to allow for the sharing of information by the RCMP to the director of Civil Forfeiture.

For any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure [8 (2) (m) (i)]

Under this provision, the responsibility for determining whether the public interest in the disclosure of personal information in any particular situation outweighs the potential invasion of privacy is left to the head of the institution. Under subsection 8 (5) the institution must notify the Privacy Commissioner that it will be disclosing personal information in the public interest. The Privacy Commissioner may express concerns, if any, with the proposed disclosure and may, if appropriate, notify the individual whose information will be disclosed. It is, however, ultimately the institution's decision as to whether it will or will not release the information, and how much it will release. The Privacy Commissioner has no authority to prevent the disclosure.

However, under a complementary provision of the *Access to Information Act*, paragraph 19 (2) (c) allows disclosure of personal information if the disclosure would be in accordance with section 8 of the *Privacy Act*. In the context of that legislation, the Federal Court has ruled that it can review a refusal to disclose personal information and, in particular, question the exercise of discretion by the head of the institution under paragraph 8 (2) (m).[87]

Disincentive to disclosures

Unlike the provincial legislation in British Columbia, there are no statutory penalties under the *Privacy Act* if personal information is disclosed in contravention of that Act.

---

[86] 2009 BCSC 322; see also *British Columbia (Director of Civil Forfeiture) v. Angel Acres Recreation and Festival Property Ltd.*, 2010 BCCA 539 and *Angel Acres Recreation and Festival Property Ltd. v British Columbia (Attorney General)*, 2019 BCSC 1421.
[87] *Canada (Information Commissioner) v. Canada (Public Works*), 1996 CanLII 12411 (FC).

The Treasury Board requires notification to the Privacy Commissioner in the case of a privacy breach, which would include both the intentional and the unintentional disclosure of personal information in contravention of the *Privacy Act* as well as the theft or compromise of such information.[88] The Commissioner has the power to include a discussion of any breaches in either a Special or Annual Report.

The Federal Court has found that this is not an adequate remedy and has allowed class actions against the federal Government for breach of privacy to proceed when disclosure of personal information has occurred in contravention of the *Privacy Act*. These actions have been based on the tort of "intrusion upon seclusion" as recognized by the Ontario court of Appeal in *Jones v. Tsige*, discussed above.[89]

Again, there appears to be a built-in disincentive to the disclosure of personal information under s. 8 of the *Privacy Act* in any situation where there is doubt as to whether the provision to be relied upon would authorize the disclosure in any particular situation.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

Application

Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) deals with the collection, use and disclosure of personal information by federal works and undertakings and by other entities engaged in commercial activities that are not subject to comparable provincial legislation. Parts 2 – 6 deal with other matters. The legislation is based on the 10 Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, which is incorporated into the legislation by way of Schedule 1.

These principles are:

---

[88] Government of Canada, "Guidelines for Privacy Breaches," (20 May 2014), *Canada.ca*, online: < https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154>.

[89] Canada v. John Doe, 2016 FCA 191, *Canada v. John Doe*, 2016 FCA 191. See also: Barbara von Tigerstrom, Direct and Vicarious Liability for Tort Claims Involving Violation of Privacy (2018) 96:3 Canadian Bar Review 539.

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The legislation applies to federal works and undertakings and to other organizations in respect of personal information that

- the organization collects, uses or discloses in the course of commercial activities; or
- is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. [s. 4]

It is the first part of this application that will likely be relevant to the combating of money laundering.

"Personal information" is defined as "information about an identifiable individual". Notably, it need not be recorded as is required by the federal *Privacy Act* and FIPPA.

The legislation applies to the commercial activities of all federal works and undertakings, which includes any work, undertaking or business that is within the legislative authority of Parliament. Notably, this includes a bank or an authorized foreign bank as defined in section 2 of the *Bank Act*.[90]

"Commercial Activity" is defined as "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".

An "organization" is defined as including an association, a partnership, a person and a trade union.

[90] SC 1991, c 46. See the discussion below regarding additional confidentiality requirements that apply to banks.

As with the *Privacy Act*, the federal Information Commissioner is responsible for the oversight of the legislation. The role of the Commissioner is set out in sections 11–13. The Commissioner may receive and investigate complaints of a violation of the provisions of the legislation [s.11 (1)]. If the commissioner undertakes an investigation, within 1 year of the complaint, the Commissioner must prepare a Report that sets out:

> (a) the Commissioner's findings and recommendations;
> (b) any settlement that was reached by the parties;
> (c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and
> (d) the recourse, if any, that is available under section 14.

Section 14 provides that an individual may apply to the Federal Court for a hearing.

Under section 16, the Court has the power to:

> (a) order an organization to correct its practices in order to comply with Divisions 1 and 1.1;
> (b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and
> (c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

The Commissioner may also enter into Compliance Agreements to ensure compliance with the legislation [s. 17.1 & 17.2]

Jurisdiction

Section 26 (2) provides that, "The Governor in Council may, by order, … if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province."

By the *Organizations in the Province of British Columbia Exemption Order*[91] the federal government has found that the BC PIPA is substantially similar. The Regulation provides:

[91] SOR/2004-220.

> An organization, other than a federal work, undertaking or business, to which the *Personal Information Protection Act*, S.B.C. 2003, c. 63, of the Province of British Columbia, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act*, in respect of the collection, use and disclosure of personal information that occurs within the Province of British Columbia.

As discussed above in respect of the BC PIPA, there may be an overlap between that legislation and PIPEDA. Whether an organization that is not a federally regulated work or undertaking is subject to BC PIPA or to PIPEDA will depend on its circumstances and whether it collects uses or discloses personal information solely with in the province of British Columbia or whether is operations and its collection, use and disclosure of personal information takes place in more than one province.

Restrictions on the Sharing of Personal Information

As with other privacy legislation, the principle of consent is key to the safeguards for personal information found in PIPEDA. Principle 3 in the Schedule provides that, "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

Principle 5 provides, in part, that, "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."

Section 7 (3) sets out the circumstances in which personal information may be disclosed by an organization, that is subject to PIPEDA, without the knowledge or consent of the individual. The following provisions of section 7 (3) may apply to circumstances where personal information is to be disclosed to aid in combatting money laundering:

> (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> - required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records [s. 7 (3) (c)];

- made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
    - the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, [s. 7 (3) (c.1) (ii)]
    - the disclosure is requested for the purpose of administering any law of Canada or a province, [s. 7 (3) (c.1) (iii)]
- made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section [s. 7 (3) (c.2)];
- made on the initiative of the organization to a government institution or a part of a government institution and the organization
    - has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed [s. 7 (3)d) (i)],
- made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation [s. 7 (3) (d.1)]
- made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud [s.7 (3) (d.2)]
- required by law [s. 7 (3) (i)].

Required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records [s. 7 (3) (c)]

As in other situations, although this provision is couched in the general terms of "may disclose" compliance with a subpoena or warrant or other court order or for the purposes of complying with court rules, such as the requirement to produce documents on discover, is clearly mandatory. This provision is discussed by the Supreme Court of Canada in *Royal Bank of Canada v. Trang*.[92]

[92] [2016] 2 SCR 41.

However, there is an obligation on organizations to ensure that the information being produced clearly falls within the scope of the subpoena, warrant or order.[93]

Made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law [s. 7 (3) (c.1) (ii)]

The reference in this paragraph to "lawful authority" has been found by the Supreme Court of Canada to refer to something other than a subpoena or warrant.[94]

The House of Commons Standing Committee on Access to Information Privacy and Ethics completed a mandatory five review of PIPEDA in 2007. In its report the Committee recommended that consideration be given to clarifying what is meant by 'lawful authority' in section 7(3)(c.1). In its response the government agreed that there is a need to clarify the concept of lawful authority. Although the Office of the Privacy Commissioner stated publicly that it would not object to adding definition for the term "lawful authority," this has not happened.

> "The government's response also sought to clarify the overall intent of the paragraph: The government wishes to confirm that the purpose of s. 7(3) (c.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with PIPEDA."[95]

Enforcing the Immigration and Refugee Act has been found to be lawful authority.[96]

> 34 "Our Office finds that the respondent disclosed the complainant's personal information within the exemption to consent parameters of subparagraph 7(3) (c.1) (ii). Specifically, the respondent disclosed the complainant's personal information to a government institution that was investigating and gathering intelligence for the purpose of enforcing the *Immigration and Refugee Protection Act*."

---

[93] Airport must change its procedures for handling third-party requests for airport terminal video surveillance to comply with subsection 7(3) of PIPEDA, 2015 CanLII 93885 (PCC).
[94] *R. v. Spencer*, [2014] 2 SCR 212.
[95] Office of the Privacy Commissioner of Canada, " Customer Name and Address (CNA) Information Consultation Document," (August 11 2007) *Office of the Privacy Commissioner of Canada*, online: <www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/lar_071108/>.
[96] See *PIPEDA Case Summary* No. 2017-009, Re 2017 CarswellNat 9690, 2017 CarswellNat 9691at para 34.

Personal information, in the form of internet subscriber information, provided by Rogers to the police was found to be done in accordance with s. 7(3) (c.1) (ii), as police have the authority to investigate crimes.[97] The Court refused to exclude evidence obtained by way of a subsequent search warrant based on the subscriber information supplied by Rogers.[98]

The *Criminal Code* has been found to provide lawful authority for the purposes of s. 7(3) (c.1) (ii), specifically section 487.014(1):

> "(1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing."[99]

Made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of administering any law of Canada or a province,[s. 7 (3) (c.1) (iii)]

Note the difference between this provision and that in sub-paragraph (ii). This provision only applies to administering any law of Canada or a Province. An example of a request related to the administration of a law of Canada can be found in requests by Statistics Canada. Section 13 of the *Statistics Act*[100] provides as follows:

> 13 A person having the custody or charge of any documents or records that are maintained in any department or in any municipal office, corporation, business or organization, from which information sought in respect of the objects of this Act can be obtained or that would aid in the completion or correction of that information, shall grant access thereto for those purposes to a person authorized by the Chief Statistician to obtain that information or aid in the completion or correction of that information.

The Privacy Commissioner has found that a request by Statistics Canada pursuant to this provision meets the requirement of sub-paragraph (iii).[101]

---

[97] See *R. v. Brousseau* 2010 ONSC 6753.
[98] But, such situations in the criminal context must be considered very carefully and on a cases by case basis. See the disclaimer above and the comments of the Supreme Court of Canada in cases such as *R. v. Spencer*, [2014] 2 SCR 212 and the British Columbia Court of Appeal in *R. v. Caza*, 2015 BCCA 374 (CanLII)
[99] See *R. v. McNeice*, 2010 BCSC 154.
[100] RSC 1985, c S-19.
[101] Credit reporting agency is authorized to rely on exemption to consent in disclosing credit information to Statistics Canada, 2019 CanLII 117793 (PCC).

Made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section [s. 7 (3) (c.2)][102]

Section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*[103] provides as follows:

> 7. Subject to section 10.1, every person or entity referred to in section 5 shall, in accordance with the regulations, report to the Centre every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that
>
> (a) the transaction is related to the commission or the attempted commission of a money laundering offence; or
>
> (b) the transaction is related to the commission or the attempted commission of a terrorist activity financing offence.

Section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* sets out the entities to which that legislation applies.[104] Section 10.1 provides that the reporting requirement does not apply to persons or entities who are legal counsel or legal firms, when they are providing legal services.

This provision no doubt adds clarity to the requirement to comply with section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, but disclosure as required by this provision could also likely be made pursuant to sub-paragraph 7 (c.1) (iii) or paragraph 7 (i).

Made on the initiative of the organization to a government institution or a part of a government institution and the organization has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed [s. 7 (3) (d) (i)]

See *R. v. Orlandis-Habsburgo* 2017 ONCA 649 at para 110 where section 7(3)(d) was found not to apply to the information sharing arrangement between Horizon and the police because Horizon did not make any independent decision to disclose information based on its conclusion that reasonable grounds existed to believe that the appellants were engaged in criminal activity.

---

[102] See the discussion below about the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* below.

[103] SC 2000, c 17.

[104] See Appendix D for a list of the entities to which the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* applies.

Instead, Horizon passed any energy consumption data on to the police if they thought the data could interest the police, or if the police requested the data.

Made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation [s. 7 (3) (d.1)]

This provision does not appear to have been the subject of consideration yet by either the courts or the Privacy Commissioner.

Made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud [s.7 (3) (d.2)]

This provision does not appear to have been the subject of consideration yet by either the courts or the Privacy Commissioner.

Required by law [s. 7 (3) (i)]

Section 52 (1) of the Ontario *Occupational Health and Safety Act*[105] requires that notice be given in certain circumstances where a person is killed or critically injured from any cause at a workplace. The Ontario Labour Relations board has found that a disclosure of personal information pursuant to section 52 (1) is a disclosure "required by law" as contemplated by this provision.[106] It is likely that disclosure pursuant to paragraph 7 (3) (i) will, in some cases, overlap with the disclosure provisions in 7 (3) (c), (c.1) (ii), (c.1) (iii) and (c.2).

Disincentive to disclosures

As noted above, sections 14 – 17 provide that an application may be made to the Federal Court for remedies that include an award of damages, including damages for humiliation. An award

[105] RSO 1990, c O.1.
[106] International Association of Bridge, Structural, Ornamental and Reinforcing Iron Workers and its Local 736 v. E.S. Fox Ltd., 2006 CanLII 468 (ON LRB), online: <http://canlii.ca/t/1mbv8>, retrieved on 2020-10-08.

of damages is discretionary[107] and the Federal court has set the bar for an award of damages quite high. The leading case on the matter continues to be *Randall v. Nubodys Fitness Centres*[108] where the Court stated:

> [55] Pursuant to section 16 of the PIPEDA, an award of damages is not be made lightly. Such an award should only be made in the most egregious situations. I do not find the instant case to be an egregious situation.
>
> [56] Damages are awarded where the breach has been one of a very serious and violating nature such as video-taping and phone-line tapping, for example, which are not comparable to the breach in the case at bar.

The alleged injury must also flow directly from the misconduct or breach of PIPEDA.[109] To date, damage awards have been in the range of $4,500.00 to $5,000.[110]

Not only does PIPEDA provide for recourse to the Federal Court for damages if personal information has been disclosed in a manner contrary to PIPEDA, but the Supreme Court has referenced the protection of personal information in PIPEDA when assessing the reasonable expectation of privacy in the context of criminal proceedings and warrantless searches by police.[111] Paragraph 7 (3) (c.1) (ii) does not, therefore, provide additional cover to law enforcement for the obtaining of personal information and PIPEDA itself may limit the ability to collect information from organizations subject to that legislation by adding further context to the concept of reasonable expectation of privacy in the context of section 8 of the *Charter*.

