Canadian and Japanese laws concerning the protection of privacy and personal information in the private sector – a comparative study

Tamotsu Nomura

Faculty of Law, McGill University, Montreal

June 2020

A thesis submitted to McGill University

in partial fulfillment of the requirements of the degree of Master of Laws (LLM)

Table of Contents

Abstract

With the progression and spread of information technologies, personal information is being used innovatively to increase individual, social, and economic benefit. At the same time, the risk of invasion of privacy has also grown higher. Currently, at international governmental meetings, many countries insist on the importance of comparing legal systems protecting privacy for the development of international economic society. This thesis aims to identify similarities and differences in Canadian and Japanese laws concerning the protection of privacy and personal information in the private sector. It also intends to shed light on the reasons for these similarities and differences, through investigation of the legislative history, judicial precedents and records in legislative procedure.

First, this thesis considers the origin and development of the "right of privacy" and personal information protection. It identifies the privacy protected by tort law, constitutional law and data law and defines the meaning of the right of privacy. Second, the thesis will inquire into the process of developing privacy and personal information protection in Canada and Japan. This thesis suggests that the process of developing privacy and personal information protection in both Canada and Japan is divided into five periods. Finally, the thesis will engage in an in-depth comparison of the personal information protection laws between Canada and Japan, *the Personal Information Protection and Electronic Documents Act* (*PIPEDA*) of Canada and *the Act on the Protection of Personal Information* (*APPI*) of Japan. The comparison will focus on three criteria: 1) what are the laws concerning personal information protection supposed to protect, 2) how do the laws protect personal information, and 3) what mechanisms guarantee the actual enforcement of the laws. A few of the most striking differences identified are the way in which the respective legislation deals with anonymously processed information, the consent principle, the opt-out procedure, and the settlement of complaints by accredited personal information protection organizations. Various reasons for these differences are suggested, and include the economic structure, intention of government, and legal framework in each country.

Résumé

Avec la progression et la diffusion des technologies de l'information, les informations personnelles sont utilisées de manière innovante pour accroître les avantages individuels, sociaux et économiques. En même temps, le risque d'atteinte à la vie privée a également augmenté. Actuellement, lors de réunions gouvernementales internationales, de nombreux pays insistent sur l'importance de comparer les systèmes juridiques de protection de la vie privée pour le développement de la société économique internationale. Cette thèse vise à identifier les similitudes et les différences dans les lois canadiennes et japonaises concernant la protection de la vie privée et des renseignements personnels dans le secteur privé. Elle vise également à faire la lumière sur les raisons de ces similitudes et différences, par le biais d'une enquête sur l'historique législatif, les précédents judiciaires et les archives de la procédure législative.

Premièrement, cette thèse considère l'origine et le développement du « droit à la vie privée » et la protection des informations personnelles. Elle identifie les aspects de la vie privée protégée par le droit des biens, le droit de la responsabilité, le droit constitutionnel et le droit des données, et définit le sens du droit à la vie privée. Deuxièmement, la thèse examinera le processus de développement de la protection de la vie privée et des informations personnelles au Canada et au Japon. Cette thèse suggère que le processus de développement de la protection de la vie privée et des informations personnelles au Canada et au Japon est divisé en cinq périodes. Finalement, la thèse proposera une comparaison approfondie des lois sur la protection des informations personnelles entre le Canada et le Japon, la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada et la *Loi sur la protection des informations personnelles* du Japon. La comparaison se concentrera sur trois critères: 1) Qu'est-ce que les lois (concernant la protection des informations personnelles) sont censées protéger? 2) Comment les lois protègent-elles les informations personnelles? et 3) Quels mécanismes garantissent l'application effective des lois. Quelques-unes des différences identifiées les plus frappantes sont la manière dont la législation respective traite les informations traitées de manière anonyme, le principe du consentement, la procédure de désabonnement et le règlement des plaintes par des organisations de protection des informations personnelles accréditées. Diverses raisons expliquant ces différences sont suggérées, notamment la structure économique, l'intention du gouvernement et le cadre juridique de chaque pays.

Acknowledgements

This thesis could not have been completed without the support of many people.

I would first like to describe my sincere gratitude and appreciation to Dr. Helge Dedek. He has been a very perseverant and generous supervisor to me, and his guidance has been invaluable.

I thank the capable researchers of JIPDEC for sharing their precious documents with me and delivering them from Japan.

I was very blessed with wonderful friends. The time I spent with them was irreplaceable to me.

I am grateful for the assistance of Rachelle Saint-Cyr and Richard Platt in reviewing the French abstract. Lucas Alcolea gave me helpful and useful advice, and Sarah Stewart not only reviewed and refined this thesis but also encouraged me.

Ultimately, I appreciate my family – my father, mother, brother and sister – for their love and support.

1 Introduction

1.1 Overview

This master's thesis aims to identify similarities and differences between Canadian and Japanese legislation concerning protection of privacy and personal information in the private sector, based on examination of earlier studies and comparison of the laws and regulations themselves. It also intends to highlight the process by which these similarities and differences arose and assess their potential effects, through investigation of the development of laws protecting privacy and personal information and records in legislative procedure. This thesis can contribute to laying the groundwork upon which future developments of international standards for the protection of privacy can be built.

1.2 Rationale

"Personal data is the new oil of the Internet and the new currency of the digital world."[1] Published in *Personal Data: The Emergence of a New Asset Class*, a report by the World Economic Forum (WEF),[2] this statement reflects the immense value that is now being placed on personal information in the modern age.[3] With the progression and spread of information technologies such as smartphones and social networking services, personal information is being used innovatively to increase individual, social, and economic benefit and public security. At the same time, the risk of invasion of privacy and discrimination is also rising.[4] In order to deal with these concerns, many countries have introduced legislations and restrictions to protect personal information. However,

---

[1] Meglena Kuneva, *Roundtable on Online Data Collection, Targeting and Profiling* (Brussels, 2009).

[2] WEF, *Personal Data: The Emergence of a New Asset Class* (World Economic Forum, 2011) at 5.

[3] See, Samson Y Esayas, "Privacy-as-a-quality parameter of competition" in Björn Lundqvist & Michal S Gal, eds, *Competition Law for the Digital Economy* (Cheltenham, UK: Edward Elgar Publishing, 2019) 126 at 128; Christine Storr & Pam Storr, "Internet of Things: Right to Data from a European Perspective" in Marcelo Corrales, Mark Fenwick & Nikolaus Forgó, eds, *New Technology, Big Data and the Law* (Singapore: Springer, 2017) 65 at 67.

[4] See, OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(2013)79 (2013) at 4.

disparities between different countries' laws and regulations can introduce complexity for international companies, and can hinder the free transborder flow of information.

Many countries have come together to attempt to address these problems at international meetings of the WEF and the Organisation for Economic Co-operation and Development (OECD). These international organizations recommend comparison of privacy and personal information protection laws between countries in order to develop international rules appropriate for the digital economic age.[5] Comparison of the legal systems protecting privacy and seeking international development and harmonization of the systems will have both social and economic significance, through enhancement of protection of privacy and individual liberties, and support of economic advancement through easing barriers to free flow of information between countries.

Interest in comparing Canadian and Japanese personal information protection laws has arisen in part as the two countries' economic spheres overlap. Recently, an increasing number of Japanese companies are taking part in the Canadian market,[6] and many of these companies are planning to expand their businesses and hire more local employees.[7] Canadian companies are also investing in Japan, and over 100 Canadian companies have a permanent Japanese presence.[8] In many of these cases, Canadian and Japanese companies already make use of personal information in each other's countries. Furthermore, these companies anticipate that information and

---

[5] See *Ibid* at paras 21, 22.

[6] The number of Japanese companies in Canada is increasing; 748 (2013), 768 (2014), 800 (2015), 803 (2016) and 811 (2017). See, Ministry of Foreign Affairs of Japan, *Kaigai zairyu hojinsu chosa tokei (Heisei 30 nen yoyaku ban)* [Annual Report of Statistics on Japanese Nationals Overseas (Summary of 2017)] (2017) at 58.

[7] See JETRO, "FY2018 JETRO Survey on Business Conditions for Japanese Companies in Canada (29th annual survey)", (18 March 2019), online: *JETRO - Japan External Trade Organization* <www.jetro.go.jp/en/news/releases/2019/e182395e4fbd1d5b.html>.

[8] See Government of Canada (Global Affairs Canada), "Canada-Japan Relations", (April 2019), online: *Embassy of Canada to Japan* <www.canadainternational.gc.ca/japan-japon/bilateral_relations_bilaterales/index.aspx?lang=eng>.

communication technologies will provide significant opportunities for investment and growth in the coming years, which will likely intensify their use of personal data.[9]

Currently, the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) System is used to freely transfer personal information with appropriate security between participating countries, which include Canada and Japan.[10] However, even if a company is certified, it must still comply with the other country's domestic law. The scope of APEC CBPR is limited to the transfer of personal information, and companies may be subject to additional laws and regulations varying by economy.[11] Moreover, even if Canadian or Japanese companies do not need to transfer data of individuals, in some cases they may still use personal information in each other's countries. Thus, these companies would still need to know each other's privacy and personal information protection laws. Many companies find that researching information about regulations and local systems and business practices is a challenging aspect of engaging in overseas business.[12] Thus if the differences between Canadian and Japanese privacy and personal information protection laws in the private sector were easily and clearly laid out and understood, Canadian and Japanese companies could reduce the risk of legal issues, and could also expand their businesses more efficiently.

Comparing Canadian and Japanese privacy and personal information laws can also contribute to further development of both countries' legal systems in this field. When the *Act on the Protection of Personal Information* (*APPI*)[13] was revised, the Japanese government researched

---

[9] See JETRO, *supra* note 7; Government of Canada (Global Affairs Canada), *supra* note 8.

[10] See TrustArc, "APEC CBPR and APEC PRP Privacy Certifications", (12 June 2019), online: *TrustArc* <www.trustarc.com/products/apec-certification/>.

[11] See APEC, "Business | Cross Border Privacy Rules System", (12 June 2019), online: *Cross Border Privacy Rules System* <cbprs.org/business/>.

[12] 42.5% of Japanese companies consider that researching 'Information about local systems (Tariffs, regulations/permits and licenses etc.)' is challenge for overseas business. JETRO, *FY2018 Survey on the International Operations of Japanese Firms - JETRO Overseas Business Survey* (2019) at 9.

[13] *Kojin joho no hogo ni kansuru horitsu* [Act on the Protection of Personal Information], Amendment of Act No. 65 of 2015.

and compared some aspects of the privacy and personal information protection laws and agreements of international organizations and countries including Canada.[14] These surveys affected the amendment of the *APPI*. Currently, the Office of the Privacy Commissioner of Canada (OPC) is preparing guidance on de-identification, and *APPI*'s provisions related to anonymously processed information could positively contribute to the guidance. The comparison between Canadian and Japanese laws in this thesis may be beneficial to Canada and Japan individually as well as cooperatively. It will hopefully prove useful to government experts, academics, businesses, and the information technology community to facilitate economic relations between the two countries, and to contribute to the future development of privacy and personal information protection rules.

1.3 Objective and Outline

The principal objective of this thesis is the comparison of Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[15]and Japan's *APPI*. *PIPEDA* applies to the handling of personal information in the private sector. However, Alberta, British Columbia and Quebec have their own general private-sector laws related to personal information protection. *PIPEDA* does not apply to organizations that operate entirely within these three provinces in cases where personal information does not cross provincial or national borders[16] because the laws in these three provinces have been deemed substantially similar to *PIPEDA*.[17] Since any personal information that crosses provincial borders must be subject to *PIPEDA*, both Canadian and

---

[14] See e.g. Study Group on Personal Data, *Dai 7 kai pasonaru deta ni kansuru kentokai shiryo 1-2 (betten)* [Document 1-2 (Appendix) of 7th Meeting of Study Group on Personal Data] (2014).

[15] SC 2000, c 5 [*PIPEDA*].

[16] See Office of the Privacy Commissioner, "Summary of privacy laws in Canada", (January 2018), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>.

[17] See Adam Kardash & Patricia Kosseim, "Canada" in *The international comparative legal guide to Data Protection 2018*, 5th ed (London: Global legal group, 2018) at 54.

international companies will in such cases be required to comply with the federal act even if operating in the three provinces which have their own laws. Furthermore, since the provincial laws in any case must not deviate significantly from *PIPEDA*, the federal act is the most appropriate reference point for consideration of Canadian privacy and personal information protection. This thesis will therefore focus predominantly on the federal statute.

While there have been some earlier studies[18] related to the topic of this thesis, they are outdated and insufficient for the current times. Previous research studies have discussed *PIPEDA* and *APPI*[19]; however, the *APPI* was revised in 2015. The revision includes some important additions such as the idea of anonymously processed information, where personal information has been processed so as not to identify a specific individual. No studies have yet compared the Canadian law with the revised Japanese Act.

To compare laws concerning privacy and personal information, we first need to explore the right of privacy and personal information protection. In Section 2, the development of the right of privacy is described in tort law and constitutional law in Canada.

In Section 3, this thesis outlines how the right of privacy was introduced into Canadian and Japanese laws. The processes of developing personal information protection in Canada and Japan are compared and differences and rationale for these differences are recognized.

In Section 4, laws concerning personal information protection for the private sector in Canada and Japan are compared following an overview of the legal systems concerning personal information. In this section, three points are compared. The first point is what the laws concerning

---

[18] See e.g.Nobuyuki Sato & Consumer Affairs Agency, *Shogaikokuto ni okeru kojin joho hogo seido no jittai chosa ni kansuru kento iinkai hokokusho* [Report of Study Committee on Actual Conditions Survey concerning Personal Information Protection Legal System in Other Countries] (2008); Rihoko Kawai & Consumer Affairs Agency, *Shogaikokuto ni okeru kojin joho hogo seido no kantoku kikan ni kansuru kento iinkai hokokusho* [Report of Study Committee on Supervisory Authority concerning Personal Information Protection Legal System in Other Countries] (2011); Takeru Ehara, *Puraibashī ken no sōgōteki kenkyū* [Comprehensive Research on Privacy Rights] (Kyoto: Horitsu Bunkasha, 1991).

[19] *Kojin joho no hogo ni kansuru horitsu* [Act on the Protection of Personal Information], Act No. 57 of 2003.

privacy and personal information are intended to protect. The second point is how the laws protect personal information, in other words, what are the duties of organizations handling personal information. The third point is how enforcement of the laws is secured, through methods such as settlement of complaints, orders from supervisory authorities, and penalties. The differences between the Canadian and Japanese laws with respect to these three points are examined, and the rationale for these differences is discussed.

2 The Right of Privacy in Canada and Japan

2.1 Complexity of Privacy

The purpose of this thesis is to help better understand and facilitate better practice of the protection of privacy and personal information. What is privacy? What is personal information? These two concepts are difficult to define, and many different views exist as to how they should be understood and handled. Both Canadian and Japanese laws define personal information as information about an identifiable individual.[20] On the other hand, neither Canadian nor Japanese laws define privacy, and even Canada's *Privacy Act*[21] does not specifically include a definition of privacy. Furthermore, the idea of privacy is complex and multi-faceted.

Beyond legal definition, there are various meanings of privacy in daily life. Some people may consider privacy as the secret information which an individual does not want to disclose to other people. However, each individual has different information that they would like to keep secret. Some for example do not hesitate to share their age, while others would not want it made known. Even if information is not hidden, there are some who insist that it is their right to keep such information private. The majority of people do not hide their faces, and the feature of an opened

---

[20] More extensive outlines of the definition of this term have also been discussed and stipulated. See House of Commons, *Towards Privacy by Design : Review of the Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics (2018), [ETHI Twelfth Report]; Hisamichi Okamura, *Kojin jōhō hogoho* [Act on the Protection of Personal Information], 3d ed (Tokyo: Shojihoumu, 2017).

[21] RSC 1985, c P-21.

face is used for identification and authentication. Some personal possessions such as a car and home can also readily be seen, at least from the exterior, by the general public; therefore, these things are not secret. However, if another person were to record or take pictures of a person without their consent, many would feel that their privacy had been violated. As another example, if a woman is told by her parents, "You should get married and have a baby soon," and she thinks that marriage and pregnancy are private matters in which she has freedom to make her own decisions, she may think that the advice of her parents is privacy invasion.

The meaning of privacy is changing with the flow of time. Evidence of this change appears in the Oxford English Dictionary. The explanation of privacy in the first edition of the dictionary is "Privacy... The state or quality of being private. 1. The state or condition of being withdrawn from the society of others, or from public interest; seclusion..."[22] and the explanation of privacy in the third edition is "Privacy... 1. The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion..."[23] The third edition adds new ideas, such as "being alone", "freedom", "choice" and "right". The phenomenon of the changing meaning of privacy is seen in not only in English countries such as Canada, the U.K. and the U.S.A, but also in Japan. It is not clear when the English word, "privacy," was imported and popularized in Japan,[24] but the fourth edition of Kojien, one of the most famous Japanese dictionaries, published in 1991, had already included a definition for privacy. The explanation of privacy in the fourth edition is "Individual's matter is secret. Secret of

---

[22] Founded mainly on the materials collected by the Philological Society and edited by Sir James Augustus Henry Murray et al, *The Oxford English Dictionary: A New English Dictionary on Historical Principles* (Clarendon Press, 1909) sub verbo "privacy".

[23] *The Oxford English Dictionary Online* (Oxford University Press, 2020) sub verbo "privacy", online: <www.oed.com/view/Entry/151596>.

[24] Privacy was selected as one of the Keywords-of-the-Year of 1961. See, TRC Inc, *Nihon sesōgo shiryō jiten: Shōwa sengohen 2 - Dai 4 Kan* [Japanese Word Reflecting Social Condition Encyclopedia; Showa after World War II Series 2 - vol. 4] (Tokyo: TRC Inc, 2008) sub verbo "puraibashī". The source of the encyclopedia is, Mitsuo Morikawa, ed, *Kindai shingo to shakai jōshiki* [Modern New Words and Social Common Knowledge] (kin-ensha, 1965).

private person."[25] In the newest seventh edition, the definition of privacy is "Freedom, which no one shall interfere, on each individual's private life."[26] Thus, the meaning of privacy changed from "secret" to "freedom".

Privacy is discussed in many academic fields. Economics includes the idea that privacy is one of the types of property like money, as well as that it is information and connected to consumption behavior.[27] Privacy can become an object for buying and selling, like books or cars, and a factor which affects consumers' choice to buy products or not. In psychology, one researcher has expressed the idea that privacy controls access to others and distance between one person and others.[28]

Privacy is just one word, but as just described, ordinary people give it various meanings: secret, territory which no one shall interfere and freedom to decide private matters by oneself. The meaning of privacy is changing. Moreover, privacy is understood differently in different academic fields. In the legal field, what does privacy mean? The concept of privacy in the minds of individuals, and the idea of privacy which should be protected by law may be different. As noted above, privacy is not defined in any acts in Canadian and Japanese law; therefore, privacy as a right in law is interpreted in various ways by jurists.[29] Nevertheless, we can catch a certain common understanding of privacy as a right by examining judicial precedents and doctrines.

---

[25] Izuru Shimmura, ed, *Kojien*, 4th ed (Tokyo: Iwanami Shoten, 1991) sub verbo "puraibashī".

[26] Izuru Shimmura, ed, *Kojien*, 7th ed (Tokyo: Iwanami Shoten, 2018) sub verbo "puraibashī".

[27] See Alessandro Acquisti, Curtis Taylor & Liad Wagman, "The Economics of Privacy" (2016) 52:2 J Econ Lit.

[28] "Recently I offered a conceptualization of privacy as the selective control of access to the self, involving dialectic, optimization, and multimodal processes" Irwin Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33:3 J Soc Issues 66 at 67; "privacy is an interpersonal boundary-control process which paces and regulates the interaction with others." Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Monterey, Cal: Brooks/Cole, 1975) at 10—11.

[29] "Various definitions of "privacy" have been adopted throughout time, illustrating a multifaceted and evolving concept." Eloïse Gratton, *Understanding personal information: managing privacy risks* (Markham, Ont: LexisNexis, 2013) at 1. Indeed, many jurists have attempted to address the right of privacy. Warren and Brandeis addressed it as the right to be let alone, based on the idea of Judge Cooley. Edward Jerome Bloustein states that the right of privacy is the right to protect individuals' spiritual values and inviolate personality. See Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964)

2.2 Right of Privacy in Canada

The way in which the Canadian legal system protects privacy may be, as we will see, a little more complex than that of Japan.[30] Many factors need to be considered to properly understand the right of privacy in Canada.

The first factor to consider is the object being protected: whether privacy itself or personal information is protected. Strictly speaking, privacy protection is different from personal information protection, although they are not mutually exclusive.[31] The development of privacy protection will be considered in this section, and the development of personal information protection will be dealt with in Section 3.

The second factor to consider is the *type* of law; for example, constitutional law, criminal law, tort law, etc. Privacy is protected by various laws which fall into several categories. Firstly, public law rules the relationship between the individual and the government, while private law governs the relationship between individuals. Within the category of public law, mainly constitutional law and criminal law protect privacy. For instance, the *Canadian Charter of Rights and Freedoms*[32] has provisions to restrict unreasonable search or seizure[33] and to guarantee the right to life, liberty and security of the person.[34] Although the *Charter* applies to the relationship between the state and the individual, the right of privacy and the core of privacy interests

---

39:6 NYUL Rev 962. Alan Furman Westin writes, "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Alan F Westin, *Privacy and freedom* (London: Bodley Head, 1970) at 7.) Alternatively, William Parent says, "I propose that privacy be defined as the condition of not having undocumented personal information about oneself known by others." (William A Parent, "A New Definition of Privacy for the Law" (1983) 2:3 Law & Phil 305 at 306.) and believes, "privacy is an ideal distinct from values like secret, solitude, and autonomy." (*Ibid* at 309.)

[30] David Elder, "Canada" in Monika Kuschewsky, ed, *Data Protection & Privacy: Jurisdictional Comparisons* (London: Sweet & Maxwell, 2012) 41 at 41; Susan Alter, Nancy Holmes & William Young, "Privacy Rights and New Technologies: Consultation Package" in *Privacy: Where Do We Draw the Line?* Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (Ottawa: House of Commons, 1997) Appendix I at 1.

[31] Colin HH McNairn & Alexander K Scott, *Privacy Law in Canada* (Toronto: Butterworths, 2001) at 3.

[32] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

[33] *Ibid* s 8.

[34] *Ibid* s 7.

recognized in the *Charter* are significantly influential to other laws protecting privacy.[35] The *Criminal Code*[36] of Canada prohibits the interception of a private communication in Part VI - Invasion of Privacy, although this thesis will not focus on privacy protection in criminal law. Within the category of private law, tort is the foremost means of privacy protection; private law is a provincial matter.[37]

The third factor to consider is the federal and provincial system in Canada. In some cases, privacy is protected by federal law, and in the other cases, it is protected by provincial law. Canada has ten provinces and three territories, and privacy problems between individuals are resolved within their provincial legal frameworks. Focusing on civil legal matters, provinces in Canada are categorized into two types, common law and civil law. Some common law provinces recognize a cause of action of invasion of privacy,[38] but the other provinces deny it.[39] Four common law provinces (British Columbia, Manitoba, Saskatchewan and Newfoundland) have statutes regulating the invasion of privacy.[40] The civil law province, Quebec, protects privacy with the *Charter of Human Rights and Freedoms*[41] and the *Civil Code of Quebec* (CCQ).[42] The *Quebec Charter* can be directly applicable to private litigations, unlike the *Canadian Charter*.[43] The CCQ has provisions to protect privacy; for example, article 35 of CCQ stipulates:

---

[35] See McNairn & Scott, *supra* note 31 at 17.

[36] RSC 1985, c C-46.

[37] *Constitution Act, 1982*, s 92, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11. See also Lewis N Klar, "The Impact of U.S. Tort Law in Canada" (2011) 38:2 Pepp L Rev 359 at 362.

[38] See e.g. *Jones v Tsige*, 2012 ONCA 32; *Grant v Winnipeg Regional Health Authority et al*, 2015 MBCA 44 at para 126.

[39] *Demcak v Vo*, 2013 BCSC 899 at para 8.

[40] British Columbia has the *Privacy Act*, RSBC 1996, c 373; Manitoba has the *Privacy Act*, CCSM, c P125; Saskatchewan has the *Privacy Act*, RSS 1978, c P-24; Newfoundland has the *Privacy Act*, RSNL1990, c P-22; See also Stuart Hargreaves, "Relational Privacy & Tort" (2017) 23:3 Wm & Mary J Women & L 433 at 442; Anastasia Powell & Nicola Henry, *Sexual Violence in a Digital Age* (London: Palgrave Macmillan, 2017) at 214.

[41] CQLR [*Québec Charter*].

[42] Government of Canada (Department of Justice), "Modernizing Canada's Privacy Act", (20 August 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.

[43] See Pierre-Emmanuel Moyse, *Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé* (2018) at 12; Law Reform Commission of Hong Kong, *Civil Liability for Invasion of Privacy* (2004) at 66.

35. Every person has a right to the respect of his reputation and privacy.
The privacy of a person may not be invaded without the consent of the person or without the invasion being authorized by law.[44]

With these factors in mind, the development of the right of privacy shall be examined. Firstly, the right of privacy as situated in the *Canadian Charter* will be studied. Next, the torts related to privacy (tort in the common law provinces, statutory tort in the common law provinces and delict in the civil law province) will be considered.

2.2.1 Right of Privacy between Government and Individual

This section will consider the interests of privacy and right of privacy between government and individual as seen in the *Canadian Charter of Rights and Freedoms*. According to the Supreme Court, the right of privacy can be found within the *Charter*.[45] At first, privacy was acknowledged as a human right in the *Canadian Human Rights Act*,[46] and later adopted by the *Charter*.[47] The *Charter* was introduced into the *Constitution Act* in 1982.[48] As Professor Pierre-Emmanuel Moyse has explained regarding its role:

> The *Canadian Charter*, which applies only in public law litigation involving the state or its representatives, has become a primary source of the right to privacy. Although it cannot be directly invoked in disputes involving private law, natural or legal persons, it has a considerable influence not only on the interpretation of personal information law but also on the development of common law. It nourishes the other rights.[49]

---

[44] CCQ at art 35.

[45] Eric H Reiter, "Privacy and the Charter: Protection of People or Places?" (2009) 88:1 Can B Rev 119 at 121.

[46] SC 1976-77, c 33. Canadian Human Rights Act was enacted in 1977, and it enshrined the right of privacy and the right of access to a person's own record including personal information in the public sector, according to point (b) of Section 2, "the privacy of individuals and their right of access to records containing personal information concerning them by any purpose including the purpose of ensuring accuracy and completeness should be protected to the greatest extent consistent with the public interest." See also David H Flaherty, *Reflections on Reform of the Federal Privacy Act* (Office of the Privacy Commissioner of Canada, 2008) at 5.

[47] See Federica Giovanella, *Copyright and Information Privacy: Conflicting Rights in Balance* (Cheltenham, UK: Edward Elgar Publishing, 2017) c 3 s 3.3.

[48] See Linda McKay-Panos, "The Canadian Charter of Rights and Freedoms: An Integral Part of Our Constitution" 37:3 LNow 20 at 21.

[49] Moyse, *supra* note 43 at 8, [translated by author].

The *Charter* has thus significantly contributed towards the protection of privacy interests in the Canadian legal system.[50]

2.2.1.1 Privacy Protected by Section 8 of Canadian Charter of Rights and Freedoms

Section 8 of the *Charter* is fundamentally concerned with protecting privacy, with section 7 contributing some additional protections.[51] Section 8 states that "Everyone has the right to be secure against unreasonable search or seizure."[52]

The purpose of this provision is principally to protect individuals against unreasonable search and seizure by government or governmental agents;[53] however, it also carries the expectation of protection against unjustified invasion of privacy interests, as per *Hunter v. Southam Inc*.[54] The judgement reached in this case provided a basis for the conclusion that section 8 of the *Charter* protects a right to privacy.[55]

The right of privacy was then applied in the case of *R. v. Dyment.*[56] At this time, the Supreme Court of Canada clearly recognized the right of privacy within the *Charter*. The plaintiff, Dyment, caused a single vehicle accident and was delivered to hospital by a Royal Canadian Mounted Police officer. While Dyment was unconscious, the doctor collected a blood sample and shared it with the officer without Dyment's knowledge. The officer found that the sample had a high blood alcohol concentration. The judges concluded that the officer's holding of the blood sample without a search warrant was a breach of section 8 of the *Charter* and a violation of the

---

[50] McNairn & Scott, *supra* note 31 at 17.

[51] See Government of Canada (Department of Justice), "Charterpedia - Section 8 – Search and seizure", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html>.

[52] *Charter*, *supra* note 32 s 8.

[53] See McNairn & Scott, *supra* note 31 at 18.

[54] [1984] 2 SCR 145 at 159, 11 DLR (4th) 641. See, McNairn & Scott, *supra* note 31 at 18.

[55] See *R v Gomboc*, 2010 SCC 55 at para 17.

[56] [1988] 2 SCR 417, 1988 CarswellPEI 7 (WL Can). See also Catherine Wedge, "Limitations on Alcohol and Drug Testing in Collective Bargaining Relationships" (1994) 2 CLELJ 461 at 463.

right of privacy.[57] The Supreme Court of Canada stated that "privacy is at the heart of liberty in a modern state"[58]

While section 8 was applied in *R. v. Dyment*, this section cannot be applied to protect the right of privacy in every case. The right of privacy in section 8 protects individuals only if the government conducts unreasonable search or seizure,[59] although the Court has quite a broad understanding of search and seizure.[60] According to the Court, the definition of "search" in section 8 is "any state activity that interferes with a reasonable expectation of privacy".[61] "To search" does not only imply looking for physical things but also incorporeal things like verbal words or digital data in a computer.[62] Additionally, "seizure" can be defined as "the taking of a thing from a person by a public authority without that person's consent",[63] with a "thing" being a broad term that can encompass something like information. Moreover, seizure can include requirements to produce something; for example, a state can enforce production of a document or information on a person.[64]

As above, the Court interprets search and seizure in a broad sense, and the expectation of privacy protected by section 8 extends to informational privacy. The breadth of the Court's interpretation of section 8 is expressed in *R. v. Plant*,[65] in which Sopinka J. stated:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from

---

[57] See *R v Dyment*, *supra* note 56.

[58] *Ibid* at para 17.

[59] See Benjamin Oliphant, "Taking Purposes Seriously: The Purposive Scope and Textual Bounds of Interpretation under the Canadian Charter of Rights and Freedoms" (2015) 65:3 UTLJ 239 at 264; *R v Evans*, [1996] 1 SCR 8 at para 11, 131 DLR (4th) 654. See also *R v Tessling*, 2004 SCC 67 at para 17—18.

[60] McNairn & Scott, *supra* note 31 at 19.

[61] Government of Canada (Department of Justice), *supra* note 51.

[62] See *R v Tessling*, *supra* note 60 at para 18—24; Government of Canada (Department of Justice), *supra* note 51.

[63] *R v Dyment*, *supra* note 56 at 431.

[64] See Joshua A Krane, "'Sir'ches and Seizures: Are Supplementary Information Requests Unconstitutional?" (2011) 52:2 Can Community LJ 232 at 239.

[65] [1993] 3 SCR 281, 84 CCC (3d) 203.

> dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[66]

Furthermore, in the recent case of *R. v. Marakah*,[67] the Supreme Court extended the informational zone, one of three privacy zones,[68] and has interpreted section 8 broadly to recognize the confidentiality of electronic communications.[69] The judge stated:

> Electronic conversations, in sum, are capable of revealing a great deal of personal information. Preservation of a "zone of privacy" in which personal information is safe from state intrusion is the very purpose of s. 8 of the *Charter*: see *Patrick*, at para. 77, per Abella J. As the foregoing examples illustrate, this zone of privacy extends beyond one's own mobile device; it can include the electronic conversations in which one shares private information with others. It is reasonable to expect these private interactions — and not just the contents of a particular cell phone at a particular point in time — to remain private.[70]

The right of privacy in section 8 of the *Charter* secures individual privacy, and the definitions of search and seizure and the areas of privacy protected by section 8 are broad. Nevertheless, since the right of privacy in section 8 only comes into play when government interference occurs through an unreasonable search and seizure, the protection provided through section 8 is still limited.[71]

2.2.1.2 Privacy Protected by Section 7 of Canadian Charter of Rights and Freedoms

The right of privacy is also found in section 7, where it is written, "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[72] The Supreme Court has not fully recognized independent privacy protection under section 7, but the Court has accepted that privacy is one of the interests

---

[66] *Ibid* at 293.

[67] 2017 SCC 59.

[68] See section 2.4. See also *Ruby v Canada (Solicitor General)*, 3 FC 589 at para 166, 187 DLR (4th) 675.

[69] Moyse, *supra* note 43 at 8.

[70] *R. v. Marakah*, *supra* note 67 at para 37.

[71] See McNairn & Scott, *supra* note 31 at 18.

[72] *Charter*, *supra* note 32 s 7.

of liberty and security for individuals.[73] In the case of *R. v. O'Connor*,[74] the Court concluded that the right to "liberty and security of the person" in section 7 includes some expectation of privacy protection.[75] Prior to this case, the right to security of the person had been applied to protect individuals' freedom of decision-making in personal matters and their mental integrity.[76] For example, this right would be applicable if the state acted to restrict an individual's choice to refuse a medical intervention or to have an abortion or an assisted suicide.[77] However, *R. v. O'Connor* determined that rights to personal autonomy and defense of mental integrity, and furthermore the idea that common law systems and section 8, among other sections of the *Charter*, delineate the values of liberty and security of the person, implied that privacy should be respected.[78]

Godbout v. Longueuil (City)[79] emphasized the aspect of freedom related to the right of privacy from the section 7 of *Charter*. The city of Longueuil required all new permanent employees to live within its boundaries. Godbout signed a declaration agreeing to live within the city and accepting the possibility that her employment could be terminated if she moved out of the city for any reason. The Court found that the city of Longueuil violated both the *Canadian Charter of Rights and Freedoms* and the *Charter of Human Rights and Freedoms*. La Forest J. cited the reasoning of Wilson J. in *R. v. Morgentaler*,[80] stating "I had "considerable sympathy" for the proposition that s. 7 includes within it a right to privacy. Moreover, the view that the right to liberty encompasses more than just physical freedom is, as I explained in *B. (R.),* supported by the vast

---

[73] See Richard Peck & Sarah Pringle, "Privacy, Technology and the Rule of Law" (2019) 77:6 Advocate 837 at 841; Government of Canada (Department of Justice), "Charterpedia - Section 7 – Life, liberty and security of the person", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html>.

[74] [1995] 4 SCR 411, 130 DLR (4th) 235.

[75] See McNairn & Scott, *supra* note 31 at 35.

[76] See *R v Morgentaler*, [1988] 1 SCR 30; Bert-Jaap Koops et al, "A Typology of Privacy" (2017) 38:2 U Pa J Intl L 483 at 511—512, n 92. See also McNairn & Scott, *supra* note 31 at 35.

[77] See Government of Canada (Department of Justice), *supra* note 73.

[78] See McNairn & Scott, *supra* note 31 at 35.

[79] [1997] 3 SCR 844, 152 DLR (4th) 577.

[80] *supra* note 73.

preponderance of American case law dealing with the subject".[81] He also stated, "The foregoing discussion serves simply to reiterate my general view that the right to liberty enshrined in s. 7 of the *Charter* protects within its ambit the right to an irreducible sphere of personal autonomy wherein individuals may make inherently private choices free from state interference."[82] This case concluded that section 7 protects personal autonomy as the right of privacy and that personal autonomy includes the choice of selecting one's home.

Although section 7 deals with the right to life, liberty and security of the person, it should not be assumed that the right to privacy in section 7 is always more comprehensive than in section 8 which limits privacy in the aspects of search and seizure, nor that the right to privacy under section 8 necessarily guarantees protection under section 7.[83] If that were true, the limitation of search and seizure under section 8 would be useless, and section 7 would always be invoked when dealing with privacy issues. The different areas of privacy protected by section 7 and 8 can be found in the example of a regulator searching business premises for commercial records belonging to an individual without a warrant. In this case, the regulator's search might violate the right to privacy under section 8, but it might not be said to be a violation of the right to privacy under section 7 because the life or personal security of the owner of those records would not necessarily be threatened.[84] Additionally, since only individuals receive benefits under section 7, this section is in one sense more limited than section 8 which considers companies as eligible for protection as legal persons.[85] In some cases, the right of privacy can reasonably be argued by both sections 7 and 8, but in other cases, only one section applies.

---

[81] See *Godbout v. Longueuil (City)*, *supra* note 79 at para 65.

[82] *Ibid* at para 66.

[83] See McNairn & Scott, *supra* note 31 at 36.

[84] See *Ibid*.

[85] Government of Canada (Department of Justice), *supra* note 73.

2.2.2 Right of Privacy between Individuals

Privacy between government and individual is protected by the *Charter*, and privacy between individuals is protected by tort in common law provinces and by delict in Quebec.[86] The tort law in common law provinces is divided into two categories, one being common law tort, and the other being statutory tort. Four common law provinces (British Columbia, Manitoba, Saskatchewan and Newfoundland) have granted statutory cause of action for invasion of privacy.[87] In the remaining common law provinces, the courts must decide whether a claim for invasion of privacy can be made under the common law tort.[88] In Quebec, as a civil law province, privacy between individuals is protected by delict.[89]

2.2.2.1 Tort in Common Law Provinces

2.2.2.1.1 Canadian Approach to Recognize the Invasion of Privacy in Common Law

Influenced by the divergent directions of the American and English courts, the Canadian courts have long deliberated over whether a tort of invasion of privacy can be acknowledged within Canadian common law.[90]

The courts in the United States have acknowledged the common law tort of invasion of privacy, accepting the theory in "The Right to Privacy"[91] written by Samuel Warren and Louis Brandeis, who were the first to insist that privacy was a legal right. English courts, by contrast, have hesitated to pursue such an approach. At times, they have used and broadened the already

---

[86] See Giovanella, *supra* note 47.

[87] See *supra* note 40. See also Huw Beverley-Smith, Ansgar Ohly & Agnès Lucas-Schloetter, *Privacy, Property and Personality* (Cambridge, UK: Cambridge University Press, 2005) at 35.

[88] See McNairn & Scott, *supra* note 31 at 42.

[89] See Giovanella, *supra* note 47 n 41.

[90] See McNairn & Scott, *supra* note 31 at 42.

[91] Samuel D Warren & Louis Dembitz Brandeis, "The Right to Privacy" (1890) 4:5 Harv L Rev 193.

established avenues of malicious falsehood, defamation, and breach of confidence to protect privacy, rather than specifically declaring a tort of invasion of privacy.[92]

Each country's approach has received commendations and criticisms. For example, the English approach allows courts to counter specific activities which are likely to invade privacy on a more targeted basis,[93] although critics contend that the approach either unnecessarily distorts the existing recognized torts or else leads the courts to unreasonably refuse to allow plaintiffs to recover.[94] On the other hand, while the American approach provides more direct protection against invasion of privacy,[95] proponents of the English approach argue that introducing a new cause of action into common law, especially dealing with such a nebulous concept as privacy, will allow uncertainty and controversial questions to arise.[96]

Canadian courts' unique development of the right of privacy in common law has not fully taken either the U.S. or English approach. For a long time, Canadian courts were unwilling to specifically recognize a common law tort of invasion of privacy, in some cases expanding existing tort actions in a similar way to the English approach. On the other hand, Canadian courts generally refused to strike out invasion of privacy claims.[97] More recently, however, Canadian courts have recognized the tort of intrusion upon seclusion and the tort of public disclosure of private facts, which are similar to the tort for invasion of privacy acknowledged in the U.S.[98]

---

[92] See McNairn & Scott, *supra* note 31 at 43.

[93] See Gerald Dworkin, "The Younger Committee Report on Privacy" (1973) 36:4 The Modern Law Review 399 at 400. See also Neil M Richards & Daniel J Solove, "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96:1 Geo LJ 123 at 166—167.

[94] See *Palad v Pantaleon*, 1989 CarswellOnt 2794 (WL Can) at para 65, [1989] OJ No 985 (QL) (Ont Dist Ct).

[95] See Warren & Brandeis, *supra* note 91 at 205.

[96] See McNairn & Scott, *supra* note 31 at 43—44. See also Dworkin, *supra* note 93 at 401.

[97] See McNairn & Scott, *supra* note 31 at 44.

[98] Chris DL Hunt, "Privacy in the Common Law: A Critical Appraisal of the Ontario Court of Appeal's Decision in Jones v. Tsige." (2012) 37:2 Queen's LJ 661 at 661—662.

2.2.2.1.2 Refusing to Strike Out Invasion of Privacy Claims

As mentioned above, Canadian courts have not tended to strike out claims framed as invasion of privacy. Refusal to strike out a claim of privacy invasion can be found in the 1970 case of *Krouse v. Chrysler Canada Ltd*.[99] In this case, someone had taken an image of the back of a Canadian Football League Player, Krouse, and used it in a Chrysler Canada advertisement, without Krouse's consent. The court neither struck out the invasion of privacy claim nor granted that the invasion of privacy action is recognized in Canadian common law, stating, "It may be that the action is novel, but it has not been shown to me that the Court in this jurisdiction would not recognize a right of privacy. The plaintiff therefore has the right to be heard, to have the issue decided after trial."[100] In the end, the Court decided that the plaintiff was allowed to recover for a tort of misappropriation of personality for commercial gain, not for invasion of privacy itself.[101] Finally, the Court of Appeal reversed the decision of Ontario High Court.[102] However, it did not do so because of a lack of recognition of the tort of misappropriation of personality for commercial gain,[103] but because it decided that this particular case did not fit under the category of that tort. Currently, the tort of misappropriation of personality for commercial gain is included in Canadian common law.[104]

After *Krouse v. Chrysler Canada Ltd*, there were some cases[105] in which courts have rejected breach of privacy claims because the common law did not recognize the cause of action

---

[99] [1970] 12 DLR (3d) 463, 3 OR 135 (Ont H Ct J).

[100] *Ibid* at 464.

[101] In U.S. doctrines, the tort of misappropriation of personality for commercial gain is one of the invasions of privacy. See Prosser's four categories of invasion of privacy in section 2.3.1.

[102] See *Krouse v Chrysler Canada Ltd et al* (1973), 40 DLR (3d) 15, 1 OR (2d) 225 (Ont CA).

[103] See *Ibid* at para 37—38.

[104] See *Athans v Canadian Adventure Camps Ltd et al* (1977), 17 OR (2d) 425, 80 DLR (3d) 583 (Ont H Ct J).