Sectoral Regulation

Introduction

Generally speaking, both federally and provincially regulated entities that may have information, including personal information, relevant to the combating of money laundering will be subject to either the public or private sector legislation discussed above. Entities that meet the definition

---

[107] *Nammo v. TransUnion of Canada Inc*., 2010 FC 1284. The Court in this case cited 3 rationales for awarding damages: compensation, deterrence and vindication.
[108] 2010 FC 681.
[109] *Stevens v. SNF Maritime Metal Inc*., 2010 FC 1137.
[110] See *Nammo*, *supra* note 107 and *Landry v. Royal Bank of Canada*, 2011 FC 687.
[111] See *R. v. Spencer*, [2014] 2 SCR 212, see also *R. v. Jones*, [2017] 2 SCR 696.

of a "public body" as defined in FIPPA will be subject to the restrictions on the collection use and disclosure as set out in that legislation. Private sector entities that are "organizations" for the purposes of BC PIPA will be governed by that legislation, unless their activities are interprovincial, in which case the federal PIPEDA may apply to all or part of their activities.

Federal "government institutions" will be subject to the federal *Privacy Act*. Private entities which meet the definition of a "federal work, undertaking or business" will be governed by PIPEDA. Private entities, even though they do not meet the definition of a "federal work, undertaking or business", will also be subject to PIPEDA if they collect, use or disclose personal information in the course of commercial activities, unless they are subject to provincial privacy legislation such as BC PIPA.

In addition, there may be sectoral legislation or regulatory requirements regarding the collection, use or disclosure of information, including personal information, which supplement or add to the requirements of these legislated privacy regimes. In this section, we discuss any additional information sharing limitations which may hamper, or assist, the flow of information that could assist in the combating of money laundering.

British Columbia

British Columbia financial institutions

Trust Companies

Trust companies in British Columbia are incorporated pursuant to the *Business Corporations Act*, SBC 2002, c 57. The *Business Corporations Act* does not specifically deal with the collection, use or disclosure of personal information or non-personal information. Trust companies incorporated under the legislation will be subject to PIPA or PIPEDA with respect to the personal information that they collect, use or disclose, depending on the scope and nature of their business and the clients that they serve.

Credit Unions

Credit unions in British Columbia are incorporated pursuant to the *Credit Union Incorporation Act*, RSBC 1996, c 82.

Credit unions incorporated under the legislation will be subject to PIPA or PIPEDA with respect to the personal information that they collect, use or disclose, depending on the scope and nature of their business and the clients that they serve.

In addition, the legislation provides for the examination of certain records kept by a credit union by directors of the credit union and by members, auxiliary members and debenture holders [s. 39.42 & 29.44]. Confidentiality obligations are placed on anyone who receives information pursuant to the act:

> **Confidential information**
> 100 An individual or entity who, under this Act, obtains
> (a) information, or
> (b) records

that are submitted in accordance with a request that is made or an obligation that is imposed under this Act must not disclose the information or records to any individual or entity, other than for the purposes of administering this Act and the regulations, for the purposes of a prosecution or if required by law.

British Columbia Financial Services Authority

Introduction

Trust companies and credit unions in British Columbia are regulated by the British Columbia Financial Services Authority (BCFSA), created in 2019 by the *Financial Services Authority Act*, 2019, SBC 2019, c 14.[112] The BCFSA replaced the Financial Institutions Commission.

The Chief Executive Officer of the BCFSA serves in a number of statutory roles, including Superintendent of Financial Institutions, under *Financial Institutions Act*, RSBC 1996, c 141. The mandate of the BCFSA includes the administration of the *Credit Union Incorporation Act* discussed above and trust companies incorporated under the *Business Corporations Act* through the auspices of the *Financial Institutions Act*. The website of the Authority states as follows:

[112] The mandate of the authority is broader than regulation of credit unions and trust companies. See the Authority website for a full review of its mandate and the statutes and financial entities that it is responsible for: BC Financial Services Authority, <www.bcfsa.ca/index.aspx>.

> The BCFSA supervises and regulates financial institutions (credit unions, insurers and trust companies) and pension plans to determine whether they are in sound financial condition and are complying with their governing laws and supervisory standards.
>
> We use a risk-based supervisory framework to identify imprudent or unsafe business practices and intervenes on a timely basis, as required. Risk assessment is forward-looking. This view facilitates the early identification of issues or problems, and timely intervention where corrective actions need to be taken, so that there is a greater likelihood of a satisfactory resolution of issues.
>
> The focus is on early identification of risk and the allocation of resources to institutions and plans with the highest risk profile.[113]

The BSFSA's Financial Institutions Division investigates complaints of regulatory matters or criminal wrongdoing against BC credit unions and trust companies. The supervisory framework of the authority continues to be set out in a 2012 document published by the Financial Institutions Commission.[114]

The BCFSA is a "Public Body" listed in Schedule 2 of FIPPA. It is therefore subject to the restrictions on the collection, use and disclosure of personal information as set out in that legislation.

Financial Services Authority Act, 2019, SBC 2019, c 14

The *Financial Services Authority Act* itself does not place additional confidentiality obligations on the BCFSA with respect to either personal information or non-personal information. However, the *Financial Institutions Act* does.

Financial Institutions Act, RSBC 1996, c 141

Trust companies and credit unions are governed by the *Financial Institutions Act*. This includes extra-provincial credit unions[115] and extra-provincial trust companies.[116] Entities subject to the

---

[113] BC Financial Services Authority, "About Us" (2019), *BCFSA*, online: <www.bcfsa.ca/index.aspx?p=about_us/mandate>.
[114] BC Financial Services Authority, *Supervisory Framework*, (Vancouver: BCFSA, 2020).
[115] "Extraprovincial credit union" means a credit union that is incorporated by or under the laws of a jurisdiction other than British Columbia and that is, under those laws, licensed, registered or in any way authorized to carry on activities that are substantially the same as trust business or deposit business or both, but does not include a federal credit union within the meaning of the *Bank Act*, SC 1991, c 46.
[116] "Extraprovincial trust corporation" means a corporation incorporated by or under the laws of a jurisdiction other than British Columbia and is, under those laws, licensed, registered or in any way authorized to carry on activities

Financial Institutions Act will be subject to PIPA or the PIPEDA with respect to the personal information that they collect, use or disclose, depending on the scope and nature of their business and the clients that they serve.

The legislation itself also provides for the confidentiality of information, including personal information, held by entities subject to the legislation:

> **Misuse of confidential information**
> 104 If a director or officer of a financial institution or of an affiliate of a financial institution knows or reasonably ought to know that information is confidential to the financial institution, or to any affiliate of the financial institution the director or officer must not
>
> (a) disclose the information, or
>
> (b) enter into a transaction in which the director or officer makes use of the information,
>
> in order, directly or indirectly, to obtain a benefit or advantage for the director, officer or anyone else other than the financial institution or any affiliate of it.
>
> **Conduct review committee**
> 112 (1)The directors of a financial institution must elect from among themselves a conduct review committee consisting of at least 3 directors and, in the case of a trust company and an insurance company, 2/3 of the committee members must be unaffiliated directors.
>
> (2) The conduct review committee, in addition to the duties set out in Part 5, must establish written procedures
>
> (a) to provide disclosure in prescribed circumstances to customers of the financial institution, and
>
> (b) designed to prevent conflicts of interest and to resolve them if they occur, setting out in those procedures techniques for the identification of potential conflict of interest situations and for restricting the flow of confidential information.
>
> (3)The conduct review committee at intervals of not more than 2 years must review the written procedures established under subsection (2).

---

that are substantially the same as trust business or deposit business or both, but does not include a credit union, a bank or a corporation that is a subsidiary of a bank and is a loan company to which the *Trust and Loan Companies Act*, SC 1991, c 45 applies.

The *Financial Institutions Act* also provides for the authority of the Superintendent (the CEO of the BCFSA) to enter into agreement with other regulators to share information, including personal information.

Agreements with other jurisdictions
219 Subject to the regulations, the Authority may enter into agreements with the government of Canada, a province or another authority respecting the administration and enforcement of this Act or of comparable legislation of Canada or of another province and, without restricting the generality of this, the agreement may provide for the provision and exchange of information.

Collecting and sharing information respecting financial institutions
219.1 (1)For the purposes of administering this Act or assisting in the administration of the laws of another jurisdiction regulating deposit business, insurance business or trust business, the superintendent or a person described in section 209 (b) may, directly or indirectly, collect information from, and use information collected from,

(a) the Insurance Council of British Columbia, the deposit insurance corporation, an insurance compensation plan prescribed for the purposes of section 66 (2) or any entity that insures deposits of an extraprovincial trust corporation or an extraprovincial credit union in Canada,
(b) a financial institution or extraprovincial corporation or the auditor or actuary of a financial institution or extraprovincial corporation,
(c) a person licensed under Division 2, or issued a permit under Division 3, of Part 6,
(d) a society referred to in section 191,
(e) a law enforcement agency, government, governmental authority or financial services regulatory authority,
(f) a central credit union designated as the stabilization authority under section 282, or
(g) prescribed organizations referred to in section 289 (3) (p.3) or (p.31).

in British Columbia or elsewhere.

(2)For the purposes of administering this Act or assisting in the administration of the laws of another jurisdiction regulating deposit business, insurance business or trust business, the superintendent may disclose information to, or share information with,

(a) the Insurance Council of British Columbia, the deposit insurance corporation, an insurance compensation plan in Canada prescribed for the purposes of section 66 (2) or any entity in Canada that insures deposits of an extra provincial trust corporation or an extra provincial credit union,
(b) the auditor or actuary of a financial institution,
(c) a law enforcement agency, government, governmental authority, financial regulatory authority or securities regulatory authority in British Columbia,
(d) a law enforcement agency, government, governmental authority or financial services regulatory authority in another jurisdiction in Canada with which the

superintendent has entered into an arrangement or agreement that relates to or includes the sharing of information,
(e) a central credit union designated as the stabilization authority under section 282, or
(f) prescribed organizations referred to in section 289 (3) (p.3) or (p.31). [these organizations are only relevant to the insurance industry]

The *Financial Institutions Act* also provides for significant powers of investigation, including:

- The power to summon witnesses [s. 216 & s.232.1];
- The power of entry into business premises [s. 216.1 & s. 232.2];
- The power to obtain a warrant to enter a residence [s. 216.2 & s. 232.3]; and
- On entering a place under s.216.1 or 216.2 or s. 232.2 or 232.3,
    - examine records or any other things that may be relevant to the purposes of the investigation;
    - remove the records or things referred to in paragraph (a) for the purposes of examination or making copies or extracts;
    - require any person to produce or provide access to records or things in the person's possession or control that may be relevant to the purposes of the investigation;
    - require a person who may have information related to the purposes of the investigation, including personal information, to provide that information.[s. 216.3 & 232.4]

Information, including personal information, obtained during the course of administering the *Financial Institutions Act* or provided pursuant to section 219 or 219.1 discussed above, is subject to the following provisions:

Confidential information
218 (1)An individual or entity that creates, compiles or receives information or records under this Act or under an agreement referred to in section 219 or 219.01 of this Act must not, subject to subsections (2) and (3) of this section, disclose the information or records.

(2)With the consent of the Authority or the superintendent and subject to any conditions that the Authority or the superintendent imposes, the information or records may be disclosed
(a) for the purposes of administering this Act or the regulations,
(b) for the purposes of a prosecution, or
(c) if permitted by another provision of this Act or a provision of the regulations.
(3) The information or records must be disclosed if required by law.

Other Provincial Entities

BC Security Commission and Security Dealers

Canada does not have a federal securities regulator. Each province and territory has its own securities regulatory authority and its own set of laws and regulations. The 13 provincial and territorial securities regulators use rules known as "national instruments" to harmonize regulation across the country. Despite the lack of a federal regulator, most provincial security commission's work under a passport system, meaning the approval of one commission essentially allows for registration in another province.[117]

Securities Act RSBC 1996 c 418[118]

BC Securities Commission

The BC Securities Commission is created by the *Securities Act* [s.4], and is responsible for the administration of the *Securities Act*. The Commission is a Public Body within the meaning of FIPPA and is subject to the restrictions with respect to the collection, use and disclosure of personal information imposed by that legislation.

According to its website,

> The British Columbia Securities Commission aims to make B.C. a place where companies and investment funds ("issuers") can flourish and people can invest with confidence. To do that, we set, monitor, and enforce requirements for issuers looking to raise money and registered individuals and firms ("registrants") that buy and sell securities on behalf of investors. We also oversee a diverse array of organizations that play a role in the efficient operation of investment markets.[119]

The role of the Commission, as set out on its website[120], includes the following:

- review the disclosure that businesses raising capital must provide to investors;
- review applications for registration from those that trade securities, provide advice, or manage portfolios or investment funds to ensure they are qualified, ethical, and solvent;
- take action against those who contravene securities laws; and

---

[117] See Gowling WLG,"Guide to doing Business in Canada: Securities Law & Corporate Governance" (October 1 2020), *Gowling WLG*, online: <https://gowlingwlg.com/en/insights-resources/guides/2019/doing-business-in-canada-securities-law/>.
[118] The legislation will be replaced by the *Securities Act*, SBC 2004, c 43, which is not yet in force.
[119] British Columbia Securities Commission, "Industry" (2020), *BCSC*, online: <www.bcsc.bc.ca/industry>.
[120] British Columbia Securities Commission, "Mission, Values & Overall Benefits" (2020), *BCSC*, online: <www.bcsc.bc.ca/about/what-we-do/mission-values-benefits>.

- educate investors to protect themselves and industry participants to understand how to comply with securities law requirements.

The Commission's Enforcement Division protects investors and upholds market integrity by investigating complaints and taking action against misconduct in the investment market.[121]

In addition to the *Securities Act*, the Commission is responsible for a number of Regulations and Rules governing the trading of securities in the province and the regulation of Securities Dealers.[122]

An "Issuer" is defined as "a person who, (a) has a security outstanding, (b) is issuing a security, or (c) proposes to issue a security;

A "Dealer" is defined as "a person who trades in securities or derivatives as principal or agent".