[105] For example, "There is no foundation whatever for claiming that from the primeval mud of the common law in force in Manitoba there has evolved the tort of "false light invasion of privacy"" See *Parasiuk v Can Newspapers Co*, [1988] 2 WWR 737 at 738, 1988 CarswellMan 108 (WL Can) (Man QB).

of invasion of privacy.[106] However, Canadian courts have generally allowed allegations of breach of privacy to proceed to trial.[107]

2.2.2.1.3 Existing Tort Action and Invasion of Privacy

While Canadian courts had usually accepted cases against breach of privacy, at first, they had not recognized recovery due to invasion of privacy, and had instead protected privacy with existing tort action, for example, nuisance.

In a 1976 case in Alberta, *Motherwell v. Motherwell*,[108] the Court of Appeal made specific acknowledgement of privacy invasion concerns through creation of a novel category of private nuisance.[109] In this case, the defendant had been excessively contacting her father and brother and brother's wife, the plaintiffs, with phone calls sometimes exceeding 60 times per day. At that time, common law had not recognized a tort of invasion of privacy in any existing category. However, in characterizing the defendant's action as a species of private nuisance, the Court of Appeal allowed the plaintiffs to gain recovery for the telephone harassment.[110] After this case, courts in other provinces referred to and followed along the lines of this decision,[111] with one of the courts calling this new cause of action in private nuisance the "tort of nuisance by invasion of privacy."[112]

Eventually, the courts began to allow for recovery for privacy invasion directly. The 1981 case of *Saccone v. Orr*[113] in an Ontario country court was the first case to officially recognize an

---

[106] See McNairn & Scott, *supra* note 31 at 80.

[107] See *Ibid* at 54.

[108] (1976) 73 DLR (3d) 62, 1976 CarswellAlta 129 (WL Can) (Alta SC [AD]).

[109] See Susan McCorquodale, "Corporations' Right to Privacy in Canada and Australia: A Comparative Analysis" (2003) 15:1 Bond L Rev 102 at 111.

[110] See Jo Bridgeman & Michael A Jones, "Harassing Conduct and Outrageous Acts: A Cause of Action for Intentionally Inflicted Mental Distress?" (1994) 14:2 LS 180 n 134.

[111] See Elizabeth Cooke, "A Development in the Tort of Private Nuisance" (1994) 57:2 Modern L Rev 289 at 292—293. See also McNairn & Scott, *supra* note 31 at 56.

[112] See *Provincial Partitions Inc v Ashcor Inplant Structures Ltd*, 1993 CarswellOnt 1119 at para 70, [1993] OJ No 4685 (QL) (Ont Ct [Gen Div]).

[113] 1981 CarswellOnt 586 (WL Can), [1981] OJ No 3132 (QL) (Ont Co Ct).

invasion of privacy and allow for recovery in Canada.[114] The plaintiff had sued his friend who had recorded a private telephone conversation, unbeknownst to the plaintiff, and had later played it at a municipal council meeting. The court stated, "I must decide as to whether an action exists with regard to invasion of privacy."[115] and "Certainly, for want of a better description as to what happened, this is an invasion of privacy, and despite the very able argument of defendant's counsel that no such action exists, I have come to the conclusion that the plaintiff must be given some right of recovery for what the defendant has in this case done."[116] Finally, the court concluded that an invasion of privacy had occurred, and awarded damages to the plaintiff.[117]

In the Ontario District Court case of *Palad v. Pantaleon*, Mandel J. expressed that the right of privacy exists in Canadian common law, stating:

> In Ontario there is no remedy legislated as in some of the other Provinces. If there is to be a remedy at present it must be forged by the Courts. At the stage of pleadings the Courts have refused to dismiss actions for invasion of privacy on the basis that it has not been shown that such a right does not exist (see *Caplan v. Caplan* (1980-81) 14 C.C.L.T. 191). In my view such a right does exist.[118]

This assessment contradicted English jurists' reasoning that recognizing a tort of invasion of privacy would work against promotion of free circulation of information.[119] In this case the court granted recovery for an invasion of privacy, rather than extending an existing cause of action connected to privacy. Moreover, Mandel J. clarified the condition by which one could recover for

---

[114] See Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44:4 McGill LJ 849 at 884.

[115] *Saccone v. Orr*, *supra* note 113 at para 8.

[116] *Ibid* at para 26.

[117] See David Debenham, *Canada's New Tort of Privacy and Its Impact on Your Fraud Investigation* (2012) at 7 online: <www.acfe.com/uploadedFiles/ACFE_Website/Content/canadian/2012/presentations/cpp-2A-David-Debenham.pdf> .

[118] *Palad v Pantaleon*, *supra* note 94 at para 71.

[119] See McNairn & Scott, *supra* note 31 at para 57.

a breach of the right of privacy in common law through another case, *Roth v. Roth*,[120] the condition being that if an individual hopes to recover for an invasion of privacy, the invasion should be "substantial and of a kind that a reasonable person of normal sensitivity would regard as offensive and intolerable."[121]

Thus, at the initial stage of privacy protection in Canadian common law tort, Canadian courts had allowed for recovery for invasion of privacy using pre-existing torts, for example, the tort of nuisance, however, it was later recognized that Canadian common law included the tort of invasion of privacy in a number of courts, especially lower courts in Ontario.[122]

2.2.2.1.4 The Relation between the Charter and Tort of Invasion of Privacy

While several courts found that a tort of invasion of privacy exists in common law, in some provinces, this idea continued to be questioned.[123] The Supreme Court also questioned the legal theory as to whether the existence of such a tort could be proved in common law.

Mandel J., in *Palad v. Pantaleon*,[124] justified his view that the right of privacy exists in Canadian common law based on the Supreme Court of Canada's decision in the case of *Hunter v. Southam*.[125] In this case, the Supreme Court recognized the right of privacy and concluded that it is not dependent upon the notion of trespass but rather is to protect citizens' reasonable expectation of privacy.[126] Working off of this assessment, Mandel J. stated, "There being such a general right not dependant on trespass to the person or property, nor in my view to proprietary interest as in

---

[120] 1991 CarswellOnt 44, [1991] OJ No 1301 (QL) (Ont Ct J [Gen Div]).

[121] *Ibid* at para 40, citing John G Fleming, *The law of torts*, 7th ed (London: Sweet & Maxwel, 1988) at 575.

[122] See McNairn & Scott, *supra* note 31 at 46.

[123] See Simon Chester, Jason Murphy & Eric Robb, "Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?" (2003) 27:4 Adv Q 357 at 361—362.

[124] *Palad v Pantaleon*, *supra* note 94.

[125] *Hunter et al. v. Southam Inc.*, *supra* note 54.

[126] *Ibid* at 158—160. *Ibid* at 159.

nuisance"[127] In this case and in the Ontario case of *Roth v. Roth*,[128] Mandel J. considered that Canadian common law should justifiably include a tort of invasion of privacy because the *Charter* protects privacy.[129] The Supreme Court has often expressed the intention to see the values of the *Charter* reflected in the development of common law even though the *Charter* does not apply directly to non-governmental actors.[130] Mandel J. concluded that an expectation of privacy should be upheld for non-governmental actors with respect to individuals' privacy claims, by means of common law, not only by governmental actors who are under the regulation of the *Charter*.[131]

However, this idea was not readily embraced by the Supreme Court, which held the view that new causes of action could not simply be generated through employing the *Charter*.[132] In *Hill v. Church of Scientology of Toronto*,[133] the Supreme Court clarified that the *Charter* concerns state actors, and does not pertain to private actors:

> Private parties owe each other no constitutional duties and cannot found their cause of action upon a *Charter* right. The party challenging the common law cannot allege that the common law violates a *Charter* right because, quite simply, *Charter* rights do not exist in the absence of State action. The most that the private litigant can do is argue that the common law is inconsistent with *Charter* values. It is very important to draw this distinction between *Charter* rights and *Charter* values.[134]

The Court stated while courts should develop the common law in accordance with the *Charter* principles,[135] they should do so through creation of new causes of action based on the *Charter*.[136]

---

[127] *Palad v Pantaleon*, *supra* note 94 at para 69.

[128] *Roth v. Roth*, *supra* note 120.

[129] McNairn & Scott, *supra* note 30 at 45.

[130] *R v Salituro*, [1991] 3 SCR 654 at 671, 68 CCC (3d) 289.

[131] McNairn & Scott, *supra* note 31 at 58.

[132] *Ibid*.

[133] [1995] 2 SCR 1130, 126 DLR (4th) 129.

[134] *Ibid* at para 95.

[135] See *Ibid* at para 91.

[136] See *Ibid* at para 95.

If the common law is to be significantly changed, "[courts] must not go further than is necessary when taking *Charter* values into account. Far-reaching changes to the common law must be left to the legislature."[137]

In a more recent case, *R v. Jarvis*[138] in 2019, it seems that the Supreme Court of Canada looked more favorably upon the idea that section 8 of the *Charter* provides a reasonable expectation of privacy against other private individuals.[139] The Court stated:

> The s. 8 case law has developed in relation to this latter purpose [that is to protect individuals' privacy interests from state intrusion]. The "reasonable expectation of privacy" that is decisive in the s. 8 context is therefore an individual's reasonable expectation of privacy vis-à-vis the state, or more specifically, vis-à-vis the instrumentality of the state that is said to have intruded on the individual's privacy... However, the s. 8 jurisprudence recognizes that the inquiry into whether an individual has a reasonable expectation of privacy vis-à-vis the state with respect to a certain subject matter may be informed, in part, by considering the individual's privacy expectations vis-à-vis other individuals... Thus, while the ultimate concern in the s. 8 context is whether there is a reasonable expectation of privacy vis-à-vis the state, the s. 8 case law contemplates that individuals may have reasonable expectations of privacy against other private individuals and that these expectations may be informed by some of the same circumstances that inform expectations of privacy in relation to state agents. This lends support to the view that the jurisprudence on s. 8 of the *Charter* may be useful in resolving the question raised in the case at bar.[140]

Thus, the Supreme Court indicated that the core value of privacy of the *Charter* could play a role in informing other laws that apply to cases between individuals. While the *Charter* itself doesn't apply to such cases, tort law should respect the spirit of the *Charter*.

---

[137] *Ibid* at para 96.

[138] 2019 SCC 10.

[139] See Moira Aikenhead, "A 'Reasonable' Expectation of Sexual Privacy in the Digital Age" (2018) 41:2 Dal LJ 273. See also, Saad Gaya, "R v Jarvis: Carving out a Contextual Approach to Privacy", (7 March 2019), online: *TheCourt.ca* <www.thecourt.ca/r-v-jarvis-carving-out-a-contextual-approach-to-privacy/>.

[140] *R. v. Jarvis*, *supra* note 138 at para 57—58.

2.2.2.1.5 Creation of New Privacy Torts

The tort of invasion of privacy was recognized in common law by several Canadian courts, with the lower courts in Ontario especially leading in this area.[141] Recently, new types of torts of invasion of privacy (the tort of intrusion upon seclusion and the tort of public disclosure of private facts) were created at the Ontario Court of Appeal. The Manitoba Court of Appeal recognized the tort of intrusion upon seclusion, but the Supreme Court of British Columbia declined it. Even now, it is uncertain whether the tort of invasion of privacy has taken root fully in the Canadian common law.

In *Jones v. Tsige*[142] in 2012, the Ontario Court of Appeal recognized a new common law tort, intrusion upon seclusion. The intrusion upon seclusion tort would be regarded as a subset of the invasion of privacy category.[143] The appellant, Sandra Jones, was an employee of a bank, and had a personal bank account there. The respondent, Winnie Tsige, worked for another branch of the same bank. She was in a common law relationship with Jones' former husband, though she and Jones were not acquainted. For four years, Tsige used her workplace computer to view Jones' personal banking activity at least 174 times without authorization, though she didn't record or share the information. At first, the Superior Court of Justice concluded that "there is no tort of invasion of privacy in Ontario."[144] However, the Ontario Court of Appeal overturned the decision of the Superior Court of Justice and recognized that intrusion upon seclusion had occurred. The conditions of the cause of action of intrusion upon seclusion are, firstly, that the intrusion is conducted intentionally (which includes recklessness); secondly, that the intrusion is toward private

---

[141] See McNairn & Scott, *supra* note 31 at 45.

[142] *Jones v. Tsige*, *supra* note 38.

[143] Rob Barrass & Lyndsay Wasser, *Seclusion Intrusion: A Common Law Tort for Invasion of Privacy* (McMillan LLP, 2012) at 2, online: <www.mcmillan.ca/seclusion-intrusion-a-common-law-tort-for-invasion-of-privacy>.

[144] *Jones v Tsige*, 2011 ONSC 1475 at para 57.

affairs or concerns without lawful justification; and thirdly, that the invasion is regarded regard as highly offensive and result in distress, humiliation or anguish in a reasonable person.[145]

The *Jones v. Tsige* case was foundational towards the decisions made in the case of *Doe 464533 v. ND* in 2016,[146] where a new privacy tort, the tort of public disclosure of private facts, was recognized.[147] The defendant, who was the plaintiff's ex-boyfriend, posted an intimate video of the plaintiff on a pornography website without her knowledge or consent. The court touched upon four tort categories related to privacy, which had been delineated by the prominent tort law author William L. Prosser,[148] and stated that although the case of *Jones v. Tsige* had provided an example of the first tort category (Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs), the given case was more closely related to the second tort category (Public disclosure of embarrassing private facts about the plaintiff).[149] The court adopted a new cause of action for public disclosure of private facts[150] and defined a new tort as a publicity of a matter concerning the private life of another, if the matter publicized or the act of the publication is highly offensive to a reasonable person and is not of legitimate concern to the public.[151]

Although the Ontario Court of Appeal recognized the new privacy torts, it is still unclear that courts of other provinces have also followed the decisions of Ontario. In *Demcak v. Vo*,[152] the Supreme Court of British Columbia stated, "No common law tort of invasion or breach of privacy

---

145 See *Jones v. Tsige*, *supra* note 38 at para 71.

146 2016 ONSC 541.

147 Lyndsay A Wasser & Mitch Koczerginski, *Can you keep a secret? The courts recognize a new tort for public disclosure of private facts* (2016) at 1, online: <https://mcmillan.ca/Can-you-keep-a-secret--The-courts-recognize-a-new-tort-for-public-disclosure-of-private-facts>.

148 See *Doe 464533 v ND*, *supra* note 146 at para 36.

149 See *Ibid* at para 41.

150 See *Ibid* at para 46.

151 See *Ibid*.

152 *Demcak v. Vo*, *supra* note 39.

exists in British Columbia."[153] However, the court mentioned the relationship between common law tort and statutory tort as pertains to invasion of privacy, and allowed that violations of privacy can be recognized by British Columbian statutory law and acted upon.[154] On the other hand, the Manitoba Court of Appeal, in *Grant v. Winnipeg Regional Health Authority et al*. in 2015,[155] touched on the possibility of a claim in tort for intrusion upon seclusion,[156] and the Nova Scotia Supreme Court suggested that a common law privacy tort could be accepted in an appropriate case in its jurisdiction in the future.[157]

2.2.2.2 Statutory Tort in Common Law Provinces

Four Canadian common law provinces grant a statutory cause of action related to individual privacy.[158] The four provinces are British Columbia, Manitoba, Saskatchewan, and Newfoundland. These provinces have statutes called Privacy Acts which lead the cause of action of privacy invasion,[159] these being the *Privacy Act*[160] of British Columbia, the *Privacy Act*[161] of Manitoba, the *Privacy Act*[162] of Saskatchewan and the *Privacy Act*[163] of Newfoundland. In this section, the four Privacy Acts are considered. Although these acts have provisions of cause of action of invasion of privacy, they were not enacted with the purpose of codifying a pre-existing common law of privacy. For example, after an electronic eavesdropping incident, the common law was seen

---

153 *Ibid* at para 8.

154 See *Ibid* at para 9.

155 *Grant v. Winnipeg Regional Health Authority et al.*, *supra* note 38.

156 See *Ibid* at para 126. See also Ellen Vandergrift, "Possible expansions to claims for breach of confidence", (29 May 2015), online: *Business Torts In Canada* <businesstorts.ca/blog/2015/5/29/possible-expansions-to-claims-for-breach-of-confidence>.

157 See *Trout Point Lodge Ltd v Handshoe*, 2014 NSSC at para 55. See also Chris DL Hunt, "The Common Law's Hodgepodge Protection of Privacy" (2015) 66 UNBLJ 161 at 173.

158 See Michael Power, *The Law of Privacy*, 2d ed (Toronto: LexisNexis Canada, 2017) at 221.

159 See Barbara McIsaac, Rick Shields & Kris Klein, *The law of privacy in Canada*, 2011 Student ed (Toronto: Carswell, 2011) at 2-58.66.

160 RSBC 1996, c 373.

161 CCSM, c P125.

162 RSS 1978, c P-24.

163 RSNL1990, c P-22.

to have insufficiencies, and the *Privacy Act* was passed in British Columbia in 1968,[164] with the intention of addressing this concern,[165] and clarifying whether common law in fact contained general tort related to privacy breaches. When the *Privacy Act* was enacted, the common law did not precisely recognize an all-purpose right to privacy, although it protected certain interests associated with privacy with other torts, for instance, trespass and nuisance.[166]

2.2.2.2.1 The Meaning of Violation of Privacy

"Violation of privacy" is defined in the four acts (see Table 2-1), and the definitions are similar. However, the four acts neither include a definition of privacy nor decide precisely the scope of the tort. Therefore, just as in provinces without such torts, the courts still need to consider and decide upon the boundaries of violation of privacy for themselves.[167]

Table 2-1 Definition of Violation of Privacy in Privacy Acts

Province	Definition
British Columbia	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.
Saskatchewan	2 It is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person.
Newfoundland	3. (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 an individual.
Manitoba	2(1) A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.

Courts have tried to find the meaning of privacy through cases. For example, in *Davis v. McArthur*,[168] in British Columbia, the court regarded the right of privacy as the right to an inviolate personality or the right to be let alone,[169] citing the U.S. case of *Hamilton v. Lumbermen's Mutual*

---

[164] See British Columbia Law Institute, "Report on the Privacy Act of British Columbia" (2008) 49 BCLI Rep, at 1, online: <www.ssrn.com/abstract=1418205>.

[165] See *Ibid* at 3.

[166] See *Ibid*.

[167] See McNairn & Scott, *supra* note 31 at 68.

[168] (1969) 10 DLR (3d) 250, 1969 CarswellBC 230 (WL Can) (BCSC).

[169] The court said, "The term "privacy" is not defined in the Act but its meaning has been dealt with in a number of cases in the United States.", and cited "... "the right to be let alone" as "the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity." It is a part of the general right of the immunity of the person. "It is like the right not to be maliciously prosecuted, the right not to be defamed". It is the right to an "inviolate personality."" *Ibid* at 254.

Casualty Co.,[170] and confirmed the meaning of privacy based on the definition from the Shorter Oxford English Dictionary, "The state or condition of being withdrawn from the society of others, or from public interest; seclusion"[171] (see the discussion of the definition in the Oxford English Dictionary in section 2.1). Although the court indicated the meaning of privacy, it hesitated to precisely define privacy, citing "The Right to Privacy" by Samuel Warren and Louis Brandeis.[172]

The boundary of the violation of privacy in the four Privacy Acts is still developing. John D. McCamus criticized that these four statutes are lacking in concreteness, "the provincial privacy tort statutes seem to do nothing more than briefly reiterate the basic principles of the American case law. The courts are given no statutory guidance as to how to apply these vague general principles to typical factual patterns. In short, the matter is legislatively remitted to the common-law method."[173] More recently, Chris D. L. Hunt wrote:

> these statutes offer little guidance as to when a privacy interest will arise, and the case law, such as it is, does little to illuminate. Although there have been dozens of cases decided pursuant to these statutes, almost all are trial level decisions, and none have analyzed in detail the factors relevant to such claims. As a result, the decided cases are largely impressionistic and often difficult to reconcile. Furthermore, despite the outpouring of academic commentary examining privacy torts in other countries, there has been no critical examination of the Canadian jurisprudence decided under these statutory regimes.[174]

The interpretation of the meaning and the scope of violation of privacy in statutory tort law in Canada is not unrelated to the *Charter* although the four Privacy Acts were enacted before the *Charter* was added into the *Constitution Act*. The meaning of the right of privacy and value of

---

[170] 82 So (2d) 61 (La Ct App 1955).

[171] *Davis v. McArthur*, *supra* note 168 at 254.

[172] See *Ibid* at 254—255.

[173] John D McCamus, "The Protection of Privacy: The Judicial Role" in Rosalie S Abella & Melvin L Rothman, eds, *Justice beyond Orwell* (Montréal: Éditions Y. Blais, 1985) 168 at 178. See also Douglas Camp Chaffey, "The Right to Privacy in Canada" (1993) 108:1 Political Science Quarterly 117 at 120—122.