A "Security" is defined as including:

> (a) a document, instrument or writing commonly known as a security,
> (b) a document evidencing title to, or an interest in, the capital, assets, property, profits, earnings or royalties of a person,
> (c) a document evidencing an option, subscription or other interest in or to a security,
> (d) a bond, debenture, note or other evidence of indebtedness, share, stock, unit, unit certificate, participation certificate, certificate of share or interest, preorganization certificate or subscription other than
>
> > (i) a contract of insurance issued by an insurer, and
> > (ii) an evidence of deposit issued by a savings institution,
>
> (e) an agreement under which the interest of the purchaser is valued, for the purposes of conversion or surrender, by reference to the value of a proportionate interest in a specified portfolio of assets, but does not include a contract issued by an insurer that provides for payment at maturity of an amount not less than 3/4 of the premiums paid by the purchaser for a benefit payable at maturity,
> (f) an agreement providing that money received will be repaid or treated as a subscription to shares, stock, units or interests at the option of the recipient or of any person,
> (g) a profit sharing agreement or certificate,
> (h) a certificate of interest in an oil, natural gas or mining lease, claim or royalty voting trust certificate,
> (i) an oil or natural gas royalty or lease or a fractional or other interest in either,
> (j) a collateral trust certificate,
> (k) an income or annuity contract, other than one made by an insurer,

[121] British Columbia Securities Commission, "Enforcement" (2020), *BCSC*, online: <www.bcsc.bc.ca/enforcement>.
[122] Again, for a listing of the various regulation, Rules and Policies, see the Commission's website: <www.bcsc.bc.ca/securities-law/law-and-policy/act-regulations-rules>.

(l) an investment contract,
(m) a document evidencing an interest in a scholarship or educational plan or trust,
(n) [Repealed 2019-38-1.]
(o) a permit under the *Oil and Gas Activities Act*,
(p) a derivative, or a derivative within a class of derivatives, described in an order made under section 3.2, or
(q) a derivative within a class of derivatives that are prescribed to be securities,
whether or not any of the above relate to an issuer, but does not include a security, or a security within a class of securities, described in an order made under section 3.1, or a prescribed security or a security within a prescribed class of securities;

A "Derivative" is defined as including,

(a) an option, swap, futures contract, forward contract or other financial or commodity contract or instrument if the market price or value of, or the delivery obligations, payment obligations or settlement obligations connected to, the option, swap, contract or instrument reference, or are derived from or based on, an underlying interest,
(b) a security, or a security within a class of securities, described in an order made under section 3.2, or
(c) a security within a class of securities that are prescribed to be derivatives,
but does not include
(d) a derivative, or a derivative within a class of derivatives, described in an order made under section 3.1, or
(e) a prescribed derivative or a derivative within a prescribed class of derivatives;

The Commission is a Public Body within the meaning of FIPPA and is subject to the restrictions with respect to the collection, use and disclosure of personal information imposed by that legislation.

The Commission also has confidentiality obligations imposed on it by the *Securities Act* which apply to both personal information and non-personal information.

Obligation to keep information confidential

11 (1) Every person acting under the authority of this Act must keep confidential all facts, information and records obtained or provided under this Act, or under a former enactment, except so far as the person's public duty requires or this Act permits the person to disclose them or to report or take official action on them.

(2) Subject to subsections (3) and (4), the facts, information and records referred to in subsection (1) must be released to the Ombudsperson[123] at the request of the Ombudsperson.

[123] The term "Ombudsperson" is not defined in the legislation. One assumes this section refers to the Ombudsperson appointed pursuant to the *Ombudsperson Act*, RSBC 1996, c 340.

(3) All facts, information and records that are obtained

(a) from a law enforcement agency, or

(b) pursuant to an investigation under this Act,

must only be released to the Ombudsperson if the Ombudsperson first produces the written consent of

(c) the law enforcement agency, or

(d) the person from whom the facts, information or records were obtained pursuant to the investigation,

to release the facts, information or records.

(4) All facts, information and records that could lead to the identification of an informant under this Act must only be released to the Ombudsperson if the person to whom the Ombudsperson makes the request first obtains the written consent of the informant to release the facts, information or records.

For a case dealing with the interplay between the confidentiality provisions of this section and the access provisions of FIPPA, see *British Columbia Securities Commission Investigation Records, Re*.[124] This case involved a request made under the access provisions of BCFIPPA on behalf of an individual for copies of records held by the Securities Commission. The request was denied and the matter appealed to the Information and Privacy Commissioner who upheld the refusal, in part, on the basis of section 11 (1) of the *Securities Act* and section 15 (1) (d) of BC FIPPA, which permits the head of a public body to refuse to disclose information, "that could reasonably be expected to … reveal the identity of an confidential source of law enforcement information. The Information and Privacy Commissioner found that the Securities Commission was involved in a law enforcement activity as defined by BC FIPPA.

Some records filed with the Commission must be made public.

Filing and inspection of records

169 (1) Unless otherwise indicated, records required by this Act or by the regulations to be filed must be filed by depositing them with the commission.

(2) Subject to the regulations, records required by this Act or by the regulations to be filed may be filed electronically in any form specified by the executive director.

(3)Subject to subsection (4), all records filed under this Act must be made available for public inspection during normal business hours.

(4) The commission may hold in confidence all or part of a record required to be filed under this Act if the commission considers that

[124] 2000 CanLII 14417 (BC IPC).

(a) a person whose information appears in the record would be unduly prejudiced by disclosure of the information, and
(b) the person's privacy interest outweighs the public's interest in having the information disclosed.

However, as provided in subsection (4), personal information may be withheld from the public record if the criteria in paragraphs (a) and (b) are both met.[125]

The Commission also has a mandate to both collect and disclose information for the purposes of administering the legislation or for the purposes of assisting in the administration of the securities legislation of other jurisdictions. This would include both the laws of other provinces and territories, but also regulators in other countries.

Information collection and sharing
169.1 (1) For the purposes of administering this Act or assisting in the administration of the securities laws of another jurisdiction, the commission may, directly or indirectly, collect information from, and use information collected from,
(a) an exchange, quotation and trade reporting system or clearing agency,
(a.1) a credit rating organization,
(a.2) a benchmark administrator,
(a.3) a benchmark contributor,
(a.4) an information processor,
(a.5) a trade repository,
(b) a self-regulatory body,
(c) a registrant or issuer, or
(d) a law enforcement agency, government, governmental authority, securities regulatory authority or financial regulatory authority, in British Columbia or elsewhere.

(2) For the purposes of administering this Act or assisting in the administration of the securities laws of another jurisdiction, the commission may disclose information to, or share information with,
(a) a person recognized under section 24,
(b) a law enforcement agency, government, governmental authority, securities regulatory authority or financial regulatory authority, or
(c) a person with whom the commission has entered into an arrangement or agreement that relates to or includes the sharing of information, in British Columbia or elsewhere.

(3) For the purposes of administering its bylaws, rules or other regulatory instruments or policies, assisting in the administration of the bylaws, rules or other regulatory

[125] See *Macdonald, Shymko & Company Ltd. (Re)*, 2016 BCSECCOM 47 and *DelMar Pharmaceuticals, Inc. (Re)*, 2017 BCSECCOM 262 (CanLII) for Commission decisions applying this section.

instruments or policies of another exchange, quotation and trade reporting system, clearing agency, self-regulatory body or trade repository, or assisting in the administration of this Act or the securities laws of another jurisdiction, a person recognized under section 24 may, directly or indirectly, collect information from, and use information collected from,

(a) an exchange, quotation and trade reporting system, clearing agency or trade repository,

(b) a self-regulatory body,

(c) a registrant or issuer, or

(d) a law enforcement agency, government, governmental authority, securities regulatory authority or financial regulatory authority, in British Columbia or elsewhere.

(4) For the purposes of administering its bylaws, rules or other regulatory instruments or policies, assisting in the administration of the bylaws, rules or other regulatory instruments or policies of another exchange, quotation and trade reporting system, clearing agency, self-regulatory body or trade repository, or assisting in the administration of this Act or the securities laws of another jurisdiction, a person recognized under section 24 may disclose information to, or share information with,

(a) an exchange, quotation and trade reporting system, clearing agency or trade repository,

(b) a self-regulatory body, or

(c) a law enforcement agency, government, governmental authority, securities regulatory authority or financial regulatory authority, in British Columbia or elsewhere.

(5) For the purposes of this section, "securities laws" means laws of a jurisdiction respecting the trading of securities or derivatives.

The Investment Industry Regulatory Organization of Canada (IROC)[126] as a self-regulatory body would be a body to which information, including personal information, could be disclosed.[127]

Securities Dealers

Securities Dealers are defined in the *Securities Act* as is the term securities. In addition to the requirements set out in that act with respect to the filing of information with the Commission, securities dealers will be subject to either PIPA or PIPEDA. In most cases, one would expect that securities dealers would be operating in more than one jurisdiction and it is likely that PIPEDA will apply to them. However, if BC PIPA is applicable, it must be remembered that the

[126]The Investment Industry Regulatory Organization of Canada is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada: see Investment Industry Regulatory Organization, "About IIROC" (2020) *IIROC*, online: <https://www.iiroc.ca/about/Pages/default.aspx>.

[127] *Golden Capital Securities Ltd. (Re)*, 2009 BCSECCOM 192 (CanLII).

definition of "investigation" in that act includes, in paragraph (e) " an investigation related to . . . trading in a security as defined in section 1 of the *Securities Act* if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying out investigations of trading in securities".

The ability to provide information under both PIPA and PIPEDA to the Commission or to an investigating organization such as IIROC was also briefly canvassed in *Golden Capital Securities Ltd. (Re)*.[128]

As noted above, Securities Dealers will have an obligation to provide information to the Commission and to other regulatory bodies as required by the *Securities Act*. Such obligations would be encompassed by a number of the provisions in BC PIPA, discussed above, including paragraphs 18 (1) (c), (i), (j) or (o). If PIPEDA is applicable, disclosure would likely fall under one of paragraph 7 (3) (c), (c.1) (ii) or (iii), (d) (i), (d.1), (d.2) or (1), as discussed above.

Land Title and Survey Authority

The following information is found on the website[129] of the BC Land Title and Survey Authority:

> The Land Title and Survey Authority of British Columbia (LTSA) is a publicly accountable, statutory corporation formed in 2005 responsible for operating the land title and survey systems of BC. These systems provide the foundation for all real property business and ownership in the province.
>
> The Province establishes the mandate, responsibilities and performance standards of the LTSA in the *Land Title and Survey Authority Act* [SBC 2004] c 66 and an Operating Agreement with the Province.

The act contains no reference to privacy, personal information, or confidentiality. As a public provincial body, FIPPA applies to the Authority.

---

[128] *Ibid.*
[129] Land Title and Survey Authority of British Columbia, "LTSA Mandate" (2020), *LTSA*, online: <https://ltsa.ca/about-ltsa/ltsa-mandate>.

The LTSA has developed a Privacy Management Framework, which is published on its website[130] and which deals with its Privacy Management Audit Plan, Personal Information Inventory and Personal Information Protection Policy.

Most importantly, when the legislation is in force, the LTSA will be responsible for Land Owner Transparency Registry to be created by the *Land Owner Transparency Act* [SBC 2019] Chapter 23. The following information is from the LTSA website[131]:

> The Land Owner Transparency Registry (LOTR) is part of the Province of BC's comprehensive plan to end hidden ownership of real estate in B.C.
>
> The first-of-its kind in Canada, LOTR is a registry of information about individuals who are deemed to have an indirect As defined in LOTA, this term refers to an estate in fee simple; a life estate in land; a right to occupy land under a lease that has a term of more than 10 years, or a right under an agreement for sale to occupy land, or require the transfer of an estate in fee simple interest in land (e.g. through corporations, trusts and partnerships) which will be housed in a searchable, public database.
>
> The Land Title and Survey Authority of British Columbia (LTSA) is responsible for developing and operating LOTR, as set out in the *Land Owner Transparency Act* (LOTA).
>
> The LTSA advises customers that the launch of the Land Owner Transparency Registry (LOTR) has been delayed to Fall 2020.
>
> The launch of LOTR is dependent upon the *Land Owner Transparency Act* being brought into force by the legislature and its associated regulations. Due to the COVID-19 pandemic, changes to the Province's legislative calendar resulted in this delay.

The LOTA will introduce a mandatory requirement for the reporting of any indirect ownership of property in the province. Indirect ownership includes interests that are not apparent from or reflected in the land title register, such as ownership by a trustee (Transparency Report) [s. 12]. The information will be recorded in a searchable public database. For more detail on how the Registry will work, see the LTSA website.[132] The requirement to report will apply retroactively.

---

[130] Land Title and Survey Authority of British Columbia, "Privacy Management Framework" (2020), *LTSA*, online: < https://www.ltsa.ca/privacy-management-framework/>.
[131] Land Title and Survey Authority of British Columbia, "News & Updates" (2020), *LTSA*, online: <www.ltsa.ca/blog/land-owner-transparency-registry>.
[132] Land Owner Transparency Registry, "Land Transparency, Protected" (2020), *LOTR*, online: < https://landtransparency.ca>.

A Transparency Report will have to be filed by entities that are designated by the legislation as Reporting Bodies, and may include some or all of the following information, known as Primary identification Information, depending on the nature of the entity that is required to file the Report:

- For an Individual (e.g. trustee or settlor of a relevant trust):
    - Full Name
    - Citizenship or permanent residence
    - City and Province/Country of residence (if in Canada or not)
    - Incorporation number and jurisdiction
- For a Corporation or LLC
    - Name
    - Registered office address and head office address, if applicable
    - Jurisdiction(s) of incorporation
- For a Partnership
    - Registered business name, if any
    - Type of partnership (e.g. LP, general)
    - Registered and/or head office address, as applicable
    - Jurisdiction of laws which govern the partnership

In addition, the following information will also be required:

Primary identification information plus the following about each interest holder:

- Date of birth, Address, Social insurance number, Tax number, Residence for tax purposes, Description of interest held in the reporting body (e.g. owns 25% of voting shares)
- Specific information based on the type of reporting body: Corporation: business number, incorporation number. Trust: information about the settlor (s. 19 or 21 of LOTA), Land Title Act trust instrument number, Partnership.
- Parcel Identifier (PID) assigned to the land for which the report relates.
- Name and contact information of person signing (certifying) the report.
- Prescribed information, if any.[133]

The Registry will be searchable by the public, but only for the primary identification information. The full Registry will be searchable by an Enforcement Officer appointed under the LOTA, Ministry of Finance Employees, Taxing Authority Employees, Law Enforcement Officers and Regulators (Securities Commission, FICOM, FINTRAC, Law Society).

Personal Information is defined in the LOTA as having the same meaning as in the *Freedom of Information and Protection of Privacy Act.*

[133] See Land Owner Transparency Registry, "About the Land Owner Transparency Act" (2020), *LOTR*, online: <https://landtransparency.ca/wp-content/uploads/2020/10/LOTR_Policy_Presentation-Oct-29.pdf>.

Section 53 sets out the powers of an Enforcement Officer to enter premises and to inspect documents, including obtaining information, including personal information relevant to the inspection.

Section 76 provides that Reporting Bodies must limit their use of any personal information that they collect for the purposes of filing a Transparency Report:

> **Prohibition against misuse of information obtained by reporting body**
> 76. A reporting body that obtains personal information for the purposes of this Act in respect of an interest holder or settlor must not disclose or use the personal information except as follows:
> (a) for the purpose of filing transparency declarations and transparency reports with the administrator;
> (b) to provide information under this Act to the administrator, enforcement officer or minister;
> (c) with the consent of the individual to whom the information relates;
> (d) as required or authorized by law;
> (e) for prescribed purposes, if any.

And section 86 provides that:

> **Enforcement officer not compellable**
> 86. The enforcement officer must not be compelled to disclose any information, document, record or thing obtained under Division 3 *[Inspections and Demands for Information]* of Part 4 *[Administration and Enforcement]* unless the disclosure is necessary for the administration or enforcement of this Act or is otherwise required by law.

Since the legislation specifically deals with the collection, use and disclosure of personal information, such collection, use and disclosure will be consistent with the requirement of PIPA[134] or PIPEDA[135] for those Reporting Bodies subject to either of those legislative regimes.

Money Services Businesses

This category includes Foreign Exchange Dealers, Money Transfer Services, Payment Services and Dealers in virtual Currencies. Although many of these services are provided by regulated

[134] Sections 12(1)(h) collection; 15(1)(h); use and 18(1)(h) disclosure.
[135] Sections 7(1)(e) (ii) collection; 7(2)(d); use and 7(3)(i) disclosure.

banks, credit unions and loan and trust companies, there are a number of other entities that provide some or all of these types of services. These entities fall under the general heading of Money Services Businesses and are not regulated in British Columbia. However, such entities are required to register with the Financial Transactions and Reports and Analysis Centre (FINTRAC). At present there is no financial intelligence unit equivalent to FINTRAC at the provincial level in BC. However, the creation of such a regulatory entity was recommended by the expert panel on money laundering which reported to the government in March of 2019.[136]

Depending on the nature of the transaction (within BC or interprovincial), Money Services Businesses are also subject to PIPA and PIPEDA, respectively.

Dealers in Precious Metals

The precious metals industry is federally regulated by the *Precious Metals Marking Act* (R.S.C., 1985, c. P-19). The object of this legislation is to ensure that the information provided to consumers about the quality of a precious metal article is uniform, and not misleading or deceptive.[137] A "Dealer" includes, "a person who is a manufacturer or an importer of any article to which this Act applies and any person who traffics by wholesale or retail in any such article and includes any director, manager, officer or agent or mandatary of that person".

The legislation contains no mention of privacy or confidentiality. However, dealers in precious metals will be subject to the applicable privacy legislation, either BC PIPA or PIPEDA, depending on the nature of their business.

Dealers in precious metals and stones must also fulfill specific obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and associated Regulations. PCMLTFA obligations apply once a person engages in the purchase or sale of precious metals, precious stones or jewellery in the amount of $10,000 or more in a single transaction. These obligations include verifying the identity of clients for certain activities and

[136]Maureen Maloney, Tsur Somerville and Brigitte Unger, *Combatting Money Laundering in BC Real Estate* (2019), Expert Panel on Money Laundering in BC Real Estate, Government of British Columbia, online: <https://www2.gov.bc.ca/assets/gov/housing-and-tenancy/real-estate-in-bc/combatting-money-laundering-report.pdf>, Recommendation # 10 at page 81.
[137]Competition Bureau of Canada, "Guide to the *Precious Metals Marketing Act* and Regulations" (4 July 2006), *Canada.ca*, online: < https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/01234.html>.

transactions, submitting reports about certain transactions and property to FINTRAC, and keeping certain transaction and client identification records in such a way that they can be provided to FINTRAC within 30 days if required to do so.[138] See the specific discussion below regarding FINTRAC.

Casinos, Lotteries, Gaming and Horseracing

While the *Canadian Criminal Code* is the federal source for the prohibition on gambling in Canada, the regulatory statutes (and regulators) are to be found at the provincial level. In the case of BC, this this is the *Gaming Control Act* [SBC 2002] c 14 which is overseen by the Gaming Policy and Enforcement Branch (GPEB).[139] The GPEB regulates all gambling[140] in British Columbia, including horse racing, ensures the integrity of gambling industry companies, people and equipment, and investigates allegations of wrongdoing. It is also responsible for regulatory oversight of the British Columbia Lottery Corporation (BCLC) (which conducts and manages lotteries, casinos and commercial bingo halls), all gambling services providers and gambling workers, B.C.'s horse racing industry, and licensed gambling events. GPEB operates pursuant to the provincial *Gaming Control Act* and *Gaming Control Regulations* and *Canada's Criminal Code*.

The GPEB and the British Columbia Lottery Corporation are both subject to FIPPA. Individual gaming operations will be subject to either the PIPA or PIPEDA.

Lawyers

The Law Society of British Columbia[141] regulates the legal profession in British Columbia. Its authority comes from the *Legal Profession Act*,[142] Law Society Rules[143]and Code of

[138] Financial Transactions and Reports Analysis Centre of Canada, "Dealers in precious metals and stones" (16 June 2020), online: <www.fintrac-canafe.gc.ca/re-ed/dpms-eng>.
[139] Government of British Columbia, " Gambling Laws, Regulations & Policies" *gov.bc.ca*, online: < https://www2.gov.bc.ca/gov/content/sports-culture/gambling-fundraising/gambling-in-bc/laws-regulations-policies > .
[140] See a discussion of the various types of gambling overseen by the Gaming Policy and Enforcement Branch at Government of British Columbia, "Gambling in BC" *gov.bc.ca*, online: < https://www2.gov.bc.ca/gov/content/sports-culture/gambling-fundraising/gambling-in-bc >.
[141] The Law Society of British Columbia, <www.lawsociety.bc.ca>.
[142] SBC 1998, c 9.
[143] The Law Society of British Columbia, *Law Society Rules 2015*, Vancouver: LSBC, 2020.

Professional Conduct.[144] Its duty is to protect the public interest in the administration of justice by setting and enforcing standards of professional conduct for lawyers. The Law Society is also subject to FIPPA, as per Schedule 3 of that Act. The Law Society's website states that "all personal information in our custody and control will be collected, used and disclosed in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Legal Profession* Act, the Law Society Rules and other applicable legislation".[145]

The most relevant provisions of the *Legal Profession Act* are:

> **Non-disclosure of privileged and confidential information**
> **88** (1) [Repealed 2012-16-46.]
> (1.1) A person who is required under this Act or the rules to provide information, files or records that are confidential or subject to a solicitor client privilege must do so, despite the confidentiality or privilege.
>
> (1.2) Information, files or records that are provided in accordance with subsection (1.3) are admissible in a proceeding under Part 2, 3, 4 or 5 of this Act, despite the confidentiality or privilege.
>
> (1.3) A lawyer who or a law firm that, in accordance with this Act and the rules, provides the society with any information, files or records that are confidential or subject to a solicitor client privilege is deemed conclusively not to have breached any duty or obligation that would otherwise have been owed to the society or the client not to disclose the information, files or records.
>
> (2) Despite section 14 of the *Freedom of Information and Protection of Privacy Act*, a person who, in the course of exercising powers or carrying out duties under this Act, acquires information, files or records that are confidential or are subject to solicitor client privilege has the same obligation respecting the disclosure of that information as the person from whom the information, files or records were obtained.
>
> (3) A person who, during the course of an investigation, audit, inquiry or hearing under this Act, acquires information or records that are confidential or subject to solicitor client privilege must not disclose that information or those records to any person except for a purpose contemplated by this Act or the rules.
>
> (4) A person who, during the course of an appeal under section 48 or an application under the *Judicial Review Procedure Act* respecting a matter under this Act, acquires

[144] The Law Society of British Columbia, *Code of Professional Conduct for British Columbia*, Vancouver: LSBC, 2019.
[145] The Law Society of British Columbia, "Privacy Statement", (2020), *LSBC*, online: <www.lawsociety.bc.ca/privacy/>.

information or records that are confidential or are subject to solicitor client privilege must not

(a) use the information other than for the purpose for which it was obtained, or
(b) disclose the information to any person.

(5) The Court of Appeal, on an appeal under section 48, and the Supreme Court, on an application under the *Judicial Review Procedure Act* respecting a matter under this Act, may exclude members of the public from the hearing of the appeal or application if the court considers the exclusion is necessary to prevent the disclosure of information, files or records that are confidential or subject to solicitor client privilege.

(6) In giving reasons for judgment on an appeal or application referred to in subsection (5), the Court of Appeal or the Supreme Court must take all reasonable precautions to avoid including in those reasons any information before the court on the appeal or application that is confidential or subject to solicitor client privilege.

(7) Despite section 14 of the *Freedom of Information and Protection of Privacy Act*, the benchers may make rules for the purpose of ensuring the non-disclosure of any confidential information or information that, but for this Act, would be subject to solicitor client privilege, and the rules may be made applicable to any person who, in the course of any proceeding under this Act, would acquire the confidential or privileged information.

(8)Section 47 (4) of the *Freedom of Information and Protection of Privacy Act* does not apply to information that, but for this Act and the production of the information to the commissioner under that Act, would be subject to solicitor client privilege.

The most relevant provision of the Legal Society Rules is:

Information sharing

Sharing information with a governing body
2-27.1 (1) This rule applies to information collected in accordance with the Act and these rules about a lawyer, former lawyer, law firm, articled student, applicant, visiting lawyer or a person who has applied to be a member of a governing body.
(2) Subject to subrule (3), when it appears to the Executive Director to be appropriate in the public interest, the Executive Director may provide information to a governing body.
(3) The Executive Director must not provide confidential or privileged information to a governing body under subrule (2) unless the Executive Director is satisfied that the information

(a) is adequately protected against disclosure, and
(b) will not be used for any purpose other than the regulation of the legal profession in the jurisdiction of the governing body.

The Rules also contain a number of specific provisions that permit the sharing of information. These are Rules 2-53 (4), 3-3 (5), 3-23 (3), 3-46 (5) (c and 4-8 (5) which permit the Executive Director, in specific circumstances to deliver any information or documents that may be evidence of an offence to a law enforcement agency.

The Code has the most comprehensive discussion of a lawyer's duty of confidentiality:

3.3 Confidentiality

Confidential information
3.3-1 A lawyer at all times must hold in strict confidence all information concerning the business and affairs of a client acquired in the course of the professional relationship and must not divulge any such information unless:
(a) expressly or impliedly authorized by the client;
(b) required by law or a court to do so;
(c) required to deliver the information to the Law Society, or
(d) otherwise permitted by this rule.

Use of confidential information
3.3-2 A lawyer must not use or disclose a client's or former client's confidential information to the disadvantage of the client or former client, or for the benefit of the lawyer or a third person without the consent of the client or former client.

Lawyers' obligation to claim privilege when faced with requirement to surrender document
3.3-2.1 A lawyer who is required, under federal or provincial legislation, to produce a document or provide information that is or may be privileged must, unless the client waives the privilege, claim solicitor-client privilege in respect of the document.

Future harm / public safety exception
3.3-3 A lawyer may disclose confidential information, but must not disclose more information than is required, when the lawyer believes on reasonable grounds that there is an imminent risk of death or serious bodily harm, and disclosure is necessary to prevent the death or harm.

3.3-4 If it is alleged that a lawyer or the lawyer's associates or employees:
(a) have committed a criminal offence involving a client's affairs;
(b) are civilly liable with respect to a matter involving a client's affairs;
(c) have committed acts of professional negligence; or
(d) have engaged in acts of professional misconduct or conduct unbecoming a lawyer,
the lawyer may disclose confidential information in order to defend against the allegations, but must not disclose more information than is required.

3.3-5 A lawyer may disclose confidential information in order to establish or collect the lawyer's fees, but must not disclose more information than is required.

3.3-6 A lawyer may disclose confidential information to another lawyer to secure legal or ethical advice about the lawyer's proposed conduct.

3.3-7 A lawyer may disclose confidential information to the extent reasonably necessary to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a law firm, but only if the information disclosed does not compromise the solicitor-client privilege or otherwise prejudice the client.

In addition, 3.2-7 and 3.2.-8 deal with a lawyer's obligation not to become involved in any criminal activity on behalf of a client and, disclosure requirement by a lawyer who is employed by an organization where he or she suspects dishonesty or fraud.

Dishonesty, fraud by client
3.2-7 A lawyer must not engage in any activity that the lawyer knows or ought to know assists in or encourages any dishonesty, crime or fraud.

Dishonesty, fraud when client an organization
3.2-8 A lawyer who is employed or retained by an organization to act in a matter in which the lawyer knows or ought to know that the organization has acted, is acting or intends to act dishonestly, criminally or fraudulently, must do the following, in addition to his or her obligations under rule 3.2-7:
(a) advise the person from whom the lawyer takes instructions and the chief legal officer, or both the chief legal officer and the chief executive officer, that the proposed conduct is, was or would be dishonest, criminal or fraudulent and should be stopped;
(b) if necessary because the person from whom the lawyer takes instructions, the chief legal officer or the chief executive officer refuses to cause the proposed conduct to be stopped, advise progressively the next highest persons or groups, including ultimately, the board of directors, the board of trustees, or the appropriate committee of the board, that the proposed conduct was, is or would be dishonest, criminal or fraudulent and should be stopped; and
(c) if the organization, despite the lawyer's advice, continues with or intends to pursue the proposed wrongful conduct, withdraw from acting in the matter in accordance with section 3.7.

In all cases, the Code provides a useful commentary as to practical application of the obligations imposed by it.

Even without these statutory and regulatory requirements for confidentiality, lawyers are subject to the common law rule of solicitor client privilege.[146]

Chartered accountants

The Chartered Professional Accountants of British Columbia (CPABC) is the body that trains, governs, and regulates over 37,000 CPA members and 5,000 CPA students. The CPABC and similar bodies in the other provinces are members of the Chartered Professional Accountants of Canada (CPA Canada). [147]The CPABC is subject to FIPPA, as per Schedule 3 of that Act.