[174] Chris DL Hunt & Nikta Shirazian, "Canada's Statutory Privacy Torts in Commonwealth Perspective", (2016), online: *Oxford University Comparative Law Forum* <ouclf.iuscomp.org/canadas-statutory-privacy-torts-in-commonwealth-perspective/>.

privacy protection which were developed in the *Charter* are influential to the interpretation of statutes. Interpretation of modern statutes fundamentally assumes that "legislation is enacted to comply with constitutional norms, including the rights and freedoms enshrined in the *Charter*".[175] Additionally, section 52 of the *Charter* emphasizes the superiority of *Charter*: "The Constitution of Canada is the supreme law of Canada, and any law that is inconsistent with the provisions of the Constitution is, to the extent of the inconsistency, of no force or effect."[176] Even though there is no *Charter* challenge to legislation, *Charter* values inform statutory interpretation "when genuine ambiguity arises between two or more plausible readings, each equally in accordance with the intentions of the statute",[177] and "where two readings of a provision are equally plausible, the interpretation which accords with *Charter* values should be adopted".[178] The role of *Charter* values is essential in statutory interpretation.[179]

2.2.2.2.2 Difference between Tort and Statutory Tort in Common Law Provinces

Although the definitions of "violation of privacy" in the Privacy Acts of the four provinces are very similar, there are some differences. British Columbia, Saskatchewan and Newfoundland do not require that the violation of privacy is substantial. If the definitions are compared with definitions of invasion of privacy (see, 2.2.2.1.3) and intrusion upon seclusion (see, 2.2.2.1.5) in common law tort, there are also differences. For example, in the definition of invasion of privacy by Mandel J., the invasion should be "substantial and of a kind that a reasonable person of normal sensitivity would regard as offensive and intolerable"[180], but none of the four Privacy Acts require that the

---

[175] *Application under s 8328 of the Criminal Code (Re)*, 2 SCR 248 at para 35.

[176] *Charter*, *supra* note 32 s 52.

[177] *CanadianOxy Chemicals Ltd v Canada (Attorney General)*, [1999] 1 SCR 743 at para 14, 171 DLR (4th) 733.

[178] *Application under s. 83.28 of the Criminal Code (Re)*, *supra* note 175 at para 35.

[179] See Government of Canada (Department of Justice), "Charterpedia - General principles for the interpretation and application of the Charter", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/principles-principes.html>.

[180] *Roth v. Roth*, *supra* note 120 at para 40.

violation is offensive and intolerable. Intrusion upon seclusion requires that the intrusion is conducted intentionally without lawful justification and is regarded as highly offensive, causing distress, humiliation or anguish by a reasonable person, but again, none of the four Privacy Acts mention intention.

Privacy Acts were enacted to address uncertainties about the existence of a common law cause of tort for privacy breach[181] not to seal tort in the common law. For example, in *Grant v. Winnipeg Regional Health Authority et al.*[182] in Manitoba, the court recognized a claim for intrusion upon seclusion; thus, the existence of a statutory cause of action in Manitoba may not preclude consideration of a common law claim for intrusion upon seclusion. Furthermore, the court explicitly states that, "Notably, The *Privacy Act* stipulates in s. 8(1) that any cause of action created by the Act is not in derogation of existing causes of action available to a claimant."[183] Also, Section 6 of the *Privacy Act* of Manitoba says, "The right of action for violation of privacy under this Act and the remedies under this Act are in addition to, and not in derogation of, any other right of action or other remedy available otherwise than under this Act"[184] There are similar provisions in section 7 (1) of the *Privacy Act* of Newfoundland and in section 8 (1) of the *Privacy Act* of Saskatchewan. Because of these provisions, if courts of these provinces recognise the existence of a right of action of invasion of privacy in common law, it is feasible that such a right could be sought by plaintiffs.[185]

British Columbia would have the same conclusion, although the *Privacy Act* of British Columbia does not have similar provisions to section 6 and 8(1) of the *Privacy Act* of Manitoba.

---

[181] See Moyse, *supra* note 43 at 12.

[182] *Grant v. Winnipeg Regional Health Authority et al.*, *supra* note 38.

[183] *Ibid* at para 114.

[184] *M Privacy Act*, *supra* note 40 s 6.

[185] See Amy M Conroy, "Protecting Your Personality Rights in Canada: A Matter of Property or Privacy?" (2012) 1:1 UWOJ Leg Stud at 7.

In *Joseph v. Daniels*,[186] the court supported the validity of not only the common law right of action, but also the statutory right of action.[187] The rights conveyed by statutory law have not been considered to minimize the rights conveyed by common law.[188] Both remedies may be valuable especially as in some circumstances one or the other claim might not be recognized.[189] However, although the *Privacy Act* of British Columbia may not rule out a common law claim, the court of British Columbia has recognized that common law tort of invasion or breach of privacy does not exist in British Columbia, as mentioned section 2.2.2.1.5.[190]

2.2.2.3 Delict in Quebec

In Quebec, the *Quebec Charter*[191] guarantees the right of privacy, and the delict of invasion of privacy exists under Quebec's *Civil Code*.[192]

2.2.2.3.1 Quebec Charter and Civil Code

As mentioned in 2.2.1, the *Canadian Charter* has an important role related to the right of privacy. Quebec also has its own *Charter of Human Rights and Freedoms*. The *Canadian Charter* regulates relationships between the state and individual, however, the *Quebec Charter* can regulate relationships between individuals.[193] The *Quebec Charter* has a "quasi-constitutional" value and recognizes the right to private life in Article 5, "Every person has a right to respect for his private

---

[186] 1986 CarswellBC No 3231, [1986] BCJ No 3231 (QL) (BCSC).

[187] See Conroy, *supra* note 185 at 8.

[188] See Moyse, *supra* note 43 at 6.

[189] See *Ibid*.

[190] See *Demcak v. Vo*, *supra* note 39 at para 8.

[191] *Quebec Charter*, *supra* note 41.

[192] See Giovanella, *supra* note 47 n 236.

[193] See Moyse, *supra* note 43 at 12.

life."[194] The right of privacy is now considered an essential freedom as a result of acceptance of this article.[195]

Quebec inherited the tradition of civil law and implemented the *Civil Code of Quebec*, which is rooted in the French Civilian tradition.[196] In the *Civil Code of Quebec*, privacy violation is identified as a delict.[197] In Article 3, the *Civil Code of Quebec* describes that every person has personality rights, notably the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy, and dictates that these rights are inalienable.[198] Moreover, the respect of reputation and privacy is protected from article 35 to article 40. Article 35 expresses that no one may be invaded without the consent. Also, Article 1457 is a general provision that allows for recovery for invasion of privacy.

2.2.2.3.2 Case Law in Quebec

Even before the CCQ came into force, Quebec citizens had successfully been compensated for privacy violations under these provisions. An example is the 1957 case of *Robbins v. Canadian Broadcasting Corp*.[199] The plaintiff was a physician who lived in Montreal. He sent the producer of a broadcasting company a letter to criticize the TV program. The producer broadcasted the letter with the plaintiff's name and address and requested the TV program's audience to write or telephone the plaintiff to "cheer him up". The plaintiff successfully sued the broadcaster under the general liability provision of the *Civil Code of Lower Canada.*

---

[194] *Quebec Charter*, *supra* note 41 s 5.

[195] "Déjà reconnu par la jurisprudence, l'adoption de l'article 5 de la charte québécoise a eu pour effet de consacrer le droit à la vie privée comme liberté fondamentale." Alain-Robert Nadeau, *Vie privée et droits fondamentaux : étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international.* (Thesis, University of Ottawa, 2000) [unpublished] at 36.

[196] See Government of Canada (Department of Justice), "Where our legal system comes from - About Canada's System of Justice", (16 October 2017), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/just/03.html>.

[197] Power, *supra* note 158 at 221.

[198] See Arts 3 CCQ.

[199] (1957) 12 DLR (2d) 35, 1957 CarswellQue 135 (WL Can) (Qc Sup Ct).

As mentioned earlier in section 2.2.1.2, *Godbout v. Longueuil (City)*[200] is a case related to both the *Canadian Charter* and the *Quebec Charter*. In this case, the court concluded that the residential limitation infringed upon both section 5 of the *Quebec Charter* and section 7 of the *Canadian Charter*.

This case referenced the judgements made in an important earlier case, *Brasserie Labatt ltée v. Villa*.[201] Pierre Villa was offered the position of vice-president of public affairs in Montreal. Villa and his wife and children needed to move to Montreal in accordance with company policy, and while Villa relocated, his family did not, and he was consequently dismissed. The court approved Villa's action for damages for wrongful dismissal, and stated that the company's requirement for Villa's family to move violated the right of privacy in art 5 of the *Quebec Charter*, which the judge argued extends to the choice of degree of cohabitation of an individual's spouse and children.[202]

In *Aubry v. Éditions Vice-Versa inc*.,[203] the Court mentioned the relationship between the right to free expression and the right of privacy, which are addressed in the *Quebec Charter*. In this case, the plaintiff's photograph was taken, published, and marketed without her consent. The Court upheld the judgement of the trial court that asserted that publication of the photograph without consent infringed upon the right to protection of image under the *Civil Code of Quebec*. Moreover, the Court concluded that in the circumstances of this case, the right of privacy rights takes precedence over the freedom of expression. The *Quebec Charter* enshrines the right of privacy in section 5 and the right to freedom of expression in section 3, and these may be conflict in some cases. The balance between the two rights relies on assessment of the situation of those concerned.

---

[200] *Godbout v. Longueuil (City)*, *supra* note 79.

[201] *Brasserie Labatt ltée v Villa*, 1994 CarswellQue 144, 1994 CarswellQue 144 (WL Can), [1994] JQ No 1002 (QL) (QCCA).

[202] *Ibid* at para 30.

[203] [1998] 1 SCR 591, 157 DLR (4th) 577.

As noted in the case: "In short, this is a question that depends on the context. For the purposes of legal analysis, it is inappropriate to resort to the notion of "socially useful information" adopted by the Court of Appeal."[204]

2.3 Right of Privacy in Japan

The development of the right of privacy in Japan is reviewed in this section. Japan's process of development of the right of privacy may be considered simpler than that of Canada because the Japanese legal system is centralized, and unlike Canada, there are neither two types of statutes at the federal and provincial level, nor is there a distinction between common law tort and statutory tort. The right of privacy in Japan was first recognized in private law, and subsequently in public law. Furthermore, the meaning of privacy expanded from traditional ideas, such as "the right to be let alone", to include more positive ideas of "freedom" and "choice", such as "the freedom of private life".

2.3.1 Influence of U.S. Doctrines and Cases and the Right of Privacy in Japanese Doctrines

U.S. doctrines and cases related to the right of privacy were influential to development of Japanese doctrines.[205] In the late 1950s, the right of privacy was actively debated in legal academia in Japan.[206] For example, "The Right to Privacy" written by Samuel Dennis Warren and Louis Dembitz Brandeis, which mentioned "the right to be let alone"[207] by Thomas McIntyre Cooley,

---

[204] *Ibid* at 593.

[205] See Nobuyoshi Ashibe, *Kempōgaku 2: Jinken sōron* [Study of Constitutional Law (2): General of Human Rights] (Tokyo: Yuhikaku, 1994) at 368; Ikuko Komachiya, "Puraibashī no kenri - kigen to seisei - [Right of Privacy - Origin and Generation -]" (2004) 15 Archives 48 at 53.

[206] See Masao Horibe, "Puraibashī kojin jōhō hogo giron no sekaiteki tenkai to nihon [Global Development of Privacy and Personal Information Protection Discussions and Japan]" (2013) 54:11 IPSJ J 1106 at 1107.

[207] Thomas McIntyre Cooley, *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Chicago: Callaghan & Company, 1880).

was translated,[208] and some books[209] to discuss about the right of privacy were published by Japanese law professors.

The four categories of invasion of privacy outlined by William Lloyd Prosser had a powerful impact on Japanese case law. Prosser wrote "Privacy"[210] in the California Law Review in 1960, and he reviewed many judgements related to the right of privacy and categorized them based on four behaviors considered as invasions of privacy. These four categories were: first, intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; second, public disclosure of embarrassing private facts about the plaintiff; third, publicity which places the plaintiff in a false light in the public eye; and fourth, appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[211] The four categories were introduced to Restatement of Tort (2nd),[212] by the American Law Institute, and American courts granted recovery for invasion of privacy according to the four categories.[213] As discussed in 2.2.2.1.5, Prosser's four categories have been cited in Ontario cases.[214] Prosser's framework for the idea of invasion of privacy has also been introduced to Japanese legal academia and courts and has had significant impact.[215]

---

[208] See Hiroshi Hokama, "Puraibashī no kenri (1) [The Right to Privacy]" (1959) 31:6 Horitsujiho 18.

[209] For example, Masami Ito, *Puraibashi no kenri* [Right of Privacy] (Tokyo: Iwanami Shoten, 1963); Sanji Suenobu, *Eibeihō no kenkyū (Jō)* [Study of Anglo-American Law (1)] (Tokyo: University of Tokyo Press, 1959); Michitaka Kaino, "Puraibashīken to sono hoshō [Right of Privacy and Guarantee]" (1959) 39:1.2.3 Minshoho Zasshi 87.

[210] William L Prosser, "Privacy" (1960) 48:3 Cal L Rev 383.

[211] See *Ibid* at 389.

[212] American Law Institute, *Restatement of the law (2nd) Torts* (St Paul, Minnesota: American Law Institute Publishers, 1977) s 652.

[213] See Stephen Todd, "Tortious Intrusions Upon Solitude and Seclusion" (2015) 27 Singapore Academy of Law Journal 731 at 732.

[214] See Hunt, *supra* note 98 at 661—662.

[215] Kazumasa Kakumoto, "Saibā jidai ni okeru puraibashī no hō riron (2) : Shihō jō no mondai wo chūshin ni [Legal Theory of Privacy in Cyber Era (2) : Focus on Issues in Private Law]" (2017) 67:5 Hokkaido L Rev 109 at 1435—1436, 1437 n 31.

The U.S. case of *Roe v. Wade*[216] was another thought-provoking case contributing to the development of Japanese legal theory.[217] In 1973, the plaintiff, Jane Roe, contended that the Texas criminal abortion law violates the *Constitution* of the U.S. at the Supreme Court of the United States. At that time, many states of America had laws prohibiting contraceptive devices and abortion from the viewpoint of religion and morality. Texas also prohibited abortion except in the case where it was deemed necessary to protect the mother's body. The plaintiff won this case by seven to two, and the law prohibiting abortion in Texas was judged as breaching the *Constitution* of the U.S. After this judicial decision, each state of America repealed its laws prohibiting abortion. In this case, Judge Blackman, who delivered the opinion of the Court, stated: "The *Constitution* does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as *Union Pacific R. Co. v. Botsford*, 141 U.S. 250, 251 (1891), the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the *Constitution*."[218] Blackman clearly used the words, the right of privacy, and expressed the opinion that the right of privacy exists under the *Constitution*. Also, the Court determined that the right of privacy legally means individual's freedom: "This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[219] The Supreme Court of the United States had the opinion that the right of privacy is

---

[216] 410 US 113 (1973). Before *Roe v Wade,* the right of privacy was already recognized as a right under the Constitution of the US, for example, *Griswold v Connecticut*, 381 US 479 (1965). However, the case of *Roe v Wade* clearly connected the right of privacy and Article 14 and showed for the first time in the U.S. that a decision to abort a pregnancy is protected by the right of privacy.

[217] See Misaki Maki, "Jiko ketteiken no ronten [Points at Issue of Right of Self-determination]" (2006) 2006:5 Reference 77 at 77―78.

[218] *Roe v. Wade*, *supra* note 216 at 152.

[219] *Ibid* at 153.

based on the Fourteenth Amendment's concept of personal liberty rather than the Ninth Amendment's protection of rights of the people, and interpreted that the right of privacy includes freedom for an individual to freely decide ones own private matters by oneself.

Many Japanese jurists have discussed whether the freedom to private life, such as birth control and contraception, is included in the right of privacy.[220] Dr. Koji Sato, a scholar at Kyoto University, insisted that the right of privacy should not include this freedom, because he separated the right of privacy and the right of personal autonomy. He thought that the right of privacy is the freedom to control information related to one's own existence, in order to provide a foundation for an environment conducive to love, friendship and trust between human beings, while the right of personal autonomy is the freedom to make decision's for one's personal life, including abortion, death of dignity and transfusion refusal.[221] Dr. Shigenori Matsui, a scholar at Osaka University, had a similar opinion, assessing the right of privacy as the guarantee that a subject can control disclosure, sharing and deletion of one's personal information data, and that the right of self-determination is the right to decide private matters without interference.[222] The reason why they made these distinctions is that they insisted that one right should have a clearly defined, homogeneous character, while they considered that the decision of private matters and the control of personal information is heterogeneous. On the other hand, Dr. Nobuyoshi Ashibe, a scholar at University of Tokyo, insisted that while he was considering the history of the development of the right of privacy in U.S., the right of privacy protects the freedom of private life which no one shall interfere, and the right includes two interests, both that one's private matters should not be shared,

---

[220] Toshiyuki Munesue, *Jinkenron no shin kōsei* [New Structure of Human Rights] (Tokyo: Shinzansha, 1992); Masahiro Akasaka, *Kempō kōgi: Jinken* [Lecture of Constitutional Law: Human rights] (Tokyo: Shinzansha, 2011) at 272―273.

[221] Koji Sato, *Kempō* [Constitutional Law], 3d ed (Tokyo: Seirin Shoin, 1995) at 453―454.

[222] Shigenori Matsui, *Nihonkoku kempō* [Constitution of Japan] (Tokyo: Yuhikaku, 1999) at 496―499.

and that one should be able to independently decide important matters concerning one's private life.[223]

Currently, the majority of Japanese jurists think that the right of privacy includes the freedom to decide private matter autonomously, but they usually use the right of privacy in the context of the right to control personal information, because in the current day, the right of privacy is mainly discussed in the context of personal information protection.[224] Japanese courts have not discussed the right of privacy in the context of the freedom to decide private matters autonomously, although they have implied it, as mentioned in sections 2.3.2 and 2.3.3.

2.3.2 Right of Privacy between Individuals

Japanese courts have granted recovery for that the invasion of privacy under article 709 (Damages in Torts) of the *Civil Code of Japan*:[225]

> Article 709 A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence.[226]

In Japan, the invasion of privacy between individuals is dealt with in the *Civil Code of Japan*. However, the right of privacy is usually understood to have been derived from Article 13 of the *Constitution of Japan*:[227]

> Article 13 All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare,

---

[223] See Ashibe, *supra* note 205 at 355—358.

[224] See Yagi Koji, *Mai nambā hō no subete* [All about My Number Act] (Tokyo: Toyo Keizai Inc., 2013) at 129; Taro Komukai, *Jōhōhō nyūmon* [Introduction to Information] (Tokyo: NTT Shuppan, 2015) at 191—192; Masatomo Suzuki, "kojin jōhō hogohō to puraibashī no kenri [The Act on the Protection of Personal Information and the Right of Privacy]" in Masao Horibe, ed, *Puraibashī kojin jōhō hogo no shin kadai* [New Issues of Protection for Privacy and Personal Information] (Tokyo: Shojihoumu, 2010) at 64—65.

[225] *Mimpo* [Civil Code of Japan], Amendment of Act No. 78 of 2006 [CCJ].

[226] Art 709 *ibid* [translated by Ministry of Justice of Japan].

[227] *Nihonkoku kempō* [Constitution of Japan], Constitution 1946.

be the supreme consideration in legislation and in other governmental affairs.[228]

The *Constitution of Japan* does not apply directly to the legal matters between individuals. Although the invasion of privacy between individuals is covered according to the provision of the *Civil Code of Japan*, its application should be consistent with and according to interpretation of the *Constitution*. In other words, the right of privacy derived from Article 13 of the *Constitution* is applied indirectly to private litigation through the *Civil Code of Japan*.[229] As a mentioned in section 2.3.1, the discussion of the right of privacy in Japanese legal academia started in the late 1950s. When the *Constitution* was promulgated in 1946, Article 13 had not initially included the right of privacy. The interpretation that Article 13 includes the right of privacy appeared in 1964.

In 1964, the case of *After the Banquet*[230] marked the first time that the right of privacy was granted in Japan.[231] The defendant, Hiraoka Kimitake,[232] wrote a novel entitled *After the Banquet*. The main character was modeled after the plaintiff, Arita.[233] The novel discussed the plaintiff's life after he was defeated in an election, and although Hiraoka had given the character a different name to that of the plaintiff, readers were able to easily recognize the character as Arita. The plaintiff insisted that the novel infringed upon his right to privacy and sued the author and

---

[228] *Ibid* Art 13 [translated by Ministry of Justice of Japan].

[229] Komukai, *supra* note 224 at 192.

[230] *Utage no ato* [After the Banquet], [1964] 15 Kakyu Saibansho Minji Hanreishu 2317, 385 Hanrei Jiho 12 (Tokyo District Court).

[231] According to Shimpo, prior to the *After the Banquet* case there was another case that mentioned the right of privacy, however, it did not approve the right of privacy. This was the *Demonstration for deterring the Japan-U.S. Security Treaty by Labour Union of Osaka Stock Exchange* case. In assessing this case, the judge stated, "The right of privacy is said to be the right of a private person to not have interference in his personal life by others, and to have naturally private matters protected from publication without consent... If the right of privacy is secured by the Constitution, unlimited photography of persons should not be allowed under any circumstances." *Osaka shoken roso ampo soshi demo* [Demonstration for deterring the Japan-US Security Treaty by Labour Union of Osaka Stock Exchange], [1964] 17 Koto Saibansho Keiji Hanreishu 384 at 392, 165 Hanrei Taimuzu 106 (Osaka High Court) [translated by author].See also Mikio Takahashi, "Higisha no shashin satsuei to shōzōken [Photographing of Suspect and Portrait Rights]" (1966) 135 Hanrei Taimuzu 73; Kiyoshi Igarashi, "Tekunorojī to puraibashī [Technology and Privacy]" (1969) 413 Jurist 134; Koji Sato, "Kenri toshiteno puraibashī [Privacy as Legal Right]" (1981) 742 Jurist 158.