The CPABC is created by the *Chartered Professional Accountants Act*[148] which also governs and regulates chartered accountants practicing in British Columbia. That act has the following provisions related to confidentiality when the CPABC becomes involved in a practice review regarding one of its members.

> **Practice review and investigation**
> 51 (1) An officer, a committee or any other person designated in accordance with the bylaws may conduct a practice review or an investigation.
>
> (2) A reviewer may conduct a practice review of a person listed in subsection (4) (a) by reviewing the person's professional practice for the purpose of identifying any deficiencies in the practice or the fitness or professional conduct of the person.
>
> (3) An investigator may conduct an investigation of the conduct of a person listed in subsection (4) (b) to determine whether grounds exist for disciplinary action against that person under section 53.
>
> (4) The persons
> (a) for the purposes of subsection (2) are as follows:
> (i) a member;
> (ii) a professional accounting corporation;
> (iii) a registered firm, and
> (b) for the purposes of subsection (3) are as follows:
> (i) a member;
> (ii) a former member;

[146] A detailed discussion of the rule of solicitor client privilege, which has been recognized as a law of evidence, is beyond the scope of this Report. See *Descôteaux et al. v. Mierzwinski*, [1982] 1 SCR 860 and jurisprudence implementing the rule.
[147] Chartered Professional Accountants British Columbia, "About Us", (2020), *CPABC*, online: <www.bccpa.ca/about-cpabc/>.
[148] SBC 2015, c 1.

(iii) a student;
(iv) a professional accounting corporation;
(v) a former professional accounting corporation;
(vi) a registered firm;
(vii) a former registered firm.

(5) If the reviewer or investigator is satisfied on reasonable grounds that a member or student possesses any information, record or thing that is relevant to a practice review or an investigation, the reviewer or investigator may make a written request to the member or student requiring the member or student to answer inquiries of the reviewer or investigator relating to the practice review or investigation and to produce to the reviewer or investigator the record or thing.

(6) A person who receives a request under subsection (5) must comply with the request.

(7) If a person who receives a request under subsection (5) refuses or neglects as soon as practicable to comply with the request, the CPABC may apply to the court for an order requiring the person to comply.

(8) The court, on being satisfied that a person has contravened subsection (6), may order that the person comply and may impose requirements as to time and manner of compliance.

(9) A person must not refuse to comply with this section on the grounds of confidentiality.

(10) A person who, in accordance with this Act and the bylaws, provides the reviewer or investigator with any information, records or things that are confidential or subject to a solicitor-client privilege is deemed conclusively not to have breached any duty or obligation that would otherwise have been owed to a client not to disclose the information, records or things.

(11) A provision of this section that applies to a member also applies to a professional accounting corporation and a registered firm.

Confidentiality
69 (1) A person acting under this Act must keep confidential all facts, information and records obtained or provided under this Act or under a former enactment, except so far as the person's public duty requires or this Act or the bylaws permit the person to disclose or to report or take official action on the facts, information and records.

(2) Insofar as the laws of British Columbia apply, a person must not give, or be compelled to give, evidence in a court or in proceedings of a judicial nature concerning knowledge gained in the exercise of a power or in the performance of a duty under Part 7 *[Practice Reviews, Investigations and Hearings]* unless
(a) the proceedings are under this Act, or
(b) disclosure of the knowledge is authorized under subsection (1) or under the bylaws.

(3) The records relating to the exercise of a power or the performance of a duty under Part 7 are not compellable in a court or in proceedings of a judicial nature insofar as the laws of British Columbia apply unless

(a) the proceedings are under this Act, or

(b) disclosure of the knowledge is authorized under subsection (1) or under the bylaws.

Individual chartered accountants, whether they are sole practitioners, inter-provincial or national firms will be subject to either PIPA or PIPEDA.

In addition to their privacy obligations pursuant to these statutes, chartered accountants are subject to the CPABC Code Of Professional Conduct August 2018.[149] The Code has a number of provisions dealing with confidentiality, the most salient of which for the purposes of this discussion are the following. Rule 208 also has a commentary discussing the import of the requirements for confidentiality of client information as set out in that Rule.

Fundamental Principles Governing conduct

Confidentiality

Chartered Professional Accountants protect confidential information acquired as a result of professional, employment and business relationships and do not disclose it without proper and CPABC specific authority, nor do they exploit such information for their personal advantage or the advantage of a third party. The principle of confidentiality obliges registrants to protect and maintain the confidentiality of information both outside of and within a registrant's firm or employing organization and to properly address a situation that may arise when confidentiality is breached.

The disclosure of confidential information by a registrant may be required or appropriate where such disclosure is:

- Permitted or authorized by the client or employer;
- Required by law; or
- Permitted or required by a professional right or duty, when not prohibited by law.

Definitions

"confidential information" means information acquired in the course of a professional services relationship with a party. Such information is confidential to the party regardless of the nature or source of the information or the fact that others may share the knowledge. Such information remains confidential until the party expressly or impliedly authorizes

[149] Chartered Professional Accountants British Columbia, *CPABC Code of Professional Conduct*, Vancouver: CPABC, 2020.

it to be divulged. In the case of an employee-employer relationship, a member or student has legal obligations to the employer that include a duty of confidentiality. The CPA Code imposes a duty of confidentiality as a professional obligation, which is in addition to the member's or student's legal obligation to the employer.

Guidance - Rule 102

9. Registrants are reminded that confidentiality agreements with respect to matters described in Rule 102.1 through 102.4 do not provide an exemption from the reporting requirements of the CPA Code

Public Protection

208 Confidentiality of information

208.1 A registrant shall not disclose any confidential information concerning the affairs of any client, former client, employer or former employer except when:

(a) properly acting in the course of carrying out professional duties;

(b) such information should properly be disclosed for purposes of Rules 101, 211 or 302 or under the Act or bylaws;

(c) such information is required to be disclosed by order of lawful authority or, in the proper exercise of their duties, by the Board, or a committee, officer or other agent of CPABC;

(d) justified in order to defend the registrant or any associates or employees of the registrant against any lawsuit or other legal proceeding or against alleged professional misconduct or in any legal proceeding for recovery of unpaid professional fees and disbursements, but only to the extent necessary for such purpose; or

(e) the client, former client, employer or former employer, as the case may be, has provided consent to such disclosure.

208.2 A registrant shall not use confidential information of any client, former client, employer or former employer, as the case may be, obtained in the course of professional work for such client or employer:

(a) for the advantage of the registrant;

(b) for the advantage of a third party; or

(c) to the disadvantage of such client or employer without the consent of the client, former client, employer or former employer.

208.3 A registrant shall:

(a) take appropriate measures to maintain and protect confidential information of any client, former client, employer or former employer, as the case may be and to ensure that access to such information by another person is limited to those with legitimate purpose to access the information; and

(b) obtain the written agreement of any such person to carefully and faithfully preserve the confidentiality of any such information and not to make use of such information other than as shall be required in the performance of appropriate professional services.

BC Notaries

The Society of Notaries Public of BC[150] is in charge of regulating the members of the Society pursuant to the *Notaries Act of British Columbia*.[151] As that Act contains nothing substantial regarding confidentiality, however, paragraphs 61 (3), (4) and (4) of the Act provide that:

> **Responsibility of members**
> 61 (3) Nothing in this Act affects, modifies or limits any law applicable to the fiduciary, confidential or ethical relationships between a member and a person receiving the professional services of that member.
>
> (4)The relationship between a notary corporation carrying on business as permitted under this Act and a person receiving notary services provided by the corporation is subject to all applicable law relating to the fiduciary, confidential and ethical relationships that exist between a member and the member's client.
>
> (5)All rights and obligations pertaining to professional communications made to or information received by a member, or in respect of any advice given by a member, apply to a notary corporation and its shareholders, directors, officers, employees and contractors.

The Society itself is subject to FIPPA as per Schedule 3 of that Act.

Individual notaries are subject to BC PIPA with respect to personal information that they collect use or disclose from clients in British Columbia. They are also bound by the Rules of the Society.[152] The Rules contain the following under the heading "Informed Consent"

> **11.05 Informed Consent**
> (b) Prior to representing more than one client in circumstances addressed in 11.04 or 11.05, the Member shall satisfy the requirements set out in (a) above and, in addition, shall:
>
> (i) inform each such party in writing as soon as possible that the Member acts for more than one party and that should a conflict arise which cannot be resolved, the Member cannot act for any party and that no information received in connection with the matter from one can be treated as confidential so far as any of the others is concerned;

[150] Society of Notaries Public of British Columbia, "Find a Notary", *SNPBC*, online: <https://find.notaries.bc.ca/home/index.rails>.
[151] RSBC 1996, c 334.
[152] Society of Notaries Public of British Columbia, *Rules of the Society*, Vancouver: Society of Notaries Public of BC, 2020.

The Rules further deal with the circumstances in which information collected by the society may be disclosed:

> **16.11 Disclosure of Corporate Information**
> All information and documents relating to a Notary Corporation which have been received by the Society under this Part are confidential, and shall not be disclosed to any person except that:
>
> (a) any such information and documents may be used by the Society for its governing and administering the affairs of the Society;
> (b) the following information may be disclosed upon request to any person: (i) the name of the Corporation;
> (ii) a Corporation's place of business;
> (iii) whether a Notary Corporation has a valid permit issued under Section 58 of the Act;
> (iv) whether a specified Member of the Society is an employee or voting shareholder of a Corporation; and
> (v) whether a specified Notary Corporation is a voting shareholder of a Notary Corporation.

Notaries are also subject to the obligations of professional secrecy with respect to the affairs of their clients.[153]

Real estate agents

The Real Estate Council of British Columbia (RECBC) regulates and enforces standards for real estate professionals in BC under the *Real Estate Services Act.*[154] The RECBC also administers the Real Estate Services Regulation[155] and the Real Estate Rules[156] which govern the conduct of real estate agents and brokers.

The RECBC is subject to FIPPA as per Schedule 3 of that act.

The *Real Estate Services Act* has the following provisions regarding confidentiality:

> **Information-sharing and confidentiality**
> 122 (1) The real estate council and the superintendent may, for the purposes of their powers and duties under this Act, share information and records obtained under this Act.

---

[153] *Chambre des notaires du Québec c. Canada (Procureur général)*, 2010 QCCS 4215 (CanLII); upheld by the Supreme Court - *Canada (Attorney General) v. Chambre des notaires du Québec*, [2016] 1 SCR 336.
[154] SBC 2004 c. 42.
[155] BC Reg 506/2004.
[156] Real Estate Council of British Columbia, <www.recbc.ca/public-protection/legislation-policies?tab=Real-Estate-Rules>.

(2) A person who, in the course of exercising powers and performing duties under this Act, obtains information or records that are submitted in accordance with a request or obligation under this Act, must not disclose the information or records to any person other than

(a) for the purposes of administering this Act, the regulations, the rules and the bylaws,

(b) for the purposes of a proceeding for an offence, or

(c) for a purpose authorized under the *Freedom of Information and Protection of Privacy Act* or as required by law.

(3) Except in respect of a proceeding under this Act, a person to whom subsection (2) applies may not be compelled in a civil proceeding to disclose or give evidence respecting any information or records obtained in the course of exercising the person's powers or performing the person's duties under this Act.

The Real Estate Rules contain a number of provisions regarding the nature of information that must be collected and from a client and disclosed as part of a transaction. Subject to those mandatory disclosures, the Rules require that certain information be kept confidential.

Duties to clients

3-3.1

Subject to sections 3-3.1 and 3-3.2, if a client engages a brokerage to provide real estate services to or on behalf of the client, the brokerage and its related licensees must do all of the following:

(e) maintain the confidentiality of information respecting the client;

Modification of duties

3-3.1

(1) By agreement between the brokerage and the client, one or more of the duties under section 3-3 may be modified or made inapplicable.

(4) Despite an agreement referred to in subsection (1), the brokerage must

(b) not disclose any confidential information concerning a client to any other person unless

(i) authorized by that client, or

(ii) required by law.

Individual real estate agents and brokers will be subject to the requirements of PIPA and, possibly, PIPEDA.

Mortgage brokers

The Registrar of Mortgage Brokers[157], a division of the BC Financial Services Authority (BCFSA), discussed above, is tasked with protecting the public and enhancing the integrity of the mortgage broker industry by enforcing mortgage broker suitability requirements and reducing and preventing market misconduct under the *Mortgage Brokers Act*[158] and Regulations.[159] The Act and Regulations provide for specific information that brokers must provide to the BCFSA. The Act and Regulations do not contain anything pertaining to privacy, personal information, or confidentiality. The BCFSA is subject to FIPPA with respect to personal information that it collects during the course of its regulation of mortgage brokers. Individual mortgage brokers would be subject to the restrictions on the collection, use and disclosure of personal information found in PIPA or PIPEDA.

Motor vehicle dealers

The Vehicle Sales Authority of British Columbia (VSA)[160] is an independent regulatory agency authorized by the provincial government to administer and enforce the *Motor Dealer Act*[161] and parts of the *Business Practices and Consumer Protection Act*[162] as it relates to the sale of personal-use motor vehicles in B.C. The Registrar is responsible for, *inter alia* licensing of motor vehicle dealerships, salespeople, broker agents, broker agent representatives and wholesalers; investigating consumer complaints, providing dispute resolution and undertaking compliance action.

The VSA also administers the Motor dealer Consumer Compensation Fund.[163]

The VSA is subject to FIPPA as per Schedule 2.

The *Motor Dealer Act* contains the following provisions regarding confidentiality:

---

[157] British Columbia Financial Services Authority, "Mortgage Brokers" (2019), *BCFSA*, online: <www.bcfsa.ca/index.aspx?p=mortgage_brokers/index> .
[158] RSBC 1996 c 3.1
[159] BC Reg 100/73.
[160] Vehicle Sales Authority of BC, <https://mvsabc.com/>, Formerly the Motor Dealer council and still listed as such in Schedule 2 to BC FIPPA.
[161] RSBC 1996 c 316.
[162] SBC 2004 c 2.
[163] The Fund provides compensation primarily to consumers who lost money because a motor dealer went out of business or has failed to meet certain legal obligations. See Vehicle Sales Authority of BC, <https://mvsabc.com/consumers/complaints/recent-compensation-claim-fund-decisions/>.

Confidentiality of information

29 (1) A person employed in the administration of this Act, including a person making an inquiry, inspection, examination, test or investigation under section 26, must maintain secrecy in respect of all matters that come to his or her knowledge in the course of his or her duties, employment, inquiry, inspection, examination, test or investigation, and must not communicate information obtained under this Act to another person not legally entitled to it except

(a) as may be required or permitted in the administration of this Act or the regulations or proceedings under this Act or the regulations,

(b) to the employee's counsel or to the court in a proceeding under this Act or the regulations,

(c) to a department or agency of a government engaged in the administration of laws, measures or rulings similar to this Act or Acts for the general protection of consumers,

(d) with the consent of the person to whom the information relates, or

(e) to a law enforcement agency if the employee suspects that a criminal offence has been committed.

(2) Except in respect of a proceeding under this Act or the regulations, a person to whom subsection (1) applies is not, in a civil proceeding, compelled to give evidence respecting information obtained by the person in the course of his or her duties, employment, inquiry, inspection, examination, test or investigation.

Financial statements

32 (1) A motor dealer must, if requested by the registrar, file a financial statement signed by the motor dealer in the form and containing the information required by the registrar and certified by a person licensed as an accountant under an Act.

(2) The information contained in a financial statement filed under subsection (1) is confidential and a person must not communicate that information to or allow access to or inspection of that information by another person not legally entitled to it under this Act.

The *Business Practices and Consumer Protection Act* has the following provision regarding confidentiality:

Confidentiality

185 (1) A person who is engaged in the administration of this Act or the regulations and who has custody of, access to or control over information or records under this Act must not disclose the information or records to any other person except

(a) if disclosure is for the purposes of the administration of this Act or the regulations,

(b) with the consent of the person to whom the information or record relates,

(c) in court proceedings related to this Act, or other similar enactments of British Columbia, another province or Canada,

(d) if an enactment of British Columbia, another province or Canada requires the disclosure,
(e) to the person's counsel,
(f) to a law enforcement agency in Canada, or
(g) under an agreement with the government.

(2) The person referred to in subsection (1) is not, except in a proceeding under this Act, compellable to disclose or give evidence about information or records the person has custody of, access to or control over.

The *Motor Dealer Act* defines a motor dealer as:

"motor dealer" means a person who, in the course of business,
(a) engages in the sale, exchange or other disposition of a motor vehicle, whether for that person's own account or for the account of another person, to another person for purposes that are primarily personal, family or household,
(b) holds himself, herself or itself out as engaging in the disposition of motor vehicles under paragraph (a), or
(c) solicits, offers, advertises or promotes with respect to the disposition of motor vehicles under paragraph (a),
but does not include a person exempted by regulation or an individual referred to in paragraph (a) of the definition of "salesperson"

Registration is necessary to carry on the business of a motor dealer in BC. Individual Motor vehicle dealers are also subject to PIPA or PIPEDA depending on whether or not they operate across provinces or internationally, respectively.

Federal

Banks Regulated by the Bank Act *S.C. 1991, c. 46*

General

Banks and authorized foreign banks, within the definitions set out in section 2 of the *Bank Act* are subject to PIPEDA [definition of federal work, undertaking or business, paragraph (g)]. The definition of “bank” in section 2 of the *Bank Act*, in turn, references Schedules I and II which set out, respectively, the Canadian banks and subsidiaries of foreign banks which are subject to the legislation. The authorized foreign banks which are subject to the *Bank Act* are listed in Schedule III. For the purposes of this discussion, all of these entities will simply be referred to as banks.

In addition to the restrictions on the collection, use and disclosure of personal information found in PIPEDA, banks are subject to restrictions on the sharing of customer personal information imposed by the common law and by the *Bank Act*.

Bankers Common Law Duty of Confidentiality- Tournier

In *Tournier v. National Provincial and Union Bank of England* [1924]1K.B. 461 (C.A.) the English Court of Appeal held that a bank owes its customers an implied contractual duty not to disclose customer information to third parties except under certain limited circumstances. This duty applies not just to personal information, but to all customer information. It would therefore apply to the non-personal information of bank customers who are not individuals, but corporate entities, associations, etc. This obligation applies to information including: the identity of a customer, a customer's investments, the nature and value of the investments, the nature and amount of deposits and withdrawals, customer loan information, any information provided by the customer about the customer's financial circumstances, and any relationship with other banks. This obligation of confidentiality has been accepted by Canadian courts as applying to banks subject to Canadian law.[164] The duty continues even after the banker/customer relationship has ceased.

This obligation is subject to the following exceptions:

- If the customer consents, either explicitly or impliedly to the disclosure;
- If there is a legal compulsion to disclose the information;
- If there is a public duty to disclose the information; or
- If the protection of the bank's own interests requires the disclosure.[165]

This duty or obligation of confidentiality, and the exceptions to the duty or obligation tend to mirror the obligations and the exceptions to disclosure that are discussed above in connection with the privacy regime in PIPEDA.

Consent

As with the privacy regimes discussed above, a bank may always seek the consent of the customer to the disclosure of information. This consent could presumably be sought on a case

[164] See for instance, *Guertin et al. v. Royal Bank of Canada et al.*, 1984 CanLII 2079 (ON CA).
[165] *Tournier v. National Provincial and Union Bank of England* [1924] 1 KB 461 (CA) at 473.; for a discussion of the *Tournier* decision in the Canadian context, see Simon Crawford, *Keeping it to Themselves: Bank Privacy Towards 2000* (1998) 29:2 Ottawa Law Review 425.

by case basis, or as part of an overall contract setting out the terms and conditions of the banking relationship.

Legal Compulsion

Legal compulsion may include a court order or warrant. For a discussion of the meaning of "compulsion of law" see, *Keeping it to Themselves* at page 434.[166]

Citing *Haughton v. Haughton*, [1965] 1 O.R. 48 and *Royal Bank of Canada v. Art's Welding & Machine Shop* (1980), (1989) 34 C.P.C. (2d) 190, A.W.L.D. 653, C.L.D. 895, the author states that, "Canada, it is clear that disclosure under compulsion of law includes disclosures made pursuant to court orders and legislation". In *Royal Bank* the Court held that a bank manager could only be compelled to testify by a specific order of the court, and that a subpoena would be insufficient. He also points out that in *Park v. Bank ofMontreal* [1997] B.C.J. No. 787 (B.C.S.C.) (Quicklaw) the Court found that compulsion of law could include compulsion under a foreign law.

This exception may now be subsumed in the exception allowing disclosure without consent found in paragraph 7 (3) (c) of PIPEDA allowing disclosure when it is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records.

It may also be covered by paragraphs 7 (3) (c.1) (ii) and (iii) allowing disclosure without consent to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that:

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

[166] *Ibid.*

Similarly, paragraph 7 (3 (c.2) of PIPPEDA allowing disclosure to the government institution (FINTRAC) mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section would fall under the exception where information is required to be disclosed by law. Paragraph 7 (3) (i) of PIPEDA is also similar.

Public duty

According to Crawford, Canadian courts have recognized a "higher duty" to protect the public interests where there is a danger to the state or to the public".[167]

The disclosure of confidential information has been found to be justified for the purpose of preventing fraud and, has been generously interpreted in at least one case.

In Can*adian Imperial Bank of Commerce v. Sayani,*[168] the issue was whether the bank breached the confidentiality implied by law in respect of information relating to its customer. The bank had disclosed to a mortgage lender which was about to re-finance a housing project for the customer that they had defaulted on a settlement with the bank in respect of their indebtedness to it, and that they then owed the bank money, a fact that was not disclosed in the financial statements supplied to the proposed lender. After a review of the *Tournier* reasons for decision, the Court stated,

> 27. I have concluded that there must be an exception which meets the case of a misrepresentation such as that involved here, whether or not it constitutes fraud or deceit in law.
>
> 28. But for the bank's disclosure of the truth, the trust company would have acted in reliance on financial statements which were materially misleading.

The Court recognized the dilemma that faced the bank at the time of the disclosure. It faced a "double jeopardy" in that divulging information might result in the loss of the financing commitment or possibly been accused of concealing information which could result in the prospective lender making a loan which it might not otherwise make. The Court concluded that, "It would, in my view, be unreasonable for the law to imply a covenant on the part of the bank that it would resolve such a dilemma in such circumstances by remaining silent."

---

[167] *Keeping it to Themselves*, *supra* note 165 at page 438, citing *Jubbal v. Royal Bank of Canada* [1987] BCJ No. 1715.
[168] 1993 CanLII 937 (BCCA).

However, it would appear that this exception may not be available for the purpose of prosecuting a fraud.[169]

Whether this exception would be available to allow for the disclosure of information relating to money laundering will depend on the circumstances. What does seem clear, however, is that the common law duty of confidentiality must now be considered in the context of the restriction imposed by PIPEDA if the information in question is personal information.[170]

Again, this exception, although much narrower, may be akin to those found in paragraphs 7 (3) (d) (i), (d.1) and (d.2) of PIPEDA

- made on the initiative of the organization to a government institution or a part of a government institution and the organization
    - has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed
- made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation
- made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud

While not directly relevant to disclosure relating the investigation of money laundering activities, disclosure under this exception would also be similar to that recognized in paragraph 7 (3) (c.1) (i), which allows disclosure without consent if the disclosure relates to national security, the defence of Canada or the conduct of international affairs. [171]

These exceptions in PIPEDA are no doubt broader than the common law would have recognized.

---

[169] *Sayani, ibid* at para 23.

[170] See *Dr. Robert Grossman v. The Toronto-Dominion Bank*, 2014 ONSC 3578 (CanLII); *Royal Bank of Canada v. Ren*, 2009 ONCA 48 (CanLII); *Royal Bank of Canada v. Trang*, 2014 ONCA 883 (CanLII) overturned on appeal by *Royal Bank of Canada v. Trang*, 2016 SCC 50 (CanLII), [2016] 2 SCR 412. In all of these cases the common law duty of confidentiality was considered in the context of the requirements of PIPEDA.

[171] PIPEDA also recognizes the public interest in disclosure of personal information without consent in paragraphs 7 (3) (d.3), (d.4) and (e) which have not been discussed as they are unlikely to relate to the disclosure of personal information for the purposes of, or in the context of, combating money laundering.

Protection of the Bank's Own Interests

According to Crawford,[172] "the classic example used to illustrate when a bank's interests can override the duty of confidentiality is the case in which the bank discloses the existence and quantum of a customer's overdraft in order to collect repayment." The exception ought to be construed narrowly.[173]

Similar exceptions are found in paragraphs 7 (3) (a) and (b) of PIPEDA:

> (a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;
> (b) for the purpose of collecting a debt owed by the individual to the organization

Summary

The important distinction between the common law duty of confidentiality imposed on banks which restricts the disclosure of customer information and the restrictions imposed by PIPEDA is that PIPEDA only applies to personal information whereas the common law restrictions apply to all customer information, including personal information.

The Bank Act

The *Bank Act* does not itself contain any comprehensive legislated restrictions regarding the disclosure of customer personal information. However, the following sections do provide some guidance by imposing duties on directors which speak to the duty of confidentiality of customer information:

> **Duty to manage**
> 157 (1) Subject to this Act, the directors of a bank shall manage or supervise the management of the business and affairs of the bank.
>
> **Specific duties**
> (2) Without limiting the generality of subsection (1), the directors of a bank shall
> (c) establish procedures to resolve conflicts of interest, including techniques for the identification of potential conflict situations and for restricting the use of confidential information;
> (d) designate a committee of the board of directors to monitor the procedures referred to in paragraph (c);

[172] *Ibid* at page 440 and the following discussion.
[173] *Park v. Bank ofMontreal* [1997] BCJ No. 787 (BCSC) (Quicklaw).

Similarly, the *Bank Act* imposes obligations on a bank to safeguard information in its records and to ensure the accuracy of such information:

> **Protection of records**
> 244 A bank and its agents shall take reasonable precautions to
> (a) prevent loss or destruction of,
> (b) prevent falsification of entries in,
> (c) facilitate detection and correction of inaccuracies in, and
> (d) ensure that unauthorized persons do not have access to or use of information in the registers and records required or authorized by this Act to be prepared and maintained.

Other Federally Regulated Financial Entities

Cooperative Credit Associations Act, SC 1991, c 48

Credit Unions (Caisses Populaires in Québec), which operate much in the same way as banks, are either provincially or federally regulated. Most credit unions in Canada are provincially regulated and restricted to operating in the province in which they are incorporated. In 2012, a framework was put in place to allow provincial credit unions and caisses populaires to continue as federal credit unions and, consequently, operate on a national basis.[174]

As discussed below, the Office of the Superintendent of Financial Institutions (OSFI) has general supervisory authority over federal credit unions.

If a credit union is in fact operating on a national basis and has customers in more than one province, its collection, use and disclosure of personal information will likely be governed by PIPEDA. However, in some cases it may also be subject to the legislation in the province in which its customers reside if that province has private sector legislation, as BC does with its BC PIPA.

In this section, we look at the additional confidentiality requirement s that apply to federally incorporated Credit Unions in addition to those imposed with respect to personal information by either PIPEDA or BC PIPA.

[174] According to the Canada Deposit Insurance Corporation website, there are currently only two federally incorporated Credit Unions - Caisse populaire acadienne ltée and Coast Capital Savings Federal Credit Union.

The federal *Cooperative Credit Associations Act* contains the following provisions relating to the confidentiality of customer information:

> **Confidential information**
> 435 (1) Subject to section 436, all information regarding the business or affairs of an association, or regarding a person dealing with an association, that is obtained by the Superintendent, [OSFI] or by any person acting under the direction of the Superintendent, as a result of the administration or enforcement of any Act of Parliament, and all information prepared from that information, is confidential and shall be treated accordingly.
>
> **Disclosure permitted**
> (2) Nothing in subsection (1) prevents the Superintendent from disclosing any information
>
> (a) to any government agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision,
> (a.1) to any other agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision,
> (a.2) to the Canada Deposit Insurance Corporation for purposes related to its operation, and
> (b) to the Deputy Minister of Finance or any officer of the Department of Finance authorized in writing by the Deputy Minister of Finance or to the Governor of the Bank of Canada or any officer of the Bank of Canada authorized in writing by the Governor of the Bank of Canada, for the purposes of policy analysis related to the regulation of financial institutions,
>
> if the Superintendent is satisfied that the information will be treated as confidential by the agency, body or person to whom it is disclosed.