[232] Hiraoka Kimitake has a pen name, Yukio Mishima.

[233] Arita was a Japanese politician and diplomat who served as the Minister for Foreign Affairs.

publisher. The judge accepted the plaintiff's assertion, and ordered the defendant to compensate for the invasion of privacy based on Article 709 of the *Civil Code of Japan*.

The judge stated that the defendant had published the depiction in a way that suggests that he had pried into the plaintiff's private life, and concluded that the defendant had infringed upon what is called the right of privacy, thus approving that the right of privacy is recognized in the laws in Japan. As the judge stated:

> The idea of individual dignity, which is one of the fundamental principals in modern law and stands under the *Constitution of Japan*, is ensured only after mutual personality is respected and a person's own self is protected from unjustifiable interference; therefore, it goes without saying that it is not permitted to publish the private matters of others without justifiable reason.[234]

The judge defined that the right of privacy is the right to have one's private life not exposed to the public without permission. He provided three standards of judgment to assess whether or not a publication constitutes as invasion of privacy: firstly, whether there is a risk that others would recognize that the publication discloses a fact about private life or something like a fact; secondly, whether ordinary people would dislike having such a fact disclosed to the public; and thirdly, whether the fact would not already be known by ordinary people, and the person about whom the fact is disclosed would feel uncomfortable and anxious.

The most notable aspects of this judgement are that the right to have one's private matters not revealed was recognized as one of the personal rights, and that the ultimate source of the right was based on the idea of individual dignity of Article 13 of the *Constitution of Japan*.

---

[234] *Utage no ato [After the Banquet]*, *supra* note 230 at 2361. [translated by author]

This theory is seen in another case, *Eros plus Massacre*.[235] The plaintiff was a member of the House of Representatives. Just after she quit her position, a movie titled *Eros plus Massacre* was released, and a character was modeled after her. The plaintiff insisted that the movie invaded her privacy and defamed her, and she asked the court to halt the movie. The Court considered the relationship between the playing of the movie and the protection of the plaintiff's privacy and fame as the relation between freedom of expression and protection for the pursuit of happiness of Article 13. In this case, the court did not support the plaintiff, because they assessed that the case did not match one of the three standards of invasion of privacy which were provided in *After the Banquet*, namely, that the aspects of the plaintiff's past which were described in the movie were already known by ordinary people. The Supreme Court of Japan supported the decision of the Tokyo High Court and rejected the plaintiff's appeal. Although the case did not result in recovery for the invasion of privacy which the plaintiff had insisted on, the court confirmed again that the right of privacy, which is derived from the *Constitution*, means mainly the protection of an individual's secrets, and that relief from the invasion of privacy is granted in tort law.

2.3.3 Right of Privacy between Government and Individual

In the *After the Banquet* case, the right of privacy was recognized only as protection of an individual's secrets. However, the right of privacy was considered as freedom of private life in the *Kyoto League of Student Self-Government* case.[236] At the time of this case, university administrative system reform was being advanced. When the plaintiff led a demonstration march to protest the reform, his photograph was taken by a police officer. The judge of the case stated:

We may say that Article 13 of the *Constitution of Japan* prescribes that the freedom of

---

[235] *Erosu purasu gyakusatsu* [Eros plus Massacre] (1970), 23 Koto Saibansho Minji Hanreishu 172, 246 Hanrei Taimuzu 129 (Tokyo High Court).

[236] *Kyoto fu gakuren* [Kyoto League of Student Self-Government], [1969] 23 Saikou Saibansho Keiji Hanreishu 1625, 242 Hanrei Taimuzu 119 (Grand Bench of Supreme Court).

> individual's private life shall be protected from even national powers such as police authority. As a part of such freedom of private life, any person has the freedom not to have photographs taken of his face or appearance without consent or good reason. Regardless whether it may be called the right of publicity or not, at least, it is a breach of Article 13 of *Constitution of Japan* if a police officer takes a picture of an individual's appearance without good reason, and thus it is not permitted.[237]

Thus, while the judge did not use the phrase "right of privacy" in his judgment, he implied the existence of the right of privacy, and he understood it as freedom of private life.

The recognition that the right of privacy is the freedom of private life is seen another case, *Rejection to be Fingerprinted*.[238] An American rejected to be fingerprinted when he applied for alien registration according to the *Alien Registration Act*,[239] and he insisted that the duty of being fingerprinted infringed upon the freedom of private life as written in Article 13 of the *Constitution of Japan*. The Court stated:

> Fingerprints are patterns on fingertips. They themselves are not information to show the personal life, personality, thought, creed, conscience, etc. However, fingerprints have unequal and unchangeable features. There is a risk that the private life or privacy is damaged depending on the usage of fingerprints. In this sense, the fingerprint imprint system is considered to be closely related to the freedom of private life. Article 13 of the *Constitution* should be interpreted in that the provision is to protect the freedom of private life of individuals against the exercise of state power; therefore, it is interpreted that any individuals have the freedom to not be forced to be fingerprinted without permission, as one of the freedoms of private life, and it is not allowed that organs of the state force individuals to fingerprint without any justifiable reasons, due to a breach of the purpose of such article of the *Constitution*. In addition, it is interpreted that the security of the freedom covers foreign people living in our state.[240]

---

[237] *Ibid* at 1631. [translated by author]

[238] *Shimon ōnatsu kyohi* [Rejection to be Fingerprinted], [1995] 49 Saiko Saibansho Keiji Hanreishu 842, 900 Hanrei Taimuzu 167 (3rd Petty Bench of Supreme Court).

[239] *Gaikokujin toroku ho* [Alien Registration Act], Amendment of Act No. 95 of 1981.

[240] *Shimon ōnatsu kyohi [Rejection to be Fingerprinted]*, *supra* note 238 at 844. [translated by author]

Although the Court judged that the enforcement of fingerprinting has sufficient rationale, that is, to complete the administrative purpose "to establish fair control over aliens residing in Japan by clarifying matters pertaining to their residence and status and through the enforcement of the registration of such aliens",[241] it also recognized that the right of privacy is not only to protect individuals' secrets, but also to allow individuals to decide upon their own private matters, as the freedom of private life.[242]

2.4 Summary: Meaning of the Right of Privacy – the Protected Interests

Section 2 started with the question, "What is privacy?" There is not one simple answer. Robert Post writes, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[243]

The development of the right of privacy in Canada and Japan has been reviewed through section 2.2 and 2.3. In summary, the privacy interests protected should again be considered. The Supreme Court of Canada recognizes that the values of privacy interests are dignity, integrity and autonomy from the *Canadian Charter*.[244] Moreover, three zones of privacy are recognized in the case of *Ruby v. Canada (Solicitor General)*[245] citing La Forest J. in *R. v. Dyment*[246] and a journal of John D.R. Craig.[247] The first of these three zones is the territorial or special zone (for example,

---

[241] *Gaikokujin toroku ho [Alien Registration Act]*, *supra* note 239 Art 1. [translated by Ministry of Justice of Japan]

[242] The idea of self-determination in the right of privacy was viewed in another previous case related to rejection of fingerprinting. The court stated, "Fingerprints are physical features having uniqueness and permanence, and they are the surest way to identify individuals. Therefore, the information of fingerprints should be under the control, with a high degree of freedom, of the principal." *Shimon onatsu kyosei* [Enforcement for fingerprinting], [1986] 1986 Koto Saibansho Keiji Saiban Sokuhoshu 160 at 161. [translated by author]

[243] Robert C Post, "Three Concepts of Privacy" (2001) 89:6 Geo LJ 2087 at 289.

[244] *R. v. Plant*, *supra* note 65 at 293.

[245] *Ruby v. Canada (Solicitor General)*, *supra* note 68 at para 166.

[246] *R v Dyment*, *supra* note 56 at 248.

[247] John DR Craig, "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997) 42:2 McGill LJ 355.

an individual's home), the second is the personal or corporeal zone (for example, body, image, voice and name) and the third is the informational zone (for example, health, sexual orientation, friendships and associations). Similar interests are protected by tort, statutory tort and delict (see section 2.2.2.1, 2.2.2.2 and 2.2.2.3). What are the privacy interests protected in Japan? They are protection of one's private secrets, the freedom of private life, the freedom of decision-making without interference in private matters, and the control of personal information (see section 2.3.1, 2.3.2, and 2.3.3).

Among various opinions concerning the right of privacy, Dr. Fumio Shimpo, a scholar at Keio University and the Commissioner for the International Academic Exchange of Personal Information Protection Commission of Japan, has organized a compelling idea illustrating the right of privacy after investigating the process of developing the right of privacy and secrecy of communication in the constitutional law of 100 countries. According to Shimpo, the right of privacy connotes three types of interests protected by law; these are protection of private territory, protection of autonomy, and protection of personal information.[248] The protection of private territory is to guarantee the ability to maintain a secluded condition from others, which includes protection of sanctuary and protection of repose, and security from unwilling invasion. The protection of autonomy is to maintain individuals' autonomy, which includes protection of personality and protection of intimacy, and secures freedom of individuals to make decisions without arbitrary interference from the government. The protection of personal information is to control personal information appropriately by individuals and to secure personal information from

[248] See Fumio Shimpo, *Puraibashī no kenri no seisei to tenkai* [Creation and Development of the Right to Privacy] (Tokyo: Seibundo, 2000) at 103.

unwilling revelation, which includes protection of anonymity and confidentiality. Fig 2-1 roughly illustrates Shimpo's theory.[249]

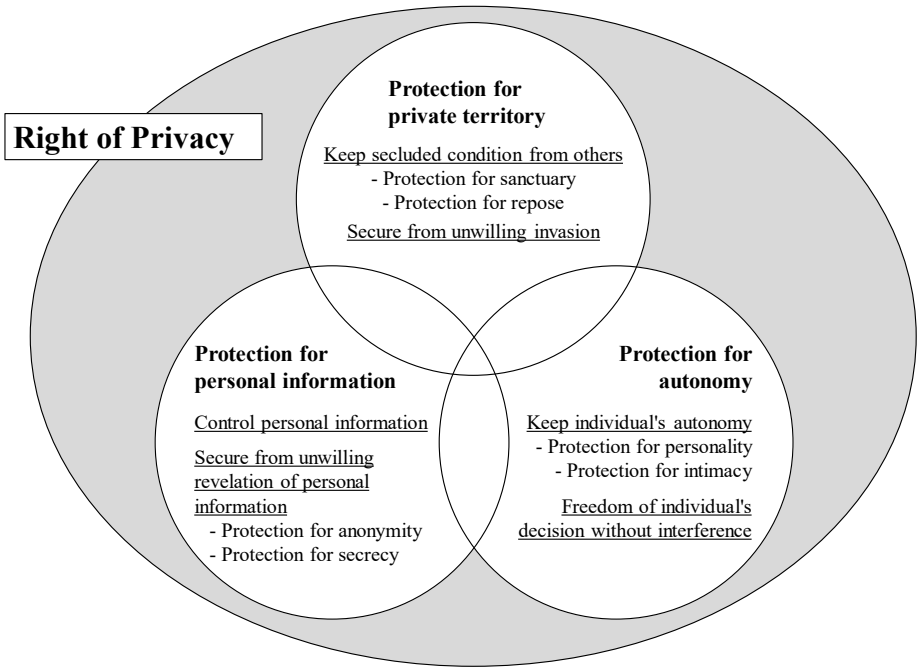

Fig 2-1 The Interests Protected by Law concerning the Right of Privacy (Shimpo's Theory)[250]

Shimpo's theory was created and organized based on the history of worldwide development of the right of privacy and on many judgements and doctrines. Furthermore, his theory is highly compatible with the right of privacy in both Canada and Japan from the perspective of their legislation and judgments (for example, the meaning of the right of privacy and three zones of privacy). This theory has provided a helpful basis for the analysis conducted in this thesis, offering a general outline that can broadly define the scope of privacy and personal information protection interests, and distinguish between their respective spheres, which will be further discussed later in this thesis.

---

[249] Strictly speaking, the right of privacy sometimes comes in opposition to other legal benefits, for example, personal information protection (See Fig 3-1 p. 55)

[250] See Shimpo, *supra* note 248 at 103.

3 Personal Information Protection in Canada and Japan

The previous section discusses the right of privacy and its interpretation and purpose in general terms. This section shows how Canada and Japan have developed personal information protection, primarily with respect to the legislation in their jurisdictions.

3.1 Initial Stage for Development of Personal Information Protection Internationally

Before addressing the development of personal information protection in Canada and Japan, the earlier step of development of personal information protection at an international level should be reviewed, particularly because of an international agreement, *the Guidelines governing the protection of privacy and transborder flows of personal data* (referred to as the *OECD Guidelines*),[251] which had an effect on Canadian and Japanese personal information protection.

Personal information protection was developed along with the progression of information technology. From the 1960s, computer technology for processing information advanced dramatically.[252] Enormous amounts of personal information could be collected, stored, and efficiently compared and connected. At the same time, problems emerged concerning processing of personal information with computers, for example, the surveillance of the public by the government, and unauthorized use of personal information.[253] However, processing personal information with a computer simplified administrative and business tasks and provided the ability to offer a service quickly to consumers and the public. At that time, the necessity to maintain the protection of personal information and the free flow of information simultaneously was advocated.

---

[251] OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(80)58/FINAL (1980).

[252] See OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Doc No DSTI/ICCP/REG(2010)6/FINAL (2011) at 7.

[253] See Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca NY: Cornell University Press, 2018) at 7.

Therefore, starting around 1970, Western countries began enacting numerous laws for the purpose of protecting personal information. For example, the *Data Protection Act*,[254] the first law in the world for protection of personal information, was established in 1969 in Hessen, Germany.[255] In 1970s in the United States, the *Fair Credit Reporting Act of 1970*,[256] the *Privacy Act of 1974,*[257] and the *Right to Financial Privacy Act of 1978*[258] were enacted in rapid succession. Sweden enacted the *Data Act*[259] in 1973, France enacted *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés*[260] in 1978, and in the same year, Norway enacted the *Personal Data Registers Act of 1978*.[261] Furthermore, over the course of three years from 1977 to 1979, laws to protect personal information were established in Germany,[262] Austria,[263] Denmark[264] and Luxembourg.[265]

Each of these laws was enacted in response to the particular domestic circumstances and affairs of each country. Therefore, their approaches and attitudes towards personal information protection vary. For example, the definition and scope of sensitive personal information differs between countries, and some countries decided that certain personal information protection laws

---

[254] *Datenschutzgesetz* [Data Protection Act], 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, Seite 625.

[255] See Eleni Kosta, *Consent in European Data Protection Law*, Nijhoff Studies in European Union Law (Leiden: Brill, 2013) at 45.

[256] Pub L No 91-508, 84 Stat 1127.

[257] Pub L No 93-579, 88 Stat 1896.

[258] Pub L No 95–630, 92 Stat 3641.

[259] *Datalagen* [Data Act], Svensk Författningssamling 1973:289.

[260] JO, 7 January 1978, 227.

[261] *Lov om personregistre mm av 9 juni 1978* [Personal Data Registers Act of 1978], 1978, Norsk Lovtidend Avd. 1, Nr. 48, 402.

[262] *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung*, 1977, Bundesgesetzblatt Teil I, Nr 7, Seite 201. See Nikolaus Forgó et al, "The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings" in Marcelo Corrales, Mark Fenwick & Nikolaus Forgó, eds, *New Technology, Big Data and the Law* (Singapore: Springer, 2017) 251 at 256.

[263] *Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten*, 1978, Bundesgesetzblatt für die Republik Österrich, Nr 565. See Gloria González-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Germany: Springer, 2014) at 65—66.

[264] Lov om private registre m. v. [Private Registers Act], 8 juni 1978, Lov nr 293. and *Lov om offentlige myndigheders registre* [Public Authorities Registers Act], 8 juni 1978, Lov nr 294.

[265] *Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques*, Journal Officiel du Grand-Duché de Luxembourg, 11 avril 1979, N° 29.

would only pertain to personal information processed electronically by computer.[266] Differences in the legal systems and rules related to personal information protection between countries raised the risk of hampering the free flow of information across borders for governments and international companies.[267] Developed countries became concerned about the possibility of adverse economic consequences due to these differences; as a result, the OECD recognized the importance of maintaining the legal system of personal information protection, and began formulating guidelines to bridge the gaps and ensure consistency across different nations' systems.[268]

In 1978, the Committee for Scientific and Technological Policy in the OECD began meeting to discuss protection of privacy and personal information.[269] Following these discussions, the OECD adapted *the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (henceforth referred to as the *Recommendation*)[270] on September 23rd, 1980. It was the world's first international agreement related to the protection of privacy and personal information.[271] The *Recommendation* requested that OECD member countries adopt laws protecting privacy and personal information and introduce eight principles concerning the protection of privacy and individual liberties into their domestic legislation, including ideas such as personal data collection limitation, safety safeguards, and accountability.[272]

---

[266] OECD, *supra* note 252 at 9.

[267] *Ibid* at 7.

[268] Kaori Ishii, *Kojin jōhō hogohō no rinen to gendaiteki kadai* [Philosophy of Personal Information Protection Law and Contemporary Issues] (Tokyo: Keiso Shobou, 2008) at 301—302.

[269] OECD, *The OECD Privacy Framework* (2013) at 39.

[270] OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(80)58/FINAL (1980).

[271] The Council of Europe (CoE) adopted *Convention 108 on the Automated Processing of Personal Data* on September 17th, 1980. However, it was not made public until the ratification by member nations in 1981. See, OECD, *supra* note 269 at 46.

[272] OECD, *supra* note 251.

The *Recommendation* does not have any legal binding force but has strong political influence.[273] Many countries adopted or changed their domestic legislation to reflect the *OECD Guidelines*. Canada and Japan are among these countries;[274] for example, Canada enacted the *Privacy Act* in 1982 and *PIPEDA* in 2000,[275] and Japan enacted *The Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs*[276] in 1988 and *APPI* in 2003.

3.1.1 Differences between Protection of Privacy and Personal Information Protection

Many countries promulgated legislation concerning privacy and personal information protection between the 1970s and 1990s. The respective pieces of legislation typically have titles such as the Personal Information Protection Act, the Data Act, the Privacy Act, etc. Although the names of the acts are different, even in cases where the name of the act specifically refers to privacy protection, their purpose includes not only privacy protection itself but also personal information protection. For example, the *Privacy Act* of Canada aims to "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."[277] Is privacy protection included in or equivalent to personal information protection? Privacy protection and personal information protection are similar in many respects, but they do have different aspects, for example, the protected object and the purpose of protection.

---

[273] See Haruo Takasaki, "Kojin jōhō hogo ni kakaru hōseido wo meguru EU no jōkyō [EU Situation regarding Legal System for Personal Information Protection]" (2014) 55:12 IPSJ J 1337 at 1338.

[274] See Miguel Bernal-Castillero, *Canada's Federal Privacy Laws* (Ottawa: Library of Parliament, 2013) at 2.

[275] The EU Privacy Directive was also influential to *PIPEDA*. See Stephen Gerard Coughlan et al, *Global reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization* (Ottawa: Law Commission of Canada, 2006) at 12.

[276] *Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu* [Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs], Act No. 95 of 1988.

[277] *Privacy Act*, *supra* note 21 s 2.

Personal information protection certainly contributes to the benefits gained from the right of privacy. Law concerning personal information protection allows individuals to keep secrets and protects information from unauthorised use and attack. Moreover, it gives individuals the right to access their personal information held by governments and companies, and the power to control it by themselves to some extent. However, the scope of personal information protection is limited to personal information, so freedom related to birth control and abortion (mentioned in section 2.3.1), freedom to decide on a place to live (mentioned in section 2.2.1.2) and freedom of private life, such as to autonomously decide to have photographs taken of one's face or to submit fingerprints or not (mentioned in section 2.3.3), are not covered by laws such as *PIPEDA* or *APPI*.

Personal information protection not only safeguards personal information but also has the purpose of facilitating use of personal information. The *Recommendation* of the OECD states that "although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information"[278] and recommends that "Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data."[279] Moreover, the purpose of *PIPEDA* is given on the assumption that "technology increasingly facilitates the circulation and exchange of information"[280] and the purpose of *APPI* is "to protect an individual's rights and interests while considering the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan."[281] In other words, the

---

[278] OECD, *supra* note 270.

[279] *Ibid*.

[280] *PIPEDA*, *supra* note 15 s 3.

[281] *APPI*, *supra* note 13 at Art 1. [translated by Ministry of Justice of Japan]

purpose for protecting personal information includes accelerating the safe and secure use of personal information in society by protecting it, although this purpose sometimes conflicts with the purpose of privacy protection. The following figure (Fig 3-1) visualizes the relationship between privacy and personal information protection.

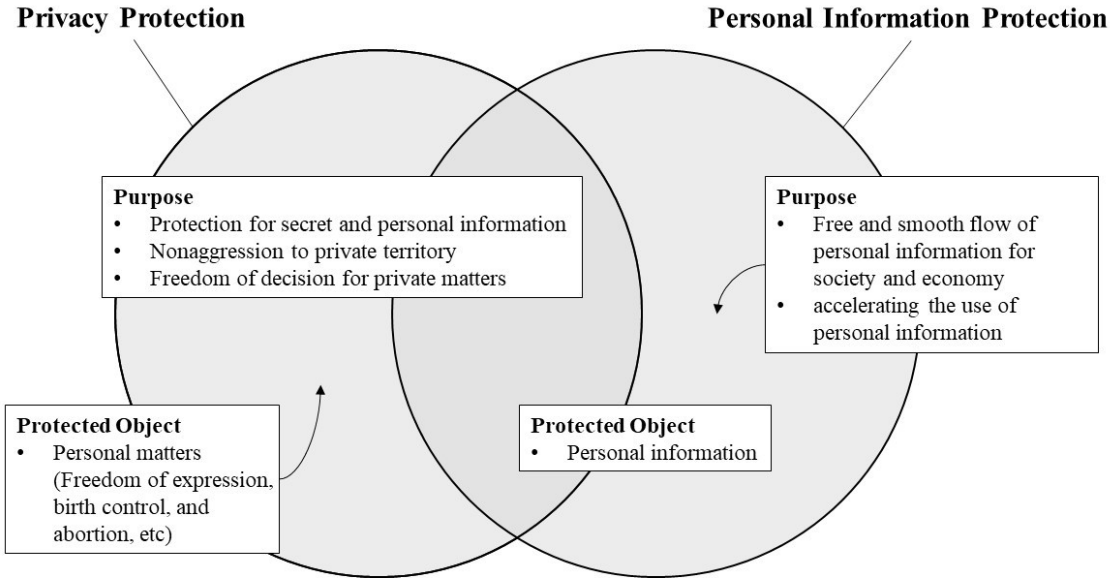

Fig 3-1 Relation between Privacy and Personal Information Protection

3.2 Development of Personal Information Protection in Canada

3.2.1 Personal Information Protection in the Public Sector at the Provincial and Federal Level

In its initial stage, Canada's contemporary data protection regulations pertained to public sector organizations' handling of personal information.[282] After the *OECD Guidelines* were adopted in 1980, although Canada initially abstained from signing the guidelines when they were adopted,[283] the Canadian government moved to enact a law to protect personal information, the *Privacy Act*.

---

[282] Power, *supra* note 158 at 5.

[283] The OECD Privacy Guidelines were adopted by 16 countries, and six countries (Australia, Canada, Iceland, Ireland, Turkey and the U.K.) did not subscribe to them at the time of their adoption. The reason for Canada's abstention has not been stated, but it may have been to avoid moral obligation. The *Recommendation* concerning the *OECD Privacy Guidelines* does not have any legal binding force but has strong political influence (See 3.1). In 1980, Canada did not have a law for personal information protection; therefore, if Canada had agreed the *Recommendation*, it would have meant that Canada was essentially forced to maintain legislation for personal information through the political influence of the OECD agreement. Canada withdrew its

Quebec enacted the legislation combining both access to information and the protection of personal information in the public sector, the *Act respecting access to documents held by public bodies and the protection of personal information*,[284] on June 23, 1982. This law allows the public to access their personal information held by public bodies in Quebec, and regulates the officers and personnel responsible for handling the personal information to ensure that they do so appropriately.[285]

At around the same time, the *Privacy Act* was adopted. It was given Royal Assent on July 7, 1982. While the law is entitled the *Privacy Act*, it mainly protects personal information. It specifies the appropriate collection, use, and disclosure of personal information by the government institutions.[286] The Act demands that government institutions respect privacy principles; at the same time, the Act has another fundamental purpose, which is allowing Canadians to access their personal information held by government institutions.[287] However, there are some exceptions, notably, the government institutions may deny Canadians access to these records if the access would pose a risk to national security or if such access could have an effect on legal matters related to the detection, prevention or suppression of crime and the enforcement of any Canadian law.[288] In these cases, citizens may even be unaware that information has been collected from their record. The decision as to whether to use this exception or not tends to be discretionary.[289]

---

abstention on June 28, 1984, after the *Privacy Act of Canada* was enacted in 1982. See Masao Horibe et al, *OECD puraibashī gaidorain - 30 nen no shinka to mirai* [OECD Privacy Guidelines: Advance for 30 Years and Future] (Tokyo: JIPDEC, 2014).

[284] CQLR c A-2.1.

[285] See Wayne Madsen, *Handbook of Personal Data Protection* (New York: Palgrave Macmillan, 1992) at 165—166.

[286] See *Privacy Act*, *supra* note 21 s 2.

[287] See *Ibid* s 12.

[288] See *Ibid* ss 19–25.

[289] See Caryn Mladen, *Privacy in Canada* (2003) at 6.

3.2.2 Personal Information Protection in the Private Sector at the Provincial Level

In Canada, laws concerning personal information protection in the private sector were initially enacted in Quebec.[290] In 1991, Quebec's *Civil Code* was amended to systematically enhance and include articles for privacy and personal information protection, and also to allow for citizens to control their personal information.[291] These are outlined in Chapter 3, "Respect of Reputation and Privacy," Articles 35 to 40.

Moreover, Quebec enacted an *Act respecting the protection of personal information in the private sector*[292] in 1994. The purpose of this Act is to establish detailed rules regarding the exercise of Articles 35 to 40 of Quebec's *Civil Code*.[293] Therefore, its regulations cover all aspects of the protection of personal information. For example, it requires companies based in Quebec to restrict collection, retention, use and communication of personal information to third parties to the minimum necessary for the purpose, and to offer any persons access to their information.

3.2.3 Personal Information Protection in Soft Law

In 1980, the *OECD Guidelines*[294] were introduced, and they recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties. In response, the Canadian Standards Association developed the *Model Code for the Protection of Personal Information*[295] (henceforth referred to as the *Model Code*) with business, government, and consumer groups in 1996.[296] The *Model Code* was also created

---

[290] See Jennifer Stoddart & Heather Black, "Message from the Privacy Commissioner of Canada" in *Learning from a decade of experience: Québec's Private Sector Privacy Act* (Ottawa: Privacy Commissioner of Canada, 2005).

[291] Paul-Andre Comeau & Andre Ouimet, "Freedom of Information and Privacy: Quebec's Innovative Role in North America" (1995) 80:3 Iowa L Rev 651 at 656—657.

[292] RSQ c P-39.1.

[293] See *Ibid* at Art 1.

[294] OECD, *supra* note 251.

[295] Canadian Standards Association, *Model Code for the Protection of Personal Information,* CAN/CSA-Q830-96.

[296] See Simone Fischer-Hübner, *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms* (Berlin: Springer-Verlag Berlin Heidelberg, 2001) at 29.

with the hope that the European Commission would not impose trade barriers on Canadian companies.[297] In 1995, the *EU Privacy Directive*[298] was introduced. The *EU Privacy Directive* prohibited EU member countries from transferring EU citizens' personal information to non-EU countries if the non-EU countries did not have adequate legislation to protect the privacy and personal information of the individuals. Although Canada had already possessed laws to protect privacy and personal information in the public sector, at that time there had not been any legislations to protect privacy and personal information in the private sector, except in Quebec. The *Model Code* has 10 principles: (1) *Accountability*, (2) *Identifying Purposes*, (3) *Consent*, (4) *Limiting Collection*, (5) *Limiting Use, Disclosure, and Retention*, (6) *Accuracy*, (7) *Safeguards*, (8) *Openness*, (9) *Individual Access*, and (10) *Challenging Compliance*. Fig 3-2 shows the correspondence between the *OECD Guidelines* and the *Model Code*. As above, the *OECD Guidelines* and the *Model Code* are highly compatible.

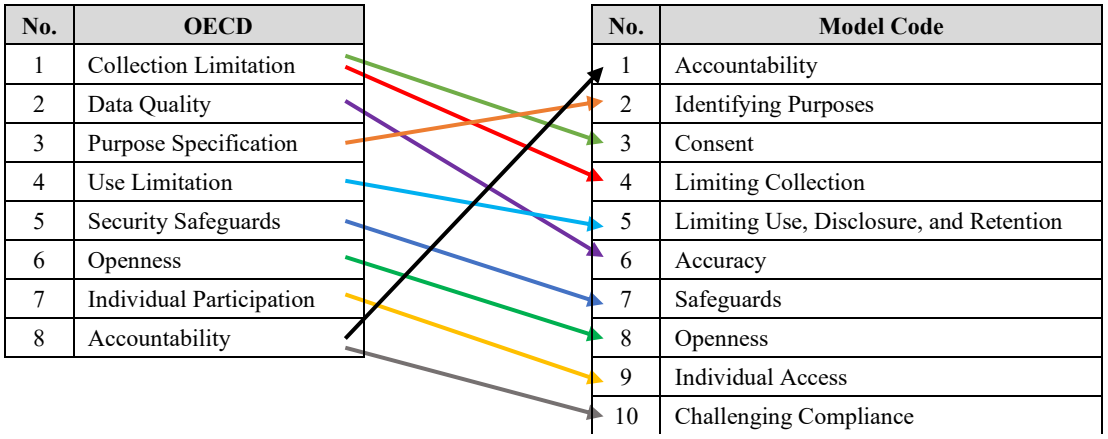

Fig 3-2 Correspondence between the *OECD Guidelines* and the *Model Code*[299]

[297] See Mladen, *supra* note 289 at 20.

[298] EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31.

[299] This Figure is created based on Nigusse and De Decker's report. See Girma Nigusse & Bart De Decker, "Capabilities and Limitations of P3P" (2009) Report CW 539 at 6.

Around this time, Dr. Ann Cavoukian, who was then the Chief Privacy Officer in Ontario, advocated Privacy by Design.[300] The meaning of "privacy" in Privacy by Design includes not only protecting and keeping personal information confidential, but also controlling it.[301] Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start, and Privacy by Design is composed of seven principles: (1) *Proactive not Reactive; Preventative not Remedial*; (2) *Privacy as the Default Setting*; (3) *Privacy Embedded into Design*; (4) *Full Functionality — Positive-Sum, not Zero-Sum*; (5) *End-to-End Security — Full Lifecycle Protection*; (6) *Visibility and Transparency — Keep it Open*; and (7) *Respect for User Privacy — Keep it User-Centric*.[302]

The worldwide spread of Privacy by Design was triggered by the *Resolution on Privacy by Design* [303] during the 32nd International Conference of Data Protection and Privacy Commissioners in October 2010. Privacy by Design was introduced as one of the three main ideas for protecting privacy in the report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*,[304] by the Federal Trade Commission of the United States on March 26, 2012. Moreover, the idea of Privacy by Design was also introduced into Article 25 (Data protection by design and by default) of the *EU General Data Protection Regulation* (*EU GDPR*).[305] In Japan, Privacy by Design was mentioned in the process of revising the *Act on the Protection of Personal Information* (*APPI*).[306] Privacy by Design itself is not

---

[300] See Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario, 2009).

[301] Ann Cavoukian, *Privacy by Design ... Take the Challenge* (Information and Privacy Commissioner of Ontario, 2009) at 17.

[302] See Cavoukian, *supra* note 300 at 2.

[303] International Conference of Data Protection and Privacy & Commissioners, *Resolution on Privacy by Design* (2010).

[304] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (2012).

[305] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1.

[306] *APPI*, *supra* note 8.

legislated because its concept was not constructed for legislation from the outset, nevertheless, Privacy by Design is widely accepted in the world.

3.2.4 Personal Information Protection in the Private Sector at the Federal Level

The *Model Code* was developed at the request of Canadian commercial industries, which were afraid of potential trade barriers that could emerge from the *EU Privacy Directive*. However, because the *Model Code* is voluntary, it was not sufficient for the *EU Privacy Directive*.[307] Therefore, *PIPEDA* was created based on the *Model Code* and passed as legislation on April 13, 2000.[308] *PIPEDA* was enforced in a step-by-step process between 2001 and 2004. The first half of *PIPEDA* concerns the protection of personal information, and the second half concerns electronic documents. The purpose of *PIPEDA* is, according to Section 3, to support and promote private business by protecting personal information. To facilitate both business and the protection of personal information, *PIPEDA* lays down basic rules for processing and management of personal information in the context of business. The legislation applies to every organization using personal information commercially, regardless of whether the organization is physical or online and small or large. However, any organization that collects, uses or discloses personal information for journalistic, artistic or literary purposes is not regulated by *PIPEDA*.[309] In January 2002, the EU agreed that Canadian laws for privacy are adequate according to the *EU Privacy Directive*, after reviewing the implementation of *PIPEDA*.[310]

---

[307] See Ian J Turnbull, *Privacy in the Workplace* (Toronto: CCH Canadian Limited, 2009) at 79.

[308] See Jennifer McClennan & Vadim Schick, "O, Privacy - Canada's Importance in the Development of the International Data Privacy Regime" (2007) 38:3 Geo J Intl L 669 at 683.

[309] See Teresa Scassa & Michael Eugene Deturbide, *Electronic Commerce and Internet Law in Canada* (Toronto, Ontario: CCH Canadian Limited, 2004) at 115.

[310] See Elia Zureik, Lynda Harling Stalker & Emily Smith, *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (Montréal: McGill-Queen's University Press, 2010) at 60.

3.2.5 Reviewing *PIPEDA*

According to section 29 of *PIPEDA*, Part 1 of the Act must be reviewed every 5 years by the government. After its first parliamentary review in 2007, various bills to amend *PIPEDA* were attempted, although not all passed.[311] In 2012, a study on privacy and social media was conducted by the Standing Committee on Access to Information, Privacy, and Ethics (ETHI), and although the study was not for the purpose of a legislative review of *PIPEDA*, matters related to modification of *PIPEDA* were discussed.[312] In 2013, OPC wrote a position paper on *PIPEDA* reform.[313] In 2015, Bill S-4, the *Digital Privacy Act*, received royal assent. This Act amended *PIPEDA*, considering some recommendations from the 2012 ETHI study and the OPC paper. Revisions consisted of allowance of the disclosure of an individual's personal information without their knowledge or consent in special circumstances, introducing new requirements for organizations in cases of a data security breach and creating offenses if organizations did not comply with these obligations, and providing provisions under some circumstances for the Privacy Commissioner to enter compliance agreements with organizations.[314] Furthermore, *Canada's Anti-Spam Legislation* was passed in 2010 and came into force in 2014, which revised *PIPEDA* to make the OPC responsible for addressing violations related to mining and collecting email addresses and illegal collection of personal information through spyware.[315]

---

[311] See House of Commons, *supra* note 20 at 9. See also Bill C–29, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 3rd Sess, 40th Parl, 2010; Bill C–12, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess, 41th Parl, 2011.

[312] See House of Commons, *supra* note 20 at 10. See also House of Commons, *Privacy and Social Media in the Age of Big Data*, Report of the Standing Committee on Access to Information, Privacy and Ethics (2013). See also Office of the Privacy Commissioner of Canada, *The Case for Reforming the Personal Information Protection and Electronic Documents Act* (2013).

[313] See House of Commons, *supra* note 20 at 10. See also Bill S-4, *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*.

[314] House of Commons, *supra* note 20 at 11—12.

[315] *Ibid* at 12.

However, a full statutory review of *PIPEDA* was not produced until February 2018, when ETHI published its Twelfth Report, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*.[316] The report provides 19 recommendations to the Government of Canada, covering aspects such as the meaning of consent, opt-in consent, regulations regarding personal information posted online, rules regarding personal information of minors, frameworks for right to erasure and de-indexing, and powers of the Privacy Commissioner, among others. The report was intended to reflect the rapid development of information technology, the imbalance between the actual use of personal information and the legal system for protecting it, and the need to maintain adequacy with the *EU GDPR*.[317]

The Government of Canada responded to the review in June 2018,[318] generally supporting the recommendations,[319] though expressing uncertainty on a few points such as whether *PIPEDA* would be the best place to address the right to de-indexing and erasure, and how changes might be made to the role of the OPC.[320] The Government expressed that a review of Canada's adequacy standing with respect to the *EU GDPR* should be anticipated by 2020, indicating a need to balance Canada's particular priorities with compliance recommendations.[321]

The importance of re-examining *PIPEDA* was emphasized by a series of recent events. One of these was the 2017 Equifax scandal. In this incident, approximately 19,000 Canadian's personal information which included names, addresses, dates of birth and social insurance numbers

---

316 House of Commons, *supra* note 20.

317 *Ibid*.

318 Canada (Minister of Innovation, Science and Economic Development), *Government Response to the Twelfth Report of The Standing Committee on Access to Information, Privacy And Ethics* (2018).

319 *Ibid* at 2—3.

320 *Ibid* at 4.

321 *Ibid* at 6.

was accessed by an attacker.[322] The second was the 2018 Facebook/Cambridge Analytica scandal. The personal information of certain of Facebook users was disclosed to a third-party application, and it was found that through this disclosure, Facebook had violated *PIPEDA*.[323] Privacy Commissioner Daniel Therrien noted that the Equifax incident prompted the OPC to consider updating rules on transborder data flows, and that both incidents suggested that the accountability principle might not offer adequate protection to Canadians in its present form.[324]

Furthermore, in late 2018, the OPC received over one hundred complaints that Statistics Canada was reported to collect personal financial information from private companies such as a credit bureau and financial institutions without individuals' prior knowledge or consent. The issue was investigated, and the OPC determined that the complaints were not well founded, because as according to *PIPEDA*, if a government institution has "identified its lawful authority to obtain the information",[325] a private organization can legally disclose personal information to the institution without knowledge or consent of an individual.[326] However, the issue raised the awareness of the Canadian personal information use in the Canadian public, and some individuals and organizations expressed disagreement with this provision and demanded that *PIPEDA* and the *Privacy Act* should be revised.[327]

---

[322] Office of the Privacy Commissioner, "PIPEDA Report of Findings #2019-001: Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information", (9 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/> at 2019–001.

[323] Office of the Privacy Commissioner, "PIPEDA Report of Findings #2019-002: Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia", (25 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.

[324] Office of the Privacy Commissioner, "Reforming Canada's privacy laws: Shifting from the whether to the how", (23 May 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-news/speeches/2019/sp-d_20190523/>.

[325] *PIPEDA*, *supra* note 15 s 7(3)(c.1)(iii).

[326] Office of the Privacy Commissioner, "Statistics Canada: Invasive data initiatives should be redesigned with privacy in mind", (9 December 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2018-19/pa_20191209_sc/>.

[327] Office of the Privacy Commissioner, "Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy", (10 December 2019), online: *Office of the Privacy Commissioner*

3.3 Development of Personal Information Protection in Japan

3.3.1 Personal Information Protection by local authorities

Until the *OECD Guidelines* were adopted in Japan, local authorities enacted ordinances related to the protection of privacy and personal information earlier than the central national government. For example, the *Ordinance on the Protection of Personal Information Pertaining to Electronic Data Processing*[328] was enforced in Tokushima City in Tokushima Prefecture on June 28, 1973. The *Ordinance on the Management of Data Processing Systems*[329] was enacted in Kunitachi City in Tokyo in March 1975. However, the object of these ordinances was limited to personal information pertaining to electronic data processing held by local public bodies; therefore, neither personal information processed manually such as personal information written on paper nor personal information processed by private persons was protected. There are several reasons for the establishment of ordinances by local authorities related to the protection of privacy and personal information. Local public bodies hold core information such as certificates of residence and family registers, so with the spread of computers, those ordinances were rapidly needed in advance of regulation by the central national government. Moreover, although the right of privacy had already been recognized by courts, the protection of privacy and personal information by courts only came into effect after the emergence of a problem. For example, a person whose sexual orientation was exposed, contrary to that person's desires, could be compensated with money by law through suing the one who disclosed such information. However, by this point, the person's secret would have already been made public, and this could have irrevocable influence on the person's life, such as

---

<www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/>; Senate of Canada, "Senate banking committee sheds light on Statistics Canada's secretive demand for Canadians' personal banking data", (11 December 2018), online: *Senate of Canada* <sencanada.ca/en/newsroom/banc-senate-banking-committee-statistics-canadas-secretive-demand-canadians-personal-banking-data/>.

328 *Denshi keisanki shori ni kakaru kojin joho nohogo ni kansuru jorei* [Ordinance on the Protection of Personal Information Pertaining to Electronic Data Processing], Promulgated on 28 June, 1973, Promulgated of 28 June, 1973.

329 *Denshi keisan soshiki no unei ni kansuru jorei* [Ordinance on the Management of Data Processing Systems], Promulgated on 26 March, 1975.

in the person's relationships with friends and family. Therefore, rules requiring appropriate handling of personal information were needed.

3.3.2 Privacy and Personal Information Protection in the Public Sector by the Central National Government

After the *OECD Guidelines* were adopted, the Study Group for Protection of Privacy was organized by the Administrative Management Agency in 1981. Dr. Ichiro Kato, a professor in the Faculty of Law at the University of Tokyo at the time, and the study group produced the *Protective Measures for Privacy with Processing Personal Data*.[330] In 1985, the Study Group for Protection of Personal Information in National Administrative Bodies was organized. Shuzo Hayashi, Director-General of the Cabinet Legislation Bureau at the time, and the group wrote the *Concept of Protective Measures for Personal Information Protection in Administrative Bodies*.[331] In December 1986, the Cabinet decided upon the *Implementation Policy for Administrative Reform - Focused on Measures to Be Taken in the Fiscal Year 1987*.[332] It stated, "All things are examined in detail in order to maintain legal measures concerning protection of personal information pertaining to electronic data processing held by administrative organs." The Cabinet submitted the *Bill on the Protection of Personal Information Electronically Processed and Held by Administrative Organs* (as the Cabinet's 82nd Bill)[333] to the 112th Diet, and it passed as the *Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs*[334] on

---

[330] Study Group on Protection of Privacy, *Kojin dēta shori ni tomonau puraibashī hogo taisaku* [Protective Measures for Privacy with Processing Personal Data] (1982).