Trust and Loan Companies Act, SC 1991, c 45

Federally incorporated trust and loan companies are governed by the *Trust and Loan Companies Act*. They may operate throughout Canada and internationally, in accordance with the laws of any foreign jurisdiction [s. 14 (3) (4)]. Accordingly, the disclosure of personal information by these entities will be governed by PIPEDA as they will, in many circumstances, be collecting, using and disclosing personal information on an interprovincial and, perhaps, international basis.

The governing legislation does not deal directly with the disclosure of customer information, either personal information or non-personal information other than in the context of disclosure mandated for supervisory purposes to the Office of the Superintendent of Financial Institutions, discussed below, and to the Financial Consumer agency of Canada.[14]

Both the Office of the Superintendent of Financial Institutions and the Financial Consumer Agency of Canada are subject to the Federal *Privacy Act*.

Office of the Superintendent of Financial Institutions (OSFI)

OSFI is an independent federal government agency that regulates and supervises federally regulated financial institutions (FRFIs). FRFIs include, *inter alia* a bank within the meaning of section 2 of the *Bank Act*, an authorized foreign bank within the meaning of section 2 of the *Bank Act*, a company to which the *Trust and Loan Companies Act* applies and an association to which the *Cooperative Credit Associations Act* applies. In the course of its regulatory activities, OSFI receives some customer information from the entities that it regulates, including customer personal information.

The *Office of the Superintendent of Financial Institutions Act*[175] has the following provision regarding confidentiality:

> **Information is confidential**
> 22 (1) Subject to subsection (3), the following information, and any information prepared from it, is confidential and shall be treated accordingly:
> (a) information regarding the business or affairs of a financial institution, foreign bank, bank holding company or insurance holding company or regarding persons dealing with any of them that is obtained by the Superintendent, or by any person acting under the direction of the Superintendent, as a result of the administration or enforcement of any Act of Parliament;
> (b) information received by any member of the committee established by subsection 18(1), or by any person referred to in subsection 18(5) designated by any member of that committee, in the course of an exchange of information permitted by subsection 18(3); and
> (c) information furnished to the Superintendent pursuant to section 522.27 of the *Bank Act*.
>
> **Disclosure by Superintendent**
> (1.1) Despite subsection (1), subsections 606(1) and 636(1) of the *Bank Act*, subsection 435(1) of the *Cooperative Credit Associations Act*, subsection 672(1) of the *Insurance Companies Act* and subsection 503(1) of the *Trust and Loan Companies Act*, the Superintendent may disclose to the Financial Transactions and Reports Analysis Centre of Canada established by section 41 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* information relating to policies and procedures that financial

[175] RSC 1985, c 18 (3rd Supp), Part I.

institutions adopt to ensure their compliance with Parts 1 and 1.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Disclosure permitted

(2) Nothing in subsection (1) prevents the Superintendent from disclosing any information

(a) to any government agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision,

(a.01) to any other agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision,

(a.1) to the Canada Deposit Insurance Corporation or any compensation association designated by order of the Minister pursuant to subsection 449(1) or 591(1) of the *Insurance Companies Act*, for purposes related to its operation, and

(b) to the Deputy Minister of Finance or any officer of the Department of Finance authorized in writing by the Deputy Minister of Finance or to the Governor of the Bank of Canada or any officer of the Bank of Canada authorized in writing by the Governor of the Bank of Canada, for the purposes of policy analysis related to the regulation of financial institutions,

if the Superintendent is satisfied that the information will be treated as confidential by the agency, body or person to whom it is disclosed.

Regulations

(2.1) The Governor in Council may make regulations prohibiting, limiting or restricting the disclosure by financial institutions, bank holding companies or insurance holding companies of prescribed supervisory information.

Disclosure

(3) The Superintendent shall disclose, at such times and in such manner as the Minister may determine, such information obtained by the Superintendent under the *Bank Act*, the *Cooperative Credit Associations Act*, the *Insurance Companies Act* and the *Trust and Loan Companies Act* as the Minister considers ought to be disclosed for the purposes of the analysis of the financial condition of a financial institution and that

(a) is contained in returns filed pursuant to the Superintendent's financial regulatory reporting requirements; or

(b) has been obtained as a result of an industry-wide or sectoral survey conducted by the Superintendent in relation to an issue or circumstances that could have an impact on the financial condition of financial institutions.

Prior consultation required

(4) The Minister shall consult with the Superintendent before making any determination under subsection (3).

Exceptions to disclosure

(5) Subject to any regulations made under a statute referred to in subsection (3) governing the use by a financial institution of any information supplied to it by its customers, no

information obtained by a financial institution regarding any of its customers shall be disclosed or made available under subsection (3).

Report respecting disclosure
(6) The Superintendent shall prepare a report, to be included in the report referred to in section 40, respecting the disclosure of information by financial institutions, and describing the state of progress made in enhancing the disclosure of information in the financial services industry.

Additionally, OSFI is responsible for other legislation, including the Bank Act (discussed above), the Trust and Loan Companies Act, the Cooperative Credit Associations Act, the Insurance Companies Act, the Pension Benefits Standards Act, 1985, and the Pooled Registered Pension Plans Act. With the exception of the Bank Act, none of these documents contain any mention of privacy or the protection of personal information.

OSFI also requires FRFIs to determine and report whether they are in possession or control of property owned or controlled by or on behalf of persons whose names appear on either the Justice for Victims of Corrupt Foreign Officials Regulations list (JVCFOR) or the Regulations Establishing a List of Entities list (RELE).[176]

OSFI itself is a Government Institution subject to the Federal *Privacy Act.*

Financial Consumer Agency of Canada

The Financial Consumer Agency of Canada was created by the *Financial Consumer Agency of Canada Act*, S.C. 2001, c. 9. The purpose of the Agency is "to ensure that financial institutions, external complaints bodies and payment card network operators are supervised by an agency of the Government of Canada so as to contribute to the protection of consumers of financial products and services and the public, including by strengthening the financial literacy of Canadians." [s. 5]

The Act applies to the Banks, Loan and Trust Companies and Credit Unions discussed above
The following specific confidentiality provisions are found in the legislation:

Confidential information

[176]Office of the Super Intendant of Financial Institutions, "Compliance: Anti-money Laundering, Anti-terrorist Financing and Sanctions" (20 Sept 2019), *Canada.ca*, online: <www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/Pages/default.aspx>.

17 (1) Subject to subsection (2) and except as otherwise provided in this Act, information regarding the business or affairs of a financial institution or external complaints body or regarding persons dealing with one that is obtained by the Commissioner or by any person acting under the Commissioner's direction, in the course of the exercise or performance of powers, duties and functions referred to in subsections 5(1) and (2) and 5.1(2), and any information prepared from that information, is confidential and shall be treated accordingly.

Disclosure permitted

(2) If the Commissioner is satisfied that the information will be treated as confidential by the agency, body or person to whom it is disclosed, subsection (1) does not prevent the Commissioner from disclosing it

(a) to any government agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision;

(b) to any other agency or body that regulates or supervises financial institutions, for purposes related to that regulation or supervision;

(c) to the Canada Deposit Insurance Corporation or any compensation association designated by order of the Minister pursuant to subsection 449(1) or 591(1) of the *Insurance Companies Act*, for purposes related to its operation; and

(d) to the Deputy Minister of Finance or any officer of the Department of Finance authorized in writing by the Deputy Minister of Finance or to the Governor of the Bank of Canada or any officer of the Bank of Canada authorized in writing by the Governor of the Bank of Canada, for the purposes of policy analysis related to the regulation of financial institutions.

Confidential information — payment card network operators

(3) Subject to subsection (4) and except as otherwise provided in this Act, information regarding the business or affairs of a payment card network operator, or regarding persons dealing with one, that is obtained by the Commissioner or by a person acting under the direction of the Commissioner, in the course of the exercise or performance of powers, duties and functions under subsection 5(1.1) or (2.1), and any information prepared from that information, is confidential and shall be treated accordingly.

Disclosure permitted

(4) If the Commissioner is satisfied that the information will be treated as confidential by the person to whom it is disclosed, the Commissioner may disclose it to the Deputy Minister of Finance, or any officer of the Department of Finance authorized in writing by the Deputy Minister of Finance, for the purpose of policy analysis related to the regulation of payment card network operators.

The Agency itself is a Government Institution subject to the Federal *Privacy Act.*

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17 & the Financial Transactions and Reports Analysis Centre of Canada

Introduction

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit. Its mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control.[177]

The focus of this Report is a review of the provisions found in privacy legislation and the legislation governing the entities discussed above that may impact, by hindering or facilitating, the sharing of information, including personal information, for the purposes of combating money laundering.

This Report will not be undertaking a comprehensive review of the provisions of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) or FINTRAC and its ability to collect use or disclose information.

However, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires most of the entities discussed above[178] to report certain transactions to FINTRAC. The entities that are listed on the FINTRAC website are:

- financial entities such as banks (that is, those listed in Schedule I or II of the *Bank Act*) or authorized foreign banks with respect to their operations in Canada, credit unions, caisses populaires, financial services cooperatives, credit union centrals (when they offer financial services to anyone other than a member entity of the credit union central), trust companies, loan companies and agents of the Crown that accept deposit liabilities);
- life insurance companies, brokers and agents;
- securities dealers;
- money services businesses;
- agents of the Crown that sell money orders;
- accountants and accounting firms (when carrying out certain activities on behalf of their clients);

[177] Financial Transactions and Reports Analysis Centre of Canada, "About FINTRAC" (25 September 2020) , *Canada.ca*, online: <https://www.fintrac-canafe.gc.ca/>.
[178] Lawyers were initially included as reporting entities but are no longer.

- real estate brokers, sales representatives and developers (when carrying out certain activities);
- casinos;
- dealers in precious metals and stones;
- public notaries and notary corporations of British Columbia (when carrying out certain activities on behalf of their clients); and
- for the purposes of suspicious transactions, employees of these reporting entities.[179]

These Reporting entities must report the following transactions:

- Suspicious transactions
- Electronic funds transfers
- Large cash transactions
- Terrorist property
- Casino disbursements
- Alternative to large cash transaction reports[180]

In addition, FINTRAC may receive voluntary information from any person or entity who believes they have information about suspicions of money laundering, he financing of terrorist activities or suspicions of non-compliance with the PCMLTFA. The FINTRAC website has a web form for this purpose.[181]

Interaction Between the PCMLTFA and Privacy legislation

FIPPA

Section 33 (1) (c) of the FIPPA allows for disclosure of personal information in accordance with an enactment of British Columbia, other than this Act, or Canada that authorizes or requires its disclosure. The BC Access to Information and Privacy Commissioner has found, in the context of s. 22 (3) (b)[182] of FIPPA that the PCMLTFA is a "law".

> The *Proceeds of Crime Act* is a federal statute that provides for penalties for the violation of that Act and, in my view, it is a "law" under s. 22(3)(b). The purpose of the *Proceeds of Crime Act* is "to facilitate combatting the laundering of proceeds of crime and combatting the financing of terrorist activities, …" This includes

[179] Financial Transactions and Reports Analysis Centre of Canada, "Who must report" (16 August 2020), *Canada.ca*, online: <www.fintrac-canafe.gc.ca/reporting-declaration/info/re-ed-eng>.
[180] For a detailed discussion of these types of transactions, see the Financial Transactions and Reports Analysis Centre of Canada, "Financial transactions that must be reported" (16 August 2020), *Canada.ca*, online: < https://www.fintrac-canafe.gc.ca/reporting-declaration/rpt-eng>.
[181] Financial Transactions and Reports Analysis Centre of Canada, "FINTRAC – Voluntary information reporting", *Canada,ca*, online: < https://www15.fintrac-canafe.gc.ca/vir-drtv/>.
[182] Dealing with instances in which disclosure is deemed to be harmful to personal privacy.

> the requirement to report "suspicious financial transactions and … cross-border movements of currency and monetary instruments." The *Proceeds of Crime Act* also establishes FINTRAC and tasks it with ensuring compliance with the Act. It also provides for the designation of violations and penalties. I am, therefore, satisfied that any LCTRs, STRs and UFT reports about the gaming activities of the third party, if they exist, would contain personal information that was compiled and is identifiable as part of an investigation into a possible violation of law.[183]

While the term used in section 22 (3) (b) is "law" and the term used in section 33 (1) (c) is "enactment", there can be little doubt that the PCMLTFA is both a "law" and an "enactment".[184]

As discussed above, section 33.2 (a) of FIPPA allows a public body to disclose personal information inside Canada "for the purpose for which it was obtained or compiled or for a use consistent with that purpose". Information collected by a public body which has an obligation to report to FINTRAC, such as the BC Lottery Corporation, for the purpose of fulfilling that obligation could also be disclosed pursuant to this provision.

In addition, it may be that a voluntary disclosure could be made to FINTRAC pursuant to section 33 (2) (i) which permits disclosure to,

> (i) to a public body or a law enforcement agency in Canada to assist in a specific investigation
> (i) undertaken with a view to a law enforcement proceeding, or
> (ii) from which a law enforcement proceeding is likely to result;

Recall that the definitions of "law enforcement" and "prosecution" may be broad enough to include FINTRAC:

> "law enforcement" means
> (a) policing, including criminal intelligence operations,
> (b) investigations that lead or could lead to a penalty or sanction being imposed, or
> (d) proceedings that lead or could lead to a penalty or sanction being imposed
> "prosecution" means the prosecution of an offence under an enactment of British Columbia or Canada[185]

[183] *British Columbia Lottery Corporation (Re),* 2019 BCIPC 32 (CanLII).
[184] See the discussion above regarding s. 18(o) of BC PIPA.
[185] Again, reference should be had to the comments of the BC Access and Privacy commissioner in the BC Lottery case, *supra* note 183.

BC PIPA

Section 18 (o) of BC PIPA allows for disclosure that is "required by law". The PCMLTFA would be a law for the purposes of this provision. Personal information collected by an organization that is subject to BC PIPA and to the reporting requirements of the PCMLTFA would be permitted, indeed required, to disclose the required information that it has collected from its customers.

Personal information may also be disclosed without consent in accordance with section 18 (1) (c) where "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding and the disclosure is reasonable for purposes related to an investigation or a proceeding." While it is not completely clear, the BC Lottery case cited above[186] suggests that a voluntary disclosure of information relating to potential money laundering could be disclosed to FINTRAC pursuant to this provision.

In addition, consent is a fundamental principle of BC PIPA and personal information may only be collected, used or disclosed with the consent of the individual [s.6 (1)] and the collection must be "reasonable" in the circumstances. [s. 4 (1)]. Organizations subject to BC PIPEDA must provide access to policies that explain what information is being collected and how it will be used and disclosed [s. 5]. Organizations subject to BC PIPA should have in place privacy policies that explain to customers what information they are collecting for the purposes of PCMLTFA compliance and that it will be disclosed to FINTRAC as required by that legislation.

Federal Privacy Act

FINTRAC itself is subject to the federal *Privacy* Act. There are no Institutions subject to the federal *Privacy Act* that have an obligation to report to FINTRAC. However, travellers crossing the border must declare any currency or monetary instruments they have which are valued at Can$10,000 or more. This amount includes Canadian or foreign currency or a combination of both. Monetary instruments include, but are not limited to, stocks, bonds, bank drafts, cheques and traveller's cheques. This report is to be made to the Canadian Border Service Agency (CBSA) [s12 of the PCMLTFA]. The CBSA is also subject to the federal *Privacy Act*.

[186] *Ibid*.

The CBSA in turn provides these reports to FINTRAC [ss (5)]. This information would be collected by both institutions in accordance with section 4 of the *Privacy Act*, which provides that, "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution." Section 7 provides a similar authority for the use of the information. Disclosure by CBSA to FINTRAC is consistent with subsections 8 (2) (a) and (b) wish provide for disclosure without consent.

> (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
>
> (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
>
> (b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

Personal information may also be disclosed to federal investigative bodies pursuant to section 8 (2) (e) or to provincial or international organisations if the requirements of section 8 (2) (e) are met.

FINTRAC also has restrictions on its use and disclosure of the reporting information that it collects, including personal information, as set out in sections 36 and 37.

Sections 55 – 61 provide the basis for disclosure of personal information as contemplated by s. 8 92) (b) of the Privacy Act - for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure.

Sections 56 and 56.1 permit FINTRAC to enter into agreements with foreign states or foreign or international institutions, for the general sharing of information and for the sharing of specific investigative information if the foreign or international institution has powers and duties similar to those of FINTRAC.

In order to facilitate disclosure FINTRAC has entered into a number of information sharing Memoranda of Understanding (MOU) with both foreign and domestic entities. According to its website[187], FINTRAC has a number of such MOU's with foreign Financial Intelligence Units,

[187] Abour FINTRAC, *supra* note 178.

with federal investigative agencies, other federal regulators such as OSFI and the Competition Bureau, provincial regulators such as the BC Securities Commission, the Real Estate Council of BC, the BC Gaming Policy and Enforcement Branch and BCFSA, and with IIROC, an industry organization.

In 2009 the Privacy Commissioner conducted an audit of FINTRAC which reviewed some 47 such MOU's.[188] While that audit is now out of date, it does provide a helpful overview of FINTRAC's information handling practices and its Privacy Act obligations.

PIPEDA

PIPEDA specifically includes a provision addressing the mandatory reporting requirements to FINTRAC pursuant to the PCMLTA. Disclosure without consent for this purpose is addressed in section 7 (3) (c.2):

> 7 (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> (c.2) made to the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* as required by that section

Subsection 7 (3) (i) which permits disclosure without consent where the disclosure is required by law would also be applicable.

A voluntary disclosure to FINTRAC could be made pursuant to section 7 (3) (d) which permits a disclosure without consent that is,

> (d) made on the initiative of the organization to a government institution or a part of a government institution and the organization
>
> (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
>
> (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

[188] Office of the Privacy Commissioner of Canada, *Financial Transactions and Reports Analysis Centre of Canada: Final Report* (Ottawa: OPCC, 2009) [OPCC 2009].

Interaction between the PCMLTFA & Sectoral Legislation

In reviewing the sectoral legislative regimes Discussed above, I did not note any impediments to the mandatory sharing of information, including personal information, with FINTRAC. Generally, such legislation provides very little guidance with respect to the sharing of information with FINTRAC by way of a voluntary disclosure. For personal information, the focus of this report, voluntary reporting may be permissible under applicable privacy legislation, but it is not always clear to what extent non personal information relating combating money laundering can be voluntarily provided to FINTRAC without violating sector specific legislation.

For that reason "safe harbour" and third agency rule provisions, as discussed in the next section, may provide more clarity.

Conclusions

While there may be an assumption among some that privacy laws in Canada act to deter the disclosure of personal information related to combatting money laundering, it is my view that, properly understood, they do not prohibit such activity. These laws have specific provisions outlining how such disclosures can be done lawfully while respecting individuals' personal privacy, thus providing a guide and assurance for would-be information sharers and users alike. However, as noted the privacy legislation in British Columbia and at the federal level leaves the sharing of personal information to the discretion of the public body or private organization involved unless there is a legal requirement to provide it. There is no incentive to disclose personal information and the existence of penalties for improper disclosure, such as adverse findings/publicity by a privacy commissioner and, in some cases the prospect of civil liability, likely act as a disincentive. For that reason, organizations such as the Canadian Bankers' Association (CBA)[189] have recommended to the government that a "safe harbour" provision be included in the PCMLTFA.

The term "safe harbour" in this context refers to a provision in a statute or in a regulation or rule that specifies that certain conduct will not create liability if certain conditions are met.[190]

[189] Canadian Bankers Association, "Strengthening Canada's anti-money laundering regime" (3 February 2020), *CBA Briefings*, online: <https://www.briefings.cba.ca/strengthening-canadas-anti-money-laundering-regime>.
[190] See https://www.winston.com/en/legal-glossary/safe-harbor.html.

Generally, such a provision would exempt the entity that has shared the information from liability or censure by a regulator if it acted in good faith in doing so. The CBA, for instance, has made the recommendation as follows:

> Critical to any information sharing regime, however, is the inclusion of a safe harbour provision in the PCMLTFA. Such a provision could be similar to what is included in relevant legislation in the United States, which provides statutory protection from liability and regulatory enforcement, or fines as it relates to the sharing of information, in good faith. Without such protections, organizations would be much less inclined to share information.[191]

A similar recommendation to allow for, and encourage, more robust sharing of information, including personal information, "between federally regulated financial institutions such as banks and trust companies, provided that FINTRAC is notified upon each occurrence of such sharing." Has been made by the Standing Committee on Finance.[192] In its response to the report, the government has indicated that it will study the matter.[193]

Not only might such a "safe harbour" provision in the PCMLTFA facilitate voluntary sharing of information with FINTRAC, but similar provisions in privacy legislation and sectoral legislation might be considered. The provisions would have to be tightly worded with a focus on information that might be relevant to combatting money laundering. They could address not only sharing with government agencies such as law enforcement agencies and FINTRAC, but might also address the sharing of information with private sector entities, as long as the focus was limited.

For instance, section 7 (3) (d), (d.1) and (d.2) of PIPEDA currently contemplate the sharing of information, without the consent of the individual, relating to possible violations of the law.

> (d) made on the initiative of the organization to a government institution or a part of a government institution and the organization
>
> (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
>
> (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

---

[191] OPCC 2009, *supra*, note 189.
[192] Canada, Parliament, House of Commons, Standing Committee on Finance, *Confronting Money Laundring and Terrorist Financing: Moving Canada Forward*, 42nd Parl, 1st Sess, No 24 (November 2018).
[193] https://www.ourcommons.ca/content/Committee/421/FINA/GovResponse/RP10326634/421_FINA_Rpt24_GR/421_FINA_Rpt24_GR_PDF-e.PDF

(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

(d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud

However, the onus is on the organization to determine if the disclosure is warranted, and there is always a risk that the Privacy Commissioner or the Federal Court might disagree.

For an example of a provision that offers protection to an organization making a disclosure in good faith, see 3 (A) of 31 US Code (Money & Finance) §5318:

(3) LIABILITY FOR DISCLOSURES.—
(A) In general.—
Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority, and any director, officer, employee, or agent of such institution who makes, or requires another to make any such disclosure, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.

In the context of information sharing, particularly the sharing of personal information and confidential information such as financial and banking information, such "safe harbour" provisions should also require that the information only be used for the purpose for which it was disclosed and not disclosed further (known as a third agency rule). For a discussion of information sharing among private sector entities for the purpose of combatting money laundering and the use of "safe harbour" provisions, including limited immunity from liability and provisions to ensure the security and confidentiality of shared information, see the Guidance

document from the Financial Action Task Force[194] entitled private Sector Information Sharing.[195]

Appendix A

Public Bodies listed in Schedule 2 of the BC FIPPA most likely to have information related to money laundering

BC Financial Services Authority
British Columbia Assessment Authority
British Columbia Lottery Corporation
British Columbia Securities Commission
Motor Dealer Council, now known as the Motor Vehicle Sales Authority of BC
Office of the Superintendent of Real Estate
Organized Crime Agency of B.C.
PRIMECORP Police
Records Information Management Environment Incorporated

[194] The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.
[195] Financial Action Task Force, *FATF Guidance: Private Sector Information Sharing* (Paris: FATF, 2017).

Appendix B

Governing Bodies listed in Schedule 3 of the BC FIPPA most likely to have information related to money laundering

Insurance Council of British Columbia
Law Society of British Columbia
Organization of Chartered Professional Accountants of British Columbia
Real Estate Council of British Columbia
Society of Notaries Public of British Columbia

Appendix C
List of investigative bodies specified in the Privacy Regulations, SOR/83-508, Schedule II

1 [Repealed, SOR/2018-39, s. 3]
1.1 [Repealed, SOR/2010-146, s. 4]
2 Boards of Inquiry, Department of National Defence
3 Office of Controlled Substances, Healthy Environments and Consumer Safety Branch, Department of Health
4 [Revoked, SOR/85-965, s. 1]
5 [Repealed, SOR/2013-115, s. 2]
6 Canadian Forces Military Police
6.01 Canadian Forces National Counter-Intelligence Unit
6.1 Canadian Security Intelligence Service
6.2 Canadian Transportation Accident Investigation and Safety Board
7 [Repealed, SOR/2013-115, s. 3]
8 Clemency and Record Suspension Division, Parole Board of Canada
8.1 Collections Directorate, Collections and Verification Branch, Canada Revenue Agency
8.2 Conservation and Protection Directorate, Department of Fisheries and Oceans
8.3 Criminal Investigations Directorate, International, Large Business and Investigations Branch, Canada Revenue Agency
9 Integrity Operations Directorate, Integrity Services Branch, Department of Employment and Social Development
9.1 [Repealed, SOR/2013-115, s. 4]
9.2 [Repealed, SOR/2013-115, s. 4]
9.3 Inland Enforcement Division, Canada Border Services Agency
10 Intelligence and Targeting Operations Directorate, Canada Border Services Agency
10.1 International and Large Business Directorate, International, Large Business and Investigations Branch, Canada Revenue Agency
10.2 Investigations Division, Office of the Commissioner of Canada Elections
10.3 Law Enforcement Branch, Parks Canada Agency
10.4 Non-Filer Programs Division, Debt Management Compliance Directorate, Collections and Verification Branch, Canada Revenue Agency
11 Personnel Security Service, Department of Foreign Affairs, Trade and Development
12 Preventive Security and Intelligence Branch, Correctional Service of Canada
12.1 Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch, Canada Revenue Agency
13 Royal Canadian Mounted Police
13.1 Security Intelligence Review Committee
14 Security and Investigative Services, Canada Post Corporation
15 Security Bureau, Passport Canada, Department of Foreign Affairs and International Trade
15.1 Criminal Investigations Division, Canada Border Services Agency

16 Scientific Research and Experimental Development Directorate, Domestic Compliance Programs Branch, Canada Revenue Agency
17 Small and Medium Enterprises Directorate, Domestic Compliance Programs Branch, Canada Revenue Agency
18 Trust Accounts Programs Division, Debt Management Compliance Directorate, Collections and Verification Branch, Canada Revenue Agency

Appendix D

List of the entities to which the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* applies

(a) authorized foreign banks within the meaning of section 2 of the *Bank Act* in respect of their business in Canada, or banks to which that Act applies;

(b) cooperative credit societies, savings and credit unions and caisses populaires regulated by a provincial Act and associations regulated by the *Cooperative Credit Associations Act*;

(c) life companies or foreign life companies to which the *Insurance Companies Act* applies or life insurance companies regulated by a provincial Act;

(d) companies to which the *Trust and Loan Companies Act* applies;

(e) trust companies regulated by a provincial Act;

(f) loan companies regulated by a provincial Act;

(g) persons and entities authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity;

(h) persons and entities that have a place of business in Canada and that are engaged in the business of providing at least one of the following services:

(i) foreign exchange dealing,
(ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
(iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
(iv) dealing in virtual currencies, or
(v) any prescribed service;

(h.1) persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

(i) foreign exchange dealing,
(ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
(iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
(iv) dealing in virtual currencies, or
(v) any prescribed service;

(i) persons and entities engaged in a prescribed business, profession or activity;
(j) persons and entities engaged in a prescribed business or profession, while carrying out a prescribed activity;

(k) the government of a province that, in accordance with paragraph 207(1)(a) of the *Criminal Code*,

(i) in a permanent establishment that is held out to be a casino, conducts and manages a lottery scheme that includes games of roulette or card games, or
(ii) in any other permanent establishment, conducts and manages games that are operated on or through a *slot machine*, as defined in subsection 207(4.01) of the *Criminal Code*, or any other similar electronic gaming device, if there are more than 50 of those machines or other devices in the establishment;

(k.1) the government of a province that, in accordance with paragraph 207(1)(a) of the *Criminal Code*, conducts and manages a lottery scheme, other than bingo or the sale of lottery tickets, that is accessible to the public through the Internet or other digital network, except if the network is an internal network within an establishment described in subparagraph (k)(ii);

(k.2) an organization that, in accordance with paragraph 207(1)(b) of the *Criminal Code*, in a permanent establishment that is held out to be a casino, conducts and manages a lottery scheme that includes games of roulette or card games, unless the organization is a registered charity, as defined in subsection 248(1) of the *Income Tax Act*, and the lottery scheme is conducted or managed for a period of not more than two consecutive days at a time;

(k.3) the board of a fair or of an exhibition, or the operator of a concession leased by such a board, that, in accordance with paragraph 207(1)(c) of the *Criminal Code*, in a permanent establishment that is held out to be a casino, conducts and manages a lottery scheme that includes games of roulette or card games;

(l) departments and agents or mandataries of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities, that issue or sell money orders to, or redeem them from, the public or that sell prescribed precious metals, while carrying out a prescribed activity; and

(m) for the purposes of section 7, employees of a person or entity referred to in any of paragraphs (a) to (l).