[331] Study Group for Protection of Personal Information in National Administrative Bodies, *Gyōsei kikan ni okeru kojin jōhō no hogo taisaku no arikata ni tsuite* [Concept of Protective Measures for Personal Information Protection in Administrative Bodies] (1986).

[332] Cabinet, *Shōwa 62 nendo ni kōzubeki sochi wo chūshin to suru gyōsei kaikaku no jisshi hōshin ni tsuite* [Implementation Policy for Administrative Reform - Focused on Measures to Be Taken in the Fiscal Year 1987], Cabinet Decision of December 30, 1986.

[333] Cabinet's 82nd Bill, *Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu an* [Bill on the Protection of Personal Information Electronically Processed and Held by Administrative Organs].

[334] *Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs]*, *supra* note 276.

December 16, 1988. This act was the first law concerning protection of personal information in Japan. Some parts of the act were put into effect on October 1, 1989, and the act was fully implemented on October 1, 1990.

3.3.3 Privacy and Personal Information Protection in Soft Law

Laws for protection of personal information were introduced in the public sectors of both local authorities and the central government; in contrast, there were no laws to protect personal information in the private sectors. In 1988, the Japan Information Processing Development Corporation (at the time),[335] JIPDEC, published the *Guideline for Protection of Personal Information in the Private Sector*.[336] This *JIPDEC Guideline* had no legally binding force; therefore, protection of personal information in the private sector was dependent upon private bodies' voluntary efforts to achieve the necessary improvements on the *JIPDEC Guideline*. Furthermore, as a general guideline in the private sector, the Ministry of International Trade and Industry (at the time), MITI, issued the *Guideline on Protection of Personal Information Pertaining to Electronic Data Processing in the Private Sector* (Ministerial Notification No. 98 of the Ministry of International Trade and Industry)[337] on March 4, 1997.

3.3.4 Certification Systems

With the aim of increasing compliance of private bodies with the *MITI Guideline*, a movement started to develop a new Japanese Industrial Standard (JIS) based on the *MITI Guideline*. The Japan Standards Association developed *Requirements for Compliance Program on Personal Information*

---

[335] JIPDEC was an incorporated foundation for development of key IT technologies and policies, co-managed by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry up until March 31, 2011. After this point, it was changed to a general incorporated foundation and its name to Japan Institute for Promotion of Digital Economy and Community. The abbreviation, JIPDEC, remains the same.

[336] JIPDEC, *Minkan bumon ni okeru kojin jōhō hogo no tameno gaidorain* [Guideline for Protection of Personal Information in the Private Sector] (1988).

[337] Ministry of International Trade and Industry, *Minkan bumon ni okeru denshi keisanki shori ni kakaru kojin jōhō no hogo ni kansuru gaidorain* [Guideline on Protection of Personal Information Pertaining to Electronic Data Processing in the Private Sector] (1997), Ministerial Notification No. 98 of the Ministry of International Trade and Industry.

Protection (JIS Q 15001)[338] on March 20, 1999, which has since been updated and is now entitled *Personal Information Protection Management Systems*. Based on JIS Q 15001, JIPDEC established a certification system called the PrivacyMark System, which started operation as of April 1, 1998. According to the website of PrivacyMark:

> PrivacyMark System assesses private enterprises that maintain systems for the appropriate handling of personal information, and grants the use of PrivacyMark for those who meet certain standards. The System has the following objectives: [to] enhance consumer consciousness toward personal information protection with the display of PrivacyMark visible to the eyes of consumers, and by promoting the appropriate handling of personal information, [to] respond to heightened awareness toward the protection of personal information of consumers, and bestow incentives to gain social credibility on business operators.[339]

As of the end of April 2020, there are 16,424 certified PrivacyMark entities.

3.3.5 Privacy and Personal Information Protection in the Private Sector

On May 30, 2003, the *Act on the Protection of Personal Information* (*APPI*),[340] which covers private enterprises, was enacted and announced. On April 1, 2005, *APPI* began to be enforced. The *APPI* was revised and came into effect on May 30, 2017. All private business enterprises handling personal information are required to comply with the *APPI*.

3.4 Comparative Analysis

Sections 3.2 and 3.3 detailed the process of developing personal information protection in Canada and Japan. In Section 3.4, the process of developing personal information protection is compared between Canada and Japan. The similarities and differences between these processes are outlined,

---

[338] Japanese Industrial Standard (JIS), *Requirements for Compliance Program on Personal Information Protection (JIS Q 15001)* (1999).

[339] JIPDEC, "Outline and Objective | PrivacyMark System", (2018), online: *PrivacyMark System* <privacymark.org/about/outline_and_purpose.html>.

[340] *APPI*, *supra* note 19.

and the rationale for these similarities and differences is considered. For both Canada and Japan, the process of developing personal information protection can be divided into five periods.

(1) First Period: Establishment of the Right of Privacy

The first period marks the establishment of the right of privacy, as discussed in sections 2.2 and 2.3. In Canada, the right of privacy appeared in the *Charter*, common law tort, statutory tort and delict. In Japan, the right of privacy is drawn out of Article 13 of the *Constitution of Japan* and article 709 of *Civil Code of Japan*.

(2) Second Period: Laws for Protecting Personal Information in the Public Sector were Enacted

The second period is when laws for protecting personal information in the public sector were enacted. In both Canada and Japan, some laws for protecting personal information were enacted at the provincial or local level earlier than personal information protection laws were implemented at the federal or central government level.

However, each country has its own reasons why provinces and local authorities were the first to enact such laws. In the case of Japan, local authorities have databases containing certificates of residence and family registers, and deal with citizens' personal information more frequently than central government ministries and agencies. Furthermore, ordinances can be established more easily by local authorities than at the national level. In the case of Canada, the province of Quebec's politicians placed a high priority on enacting rules for personal information protection, seemingly more so than other provinces and the federal government. Thus, Quebec was the first to establish such laws.[341] In Quebec, laws for the protection of personal information in the public sector were advanced as part of electoral reform. In 1972, the U.S. Watergate scandal marked a turning point

[341] Office of the Privacy Commissioner of Canada & Paul-André Comeau, *Control Authorities: Personal information in the French-speaking world* (2007) at 27.

after which some politicians became interested in both the access to information and the protection of privacy and personal information, which provide the basis of democracy.[342] In the mid-1970s, René Lévesque, the head of the government of Quebec at that time, appointed Robert Burns as the Minister responsible for Electoral Reform. Burns stated: "It would be necessary for a law to stipulate the right of free access to all public documents with the restrictions which are necessary for the security of the state and the private life of individuals."[343] The Study Commission on Access to Information and Protection of Privacy (La Commission d'étude sur l'accès à l'information et la protection de la vie privée) was formed on September 3, 1980.[344] Thanks to the achievements of this commission and the personal support of Minister René Lévesque, the *Act respecting access to documents held by public bodies and the protection of personal information* was passed unanimously.[345]

The background of the Canadian federal and Japanese central governments' enactment of laws for protecting personal information in public sector was the establishment of the *OECD Guidelines*. These guidelines have provided a basis for laws regulating the appropriate use of personal information in many countries, including Canada and Japan, despite not providing any legal force themselves.[346]

In the case of Canada, the *OECD Guidelines* impacted the federal level legislation for protecting personal information in the public sector even though Canada did not initially agree to follow the guidelines. On the other hand, Japan did sign to agree to the guidelines. The document

---

[342] See Rick Perlstein, *Britannica Academic* (20 September 2017), online: < academic-eb-com.proxy3.library.mcgill.ca/levels/collegiate/article/Watergate-scandal/76257 >.

[343] André Larocque, "La réforme électorale. L'héritage démocratique du Premier ministre René Lévesque" in *L'éthique gouvernementale: Cahiers de recherche éthique 21* (Montréal: Fides, 1997) at 339. [translated by author]

[344] *Ibid* at 340.

[345] *Ibid* at 341.

[346] Bernal-Castillero, *supra* note 274 at 2.

published by the Economic Affairs Bureau, of the Ministry of Foreign Affairs of Japan on November 30, 1984 shows the internal and external motivation to enact laws for protecting personal information:

> In our nation, it is the present situation that the consensus for the privacy protection has not been completely formed yet. However, we hope to contribute to future harmonized international development in the field of Information, Computer, Communications Policy. From this view point, our nation thinks that we shall respect the purpose of the *OECD Guidelines* and hopes to make efforts to reflect the guidelines in future domestic policy in a way that is suited to the conditions of Japan.[347]

(3) Third Period: Voluntary Efforts to Protect Personal Information in the Private Sector are Made

The third period is the period when voluntary efforts were made to protect personal information in the private sector. The OECD recommended that the *OECD Guidelines* should be introduced for both the public and the private sectors. Why were laws for protecting personal information in the private sector enacted later than the personal information protection laws for the public sector?

In the case of Japan, Dr. Katsuya Uga, a Justice of the Supreme Court of Japan and an honorary professor at University of Tokyo, has explained that the reason for this delay was that, "legalizing personal information protection was considered from the beginning as a part of movements to secure trust of the government administration. On the other hand, legislation of personal information protection in the private sector required adjustment to balance the relationship with freedom of business."[348] Furthermore, Dr. Shizuo Fujiwara, a professor at Chuo University, has explained that when the Japanese government decided that laws for protecting personal

---

[347] Masao Horibe, "1980 nen OECD puraibashī gaidorain to nihon [OECD Privacy Guidelines in 1980 and Japan]" in *OECD puraibashī gaidorain - 30 nen no shinka to mirai* [OECD Privacy Guidelines: Advance for 30 Years and Future] (Tokyo: JIPDEC, 2014) at 33. [translated by author]

[348] Katsuya Uga, *Kojin jōhō hogohō no chikujō kaisetsu* [Commentary on Personal Information Protection Laws], 6th ed (Tokyo: Yuhikaku, 2018) at 8. [translated by author]

information in the public sector would be enacted first, it judged that legislating personal information protection law in the private sector was premature because the Japanese government and main industrial groups had not sufficiently discussed personal information protection in private sector, and many private companies had not yet prepared for personal information protection legislation.[349]

The reasons for the delay to enshrine laws for the protection of personal information in the private sector in Canada are unclear. However, it can be conjectured that Canada also needed more time to consider the balance between business and personal information protection, as was the case for Japan. Furthermore, according to Karlstad University professor Simone Fischer-Hübner, "Voluntary privacy codes and standards have generally been the preferred approach of Canadian business and industry associations."[350] While Quebec moved quickly to enact legislations for the private sector, the delayed enactment of federal-level personal information protection legislation resulted in some initiatives to protect personal information in the private sector through voluntary actions rather than by legislation, due to a sense of urgency to make rules to regulate private organizations which in various situations had already retained and used large amounts of personal information.

Moreover, for both Canada and Japan, the making of rules related to handling of personal information in the private sector was motivated by a potential trading and economic risk due to the *EU Privacy Directive*,[351] which prohibited transfer of personal information to countries and organizations not achieving sufficient levels of personal information protection.[352]

---

[349] Shizuo Fujiwara, *Chikujō kojinjōhō hogohō* [Annotations to Act on the Protection of Personal Information] (Tokyo: Kobundo, 2003) at 4.

[350] Fischer-Hübner, *supra* note 296 at 29.

[351] EC, *supra* note 298.

[352] See Harumi Shinohara, "JIS Q 15001 kaisei ni itaru keii [The Background for amending JIS Q 15001]" *Information From JADAC and Experts* (July 2018) at 4.

In Canada, voluntary initiatives to protect privacy include Privacy by Design, which was proposed by Dr. Ann Cavoukian.[353] Additionally, the *Model Code* was produced by the Canadian Standards Association. In Japan, JIPDEC and MITI formulated guidelines for the private sector, and the Japan Standards Association made JIS Q 15001. At that time, problems related to leakage of personal information had already occurred; therefore, the development of the certification mark system, PrivacyMark, began to give private companies incentive to voluntarily comply with JIS Q 15001, as it allowed consumers to easily understand that companies obtaining such certification deserved trust to ensure privacy and personal information protection. Although both Japan and Canada initially developed only voluntary initiatives to protect privacy and personal information in the private sector, during this time, the province of Quebec was an exception as it actually did legislate some acts for the private sector. Quebec politicians at the time were very positive towards action for democracy, and their attitudes towards privacy and personal information protection were advanced, as mentioned in the discussion above on the second period. Quebec added some provisions concerning privacy and personal information protection in the *Civil Code* in 1991[354] and passed the *Act respecting the protection of personal information in the private sector* unanimously in 1994.[355] This act was the first law enacted in Canada to protect personal information in the private sector,[356] and it was enacted earlier than *PIPEDA* and the *EU Privacy Guidelines*.

(4) Fourth Period: Laws for Protecting Personal Information in Private Sector are Enacted.

---

[353] See section 3.2.3.

[354] Comeau & Ouimet, *supra* note 291 at 656—657.

[355] *Ibid* at 651.

[356] See Fischer-Hübner, *supra* note 296 at 29.

The fourth period marked the establishment of laws for protecting personal information in the private sector. In Canada, *PIPEDA*, which included the *Model Code*, was enacted in 2000. *PIPEDA* applies to private organizations in all provinces except provinces having legislations deemed substantially similar to *PIPEDA* (these are Alberta, British Colombia, and Quebec). With the establishment of *PIPEDA*, both the public and the private sector had legal systems concerning personal information protection. In Japan, the *Act on the Protection of Personal Information*, *APPI*, was announced in 2003 and came into force in 2005 (*APPI* regulates private companies in all prefectures of Japan). Once *APPI* had come into force, the number of companies obtaining PrivacyMark certification increased dramatically.[357]

(5) Fifth Period: Certification Systems are Implemented.

Finally, the fifth period is when certification systems spread. When the *OECD Guidelines* were amended in 2013, the guidelines stated the importance of management systems. The *EU GDPR*, which was passed on April 14, 2016, also recommended the introduction of certification systems into member states' domestic laws. In Canada, Privacy by Design Certification was launched in 2015. In Japan, certification systems based on JIS Q 15001, such as PrivacyMark, had already been introduced since 1998, and many companies had already been granted certification. Why then did Canada introduce certification systems so much later than Japan? The reason is uncertain, however, it may be due to Canada's decision to include the *Model Code* into *PIPEDA*. Section 5 of *PIPEDA* states that organizations must comply with the obligations of the Schedule 1, which is the *Model Code*. This means that all organizations are essentially mandated to comply with the *Model Code* through *PIPEDA*; thus, Canada did not need to make certification systems. On the other hand, *APPI* in Japan provides only the minimum requirements for protecting personal information, and

[357] JIPDEC, *The PrivacyMark System* (2017) at 3.

anticipates that companies will voluntarily strive to protect personal information at a higher level than *APPI*. Thus, certification systems, which have more strict criteria than needed to comply with national guidelines and reflect the special circumstances of each industrial field, filled a more critical role in Japan than in Canada, and thus were developed earlier. Then why now is Canada moving to promote the spread of certification systems, even though *PIPEDA* has included the *Model Code*? The purpose of the Privacy by Design Certification System reflects that it is important for organizations not only to comply with the law, but also to respect the interests of consumers, which may not be adequately taken into account by the law. Moreover, the *OECD Guidelines* and the *EU GDPR* state that certification systems demonstrate increased transparency of the handling of personal information by organizations. Table 3-1 shows the five periods of the process of developing privacy and personal information protection in Canada and Japan.

Table 3-1 The Five Periods of the Process of Developing Privacy and Personal Information Protection in Canada and Japan

	Canada	Japan
1890		*Civil Code* (1896)
1940		*Constitutional Law* (1940)
1950		
1960		*After the Banquet* case (1964)
	Provincial	
	Privacy Act of British Columbia (1968)	
		Kyoto League of Student Self-Government case (1969)
1970	*Privacy Act* of Manitoba (1970)	Local
		Ordinance on the Protection of Personal Information Pertaining to Electronic Data Processing (Tokushima city: 1973)
	Privacy Act of Saskatchewan (1974)	
	Charter of Human Rights and Freedoms (1975)	
	Human Rights Act (1977)	
1980	*OECD Guidelines*	
	Privacy Act of Newfoundland (1981)	
	Canadian Charter of Rights and Freedoms (1982)	
	Act respecting access to documents held by public bodies and the protection of personal information (1982)	
	Privacy Act (1982)	
		Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs (1988)
		JIPDEC Guideline for Protection of Personal Information in the Private Sector (1988)
1990	*Civil Code* (1991)	
	Act respecting the protection of personal information in the private sector (1994)	
	EU Data Directive	
	Privacy by Design (1995)	
	Model Code for the Protection of Privacy (1996)	
		MITI Guideline on Protection of Personal Information Pertaining to Electronic Data Processing in the Private Sector (1997)
		PrivacyMark (established: 1998)
		JIS Q 15001 (1999)
2000	*Personal Information Protection and Electronic Documents Act* (2000)	
		Act on the Protection of Personal Information (2003)
		PrivacyMark (expanded: 2005)
2010	*OECD Guidelines* (amended: 2013)	
	Privacy by Design Certification (2015)	*Act on the Protection of Personal Information* (amended: 2015)
	EU GDPR (2016)	

1. Green is the first period of establishment of the right of privacy.
2. Blue is the second period when laws for protecting personal information in the public sector are enacted.
3. Yellow is the third period when voluntary efforts to protect personal information in the private sector are made.
4. Red is the fourth period when laws for protecting personal information in private sector are enacted.
5. Purple is the fifth period when certification systems are implemented

4 Comparison of Personal Information Protection Law for the Private Sector between Canada and Japan

4.1 Overview

4.1.1 Canada

As it is written in section 3.2, the legal structure for personal information protection in Canada consists of both federal personal information laws and provincial and territorial personal information laws.[358] The two federal personal information laws are the *Privacy Act* and the *PIPEDA*.[359] There are over 30 provincial and territorial personal information laws in Canada,[360] and each province and territory has its own laws. These federal and provincial and territorial personal information laws can be categorized into three sectors: public, private and health sector.[361]

The *Privacy Act*, as the personal information law for the public sector, applies to government institutions, that is, any department or ministry of state of the Government of Canada, or any body or office listed in the schedule of the Act and Crown corporation.[362] Every province has personal information protection laws to regulate the provincial bodies. Ontario, Saskatchewan and Nova Scotia have distinct statutes or provisions dealing with municipally held personal information.[363]

Organizations which collect, use or disclose personal information in the course of a commercial activity must comply with *PIPEDA*. Alberta, British Columbia and Quebec have laws concerning personal information protection in the private sector which have been deemed

---

[358] See Office of the Privacy Commissioner, *supra* note 16.

[359] *Ibid*.

[360] See Office of the Privacy Commissioner of Canada, "Provincial and territorial privacy laws and oversight", (6 November 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/>.

[361] See Power, *supra* note 158 at 3.

[362] See *Privacy Act*, *supra* note 21 s 3.

[363] *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56., *Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1., and Part XX of *Municipal Government Act*, SNS 1998, c 18, SNS 1998, c 18. See Power, *supra* note 161 at 5, and Office of the Privacy Commissioner of Canada, *supra* note 360.

substantially similar to *PIPEDA*; as a result, it has been permitted that organizations in these provinces be subject to their province's own personal information laws rather than to *PIPEDA*.[364] Nevertheless, when personal information crosses provincial or national borders, all businesses handling personal information are subject to *PIPEDA*.[365] Additionally, federally regulated businesses,[366] such as banks, airlines and telecommunications companies, are always required to comply with *PIPEDA*.

In terms of health sector personal information laws, some provinces, for example, Ontario and New Brunswick, have specific statutes to protect health information.[367] Health information is generally not covered by the private sector law in cases where a province has both private sector and health sector personal information laws.[368] Likewise, provinces that broaden public sector access laws to include health care institutions do not include regulation of health information within these laws.[369] Health information is not considered separately from other personal information at the federal level.[370]

Various sector-specific personal information laws have also been enacted, such as the *Bank of Canada Act*,[371] which applies to federally regulated financial institutions' handling of personal financial information.[372]

---

364 See Valerie D Thompson, *Health and Health Care Delivery in Canada* (Toronto: Elsevier Health Sciences, 2015) at 136.

365 See Office of the Privacy Commissioner, "PIPEDA in brief", (May 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>.

366 See Employment and Social Development, "Federally Regulated Businesses and Industries", (15 April 2020), online: *Canada.ca* <www.canada.ca/en/employment-social-development/programs/employment-equity/regulated-industries.html>.

367 Office of the Privacy Commissioner of Canada, *supra* note 360.

368 See Power, *supra* note 158 at 6.

369 See *Ibid*.

370 See *Ibid*.

371 RSC 1985 c B-2.

372 Office of the Privacy Commissioner, *supra* note 16.

Personal information protection in Canada is also accomplished through additional standards. The first of these is the *Model Code*, which was originally created by the Canadian Standards Association. Although it was initially developed as a voluntary standard, it was later included as a foundational aspect of *PIPEDA*. Thus, it is essentially enforced. A further voluntary initiative has been the recommendation for Privacy by Design Certification. This certification was created and is maintained by the Privacy by Design Centre of Excellence, but it is not formally incorporated into Canadian personal information protection law.

4.1.2 Japan

The legal structure for personal information protection in Japan is composed of four main laws: the *Act on the Protection of Personal Information* (*APPI*),[373] the *Act on the Protection of Personal Information Held by Administrative Organs*,[374] the *Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.*[375] and the ordinances on personal information protection, which are regulated by each local authority.

APPI has seven chapters. The purpose of the *APPI*, definition, overall vision, responsibilities of the local governments, and basic rules which apply to both public and private sectors are written within Chapters 1 through 3 of *APPI*. Chapter 4, 5, 6, and 7 apply principally to the private sector, and they provide obligations for personal information handling business operators (PIHBOs), the responsibilities of the Personal Information Protection Commission (PPC), which supervises PIHBOs, and penalties for breaching these obligations.

---

[373] *APPI*, *supra* note 8.

[374] *Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu* [Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs], Amendment of Act No. 51 of 2016.

[375] *Dokuritsu gyosei hojin to no hoyu suru kojin joho no hogo ni kansuru horitsu* [Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc], Amendment of Act No. 89 of 2016.

The Act on the Protection of Personal Information Held by Administrative Organs is a general law which regulates administrative organs retaining personal information. Most parts of this act are similar to *APPI*, however, there are some notable differences. For example, this act requires administrative organs to provide documentation of a Purpose of Use of Personal Information File[376] and particulars recorded in the Personal Information File to the Minister of Internal Affairs and Communications when they hold personal information (Paragraph (1) of Article 10), and they must prepare and publish a register describing the particulars (Paragraph (1) of Article 11). The idea of the Personal Information File is similar to Personal Information Banks (PIBs)[377] of Canada (see. 4.1.1). Moreover, this act regulates the procedures related to acquisition, disclosure and correction of personal information in detail. These functions are not seen in *APPI*.

The Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. applies to the handling of personal information by independent administrative agencies. It is quite similar to *the Act on the Protection of Personal Information Held by Administrative Organs* although it has some notable differences. For example, *the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.* has a provision to prohibit that independent administrative agencies, etc. acquire personal information by deceit or other improper means (Article 5), while *the Act on the Protection of Personal Information Held by Administrative Organs* does not have such a provision because of the legal promise that their administration must always be fair.

---

[376] Personal Information File means "A collection of information systematically arranged in such a way that specific Retained Personal Information can be retrieved by a computer for achieving the purpose of certain processes" (item (i) of Paragraph (6) of Article 6 of the Protection of Personal Information Held by Administrative Organs).

[377] See Treasury Board of Canada Secretariat, "Standard personal information banks", (20 March 2017), online: *Canada.ca* <www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/information-about-programs-information-holdings/standard-personal-information-banks.html>.

The ordinances on personal information protection are passed by each local government, and they regulate their own governments. Because each local government makes these ordinances, their contents are varied.

The scope of the acts and ordinances mentioned above is the handling of personal information in general fields, so there are also some specific laws, for instance, the *Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures*.[378]

Guidelines concerning *APPI* are published by the PPC and each Ministry. For example, the *Guidelines to the Act on the Protection of Personal Information (General)*[379] were made by the PPC and each Ministry, the *Guidelines for Personal Information Protection in the Financial Field*[380] by the PPC and the Financial Services Agency, and the *Guidelines for Personal Information Protection in the Business Using Individual Genetic Information in the Economy, Trade and Industry Field*[381] by the Ministry of Economy, Trade and Industry. These guidelines indicate the interpretation of *APPI* and the recommendations that those handling personal information should comply with, although they do not have direct legal enforcement.

JIS Q 15001, *Personal Information Protection Management Systems - Requirements*,[382] is the Japanese industrial standard. It provides safer and more appropriate regulations for protecting personal information than legislations such as *APPI*. The requirements of JIS Q 15001 include

---

[378] *Gyosei tetsuzuki ni okeru tokutei no kojin wo shikibetsu suru tame no bango no riyo to ni kansuru horitsu* [Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures], Amendment of Act No. 63 of 2013.

[379] Personal Information Protection Commission, *Kojin jōhō no hogo ni kansuru hōritsu nitsuite nogaidorain (tsūsoku hen)* [Guidelines to the Act on the Protection of Personal Information (General)] (2016).

[380] Personal Information Protection Commission & Financial Services Agency, *Kin-yū bun-ya ni okeru kojin jōhō hogo ni kansuru gaidorain* [Guidelines for Personal Information Protection in the Financial Field] (2017).

[381] Ministry of Economy, Trade and Industry, *Keizai sangyō bun-ya no uchi kojin iden jōhō wo mochiita jigyō bun-ya ni okeru kojin jōhō hogo gaidorain* [Guidelines for Personal Information Protection in the Business Using Individual Genetic Information in the Economy, Trade and Industry Field] (2017).

[382] Japanese Industrial Standard (JIS), *Personal Information Protection Management Systems - Requirements (JIS Q 15001: 2017)* (2017).

making policy, reviewing operation, and accessing managing systems. These requirements are used as the standard of the third party certificate, PrivacyMark.

4.1.3 Note related to Comparison

It is the ambit of this thesis to compare personal information protection in the private sector between Canada and Japan. Therefore, the rest of this section mainly concerns the comparison between *PIPEDA* as a personal protection law in the private sector in Canada and *APPI* as a personal protection law in the private sector in Japan. Although Alberta, British Columbia, and Quebec have laws concerning personal information protection in the private sector, they are considered substantially similar to *PIPEDA*, so this thesis will use *PIPEDA* as the object of comparison.

In the process of comparing personal information protection law for the private sector between Canada and Japan, Canadian and Japanese case law shall be examined. However, it bears mentioning from the outset that in Japan, only a small number of cases related to *APPI* have been decided.[383] There are few possible reasons for this. First of all, Japanese courts have not conceded that individuals may make claims based on *APPI*. *APPI* is one of the administrative laws and applies principally between companies handling personal information and the PPC. In one case,[384] before *APPI* was amended, the Japanese court stated that *APPI* mainly describes the duties of a PIHBO, and does not have any provisions for individuals' claims, for example, the right to request for disclosure and the right to request for correction. Thus, they did not allow for an individual to claim damages based on *APPI*. A European Commission report,[385] written by professor Graham

---

[383] Itakura Yoichiro, "Kojin jōhō hogo hō ihan wo riyū to suru songai baishō seikyū ni kansuru kōsatsu [Consideration on Claims for Damages Due to Violation of Act on the Protection of Personal Information]" (2012) 11 Inf Network L Rev 2.

[384] *Kojin joho hogoho ni motozuku hoyu kojin deta kaiji seikyu* [Disclosure Request for Retained Personal Data according to Act on the Protection of Personal Information], [2007] 1275 Hanrei Taimuzu 323. See, in detail, 4.4.2.2.

[385] Graham Greenleaf, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Country Studies – B5 Japan* (2010).

Greenleaf, pointed out that individuals have limited means by which to take action against violations of *APPI*.[386] The current version of *APPI* has a provision by which a principal may file a lawsuit seeking disclosure, correction, and cessation of utilization etc., in order that *APPI* be aligned with the *OECD Guidelines* and *EU GDPR*,[387] however, as of yet there have been no cases in which an individual has filed a lawsuit according to the provision. Secondly, *APPI* has well-functioning alternative methods for dispute resolution. As Greenleaf has stated, Japanese personal information law is structured relying on relatively informal means of dispute resolution, rather than litigation.[388] If a company breaches a provision of the *APPI*, an accredited personal information protection organization (APIPO) may hold consultation with a concerned individual and request the company's expeditious resolution of the concern, providing guidance or recommendations. Alternatively, the PPC may give guidance and advice and recommendations or orders to rectify. For example, in 2018, 43 APIPOs handled 411 complaints, called for 56 reports, requested submission of referential material in 43 instances, provided 180 instances of guidance, and took 152 other necessary actions, and the PPC called for 444 reports, did 32 onsite inspections and provided 238 instances of guidance and advice. Ultimately, all companies accepted the input of the APIPOs and the PPC.[389] Since thus far most Japanese companies have obeyed the instructions of these entities, such situations have rarely gone to court.[390] The PPC has stated that Japanese companies typically obey such instructions and have rarely gone to court because they believe that

---

[386] As an extra-judicial conciliation method, *APPI* has a provision for settlement of a complaint by an accredited personal information protection organization. See, section 4.4.1.2.

[387] Katsuya Uga et al, *Kojin jōhō hogohō to toriatsukai jitsumu* [Act on the Protection of Personal Information and Practice] (Tokyo: Nihon Horei, 2017).

[388] Greenleaf, *supra* note 383 at 31; Greenleaf criticized that the informal methods of dispute resolution in Japan have resulted in a lack of evidence as to the effectiveness of the actual legislation. However, after *APPI* was amended, the number and status of enforcements and settlements by the Personal Information Protection Commission and accredited personal information protection organizations were made open through an annual report of the Commission.

[389] Personal Information Protection Commission, *Heisei 30 nendo nenji hōkoku* [Annual Report in the Fiscal Year 2018] at 36—42.

[390] Personal Information Protection Commission, *Kojin jōhō hogohō seido kaisei taikō* [Reform Proposals of Act on the Protection of Personal Information] (2019) at 27.

the instructions they receive are not irrational, and the cost of losing trust from consumers is too high.[391]

Within this section, any bracketed reference to a section (abbreviated as "s.") is referring to a provision in the body of *PIPEDA*, and any bracketed reference to a clause (shortened to "cl.") is referring to a provision in Schedule 1 of *PIPEDA*. Also, any bracketed reference to an article (shortened to "art.") is referring to a provision of *APPI* and any bracketed reference to a number (shortened to "n.") is referring to a number of a heading of the *Guidelines to the Act on the Protection of Personal Information (General)* of Japan.

4.2 Concept of Personal Information in Laws

4.2.1 Information about Individual

4.2.1.1 Canada

The definition of personal information within *PIPEDA* is very simple: "personal information means information about an identifiable individual" (s. 2 (1)). Table 4-1 provides examples of personal information under *PIPEDA* based on interpretation by the OPC.[392]

Table 4-1 Examples of Personal Information under *PIPEDA*

Personal information	Instances where *PIPEDA* does not apply.
• age, name, ID numbers, income, ethnic origin, or blood type • opinions, evaluations, comments, social status, or disciplinary actions • employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).	• Personal information handled by federal government organizations listed under the Privacy Act • Provincial or territorial governments and their agents • Business contact information such as an employee's name, title, business address, telephone number or email addresses that is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment or profession • An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list) • An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes

[391] *Ibid*.

[392] See Office of the Privacy Commissioner, *supra* note 365.Canada, *supra* note 322.

According to author Michael Power[393] and the OPC,[394] personal information includes name, home address, telephone number, e-mail address; ancestry, color, race, national or ethnic origin; religion, creed, or religious belief, association or activity; age, sex, sexual orientation, marital status; medical, education or employment history; source of income or financial circumstances, activities or history; DNA, health information, blood type, fingerprints or other hereditary characteristics; identifying numbers such as a social insurance number or driver's license number; personal views or opinions.

According to Michel W Drapeau, case law indicates that the definition of personal information is broad.[395] This breadth can be seen in the case of *Rousseau v. Wyndowe*,[396] Mr. Rousseau requested access to notes made by Dr. Wyndowe during a medical examination, but Dr. Wyndowe declined his request under the assumption that the notes were not subject to right of access under *PIPEDA*. The court sided with Rousseau, noting that medical history is included the definition of personal information in Privacy Act, concluding that since the definition in *PIPEDA* is broader than that in the Privacy Act, it was reasonable to interpret the definition in *PIPEDA* as broad enough to catch medical history and other medical information and, nothing in *PIPEDA* indicates that health information should be excluded from the definition of personal information.[397]

On the other hand, according to the OPC, personal information does not include "[i]nformation that is not about an individual, because the connection with a person is too weak or far-removed (for example, a postal code on its own which covers a wide area with many homes); Information about an organization such as a business; Information that has been rendered anonymous, as long as it is not possible to link that data back to an identifiable person; A person's

---

393 See Power, *supra* note 159; Power, *supra* note 147.

394 See Office of the Privacy Commissioner, *supra* note 16; Canada, *supra* note 17.

395 See Michel W Drapeau & Marc-Aurèle Racicot, *Protection of privacy in the Canadian private and health sectors* (2013) at FED-11.

396 2006 FC 1312.

397 *Ibid* at para 30.

business contact information that an organization collects, uses or discloses for the sole purpose of communicating with that person in relation to their employment, business or profession."[398]

4.2.1.2 Japan

Information related to individuals is defined in detail in *APPI* of Japan. Information related to individuals is categorized into four types: personal information, personal data, retained personal data, and sensitive information. Furthermore, *APPI* defines anonymously processed information which is generated using personal information. These categories are outlined in Fig 4-1.[399]

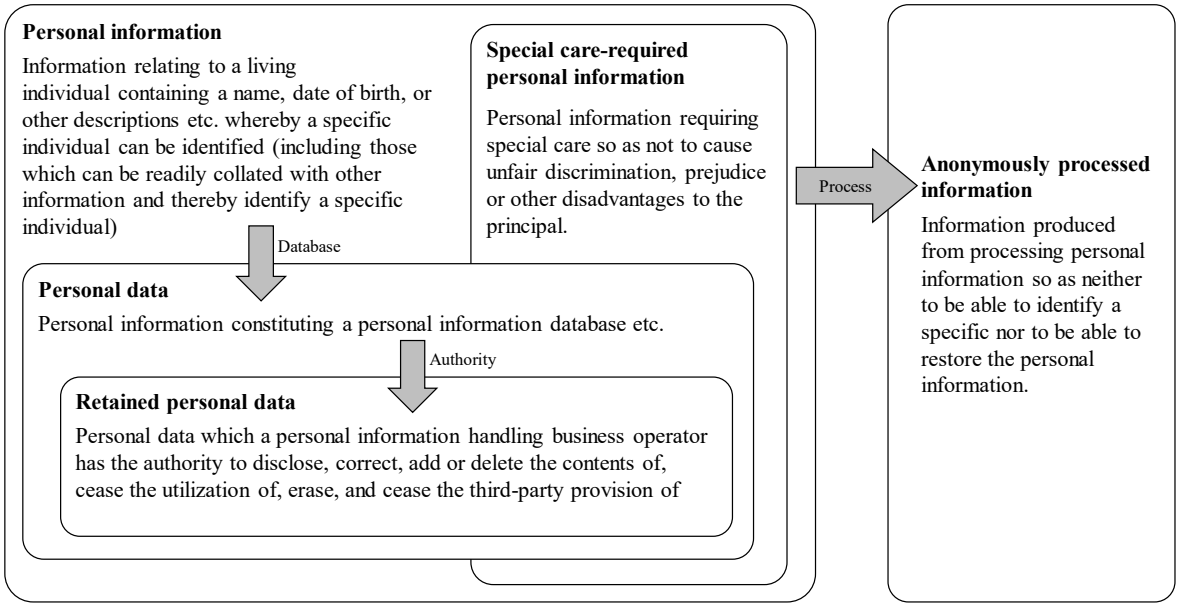

Fig 4-1 Types of Information which are Defined by the Act on the Protection of Personal Information

4.2.1.2.1 Personal information

APPI defines personal information as information relating to a living individual whereby a specific individual can be identified (art. 2 (1)). Information relating to a company or organization is not personal information. Information relating to a deceased person is not personal information, but if

---

[398] Office of the Privacy Commissioner, *supra* note 16.

[399] Fig 4-1 is constructed based on the diagram of Itsuo Sonobe & Shizuo Fujiwara, *Kojin jōhō hogohō no kaisetsu* [Commentary on Personal Information Protection Laws], 2d ed (Tokyo: Gyosei, 2018) at 87.

the information is also related to living family or relatives of the deceased at the same time, the information may be considered information relating to a living individual; thus, it becomes personal information.

There are two types of information which can identify a specific individual. One type is information that can be used to identify a specific individual using one sole piece of information. The other type is information that can be used to identify a specific individual as part of a combination of information. The information that can singularly identify a specific individual may be further subdivided into two types. The first of these is that information that can identify a specific individual by the contents of such information, like name, date of birth, or other descriptions etc. (art. 2 (1) (i)) For example, the information, "Taro Yamada, born on January 15, 1989, lives in Minato-ku of Tokyo," falls within the scope of personal information. Of course, even if information does not include any name, date of birth or address, if a specific individual can be identified by other descriptions included within certain information, such information is also classified as personal information.

The second of these types within the subdivision is information that contains an "individual identification code". An "individual identification code" refers to codes prescribed by cabinet order which involve any characters, letters, numbers, symbols or other data used to form codes (art. 2 (1) (ii)). There are two types of individual identification codes. The first is a character, letter, number, symbol or other code into which a body part feature of a specific individual has been converted in order to be used by computers (art. 2 (2) (i)), for example, DNA, facial appearance, iris' pattern, voiceprint, etc. The other code type is a character, letter, number, symbol or other code which is assigned to an individual (art. 2 (2) (ii)), for instance, a passport number, a basic pension number, a number of a driver's license, a resident record code, a (national) individual number, or a number of health insurance card. An individual identification code is interpreted as a

code such that a specific individual can be identified by the individual identification code alone. In other words, in the case that a company has information which includes only passport numbers, even if the company does not know whose each passport number is, *APPI* concludes that the company has personal information because a passport number is an individual identification code which is prescribed by cabinet order. All individual identification codes are listed in Article 1 of *Cabinet Order to Enforce the Act on the Protection of Personal Information*[400] and Article 3 and 4 of *Enforcement Rules for the Act on the Protection of Personal Information*.[401] Codes which are not listed in the order and the enforcement rule are not individual identification codes. For example, a mobile telephone number, an e-mail address, the number of a credit card, and the identifier of a mobile device such as an IMEI (International Mobile Equipment Identity) are not individual identification codes. However, the fact that those numbers are not individual identification codes does not always mean that they are not personal information, because information which can be readily collated with other information and thereby identify a specific individual is also personal information (art. 2 (1) (i)). Of course, the identifier of a mobile device by itself is not personal information. However, in the case that a company has a database which includes only identifiers of mobile devices, if the company can easily collate this database of identifiers of mobile devices with other databases such as an access log or a consumer database and identify a specific individual by that collation, *APPI* concludes that the information on the database which includes only identifiers of mobile devices corresponds to personal information. Fig 4-2 depicts the Classification chart of personal information of Japan.

---

[400] *Kojin joho no hogo ni kansuru horitsu shiko rei* [Cabinet Order to Enforce the Act on the Protection of Personal Information], Amendment of Cabinet Order No. 324 of 2016.

[401] *Kojin joho no hogo ni kansuru horitsu shiko kisoku* [Enforcement Rules for the Act on the Protection of Personal Information], Rules of the Personal Information Protection Commission No. 3 of 2016.

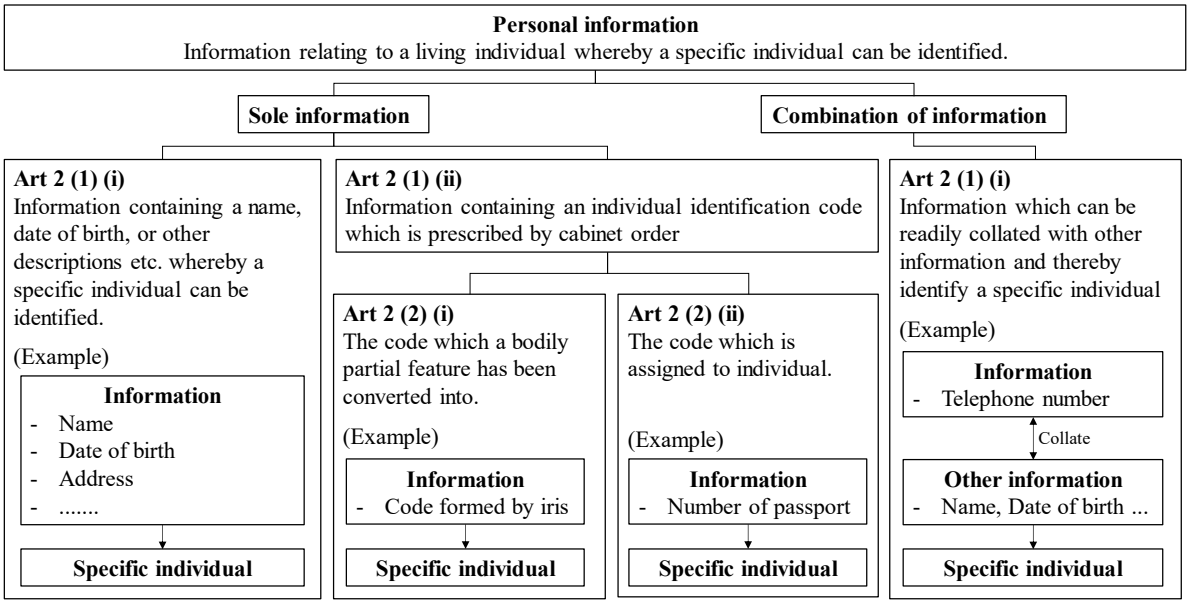

Fig 4-2 Classification Chart of Personal Information of Japan

4.2.1.2.1 Personal information database etc. and personal data

APPI defines "personal information database etc." as a collective body of information comprising personal information "systematically organized so as to be able to search for particular personal information using a computer" (art. 2 (4) (i)) or "prescribed by cabinet order as having been systematically organized so as to be able to easily search for particular personal information." (art. 2 (4) (ii)). For example, an address book as part of an e-mail software comes under the former, and a business card file arranged alphabetically in an office comes under the latter. However, a business card file which contains randomly stored business cards without any regularity or order is a collective body of information comprising personal information but not a personal information database etc. because it is not systematically organized. Also, phone books and social registers on the general market are not considered personal information database etc. according to Article 3 of *Cabinet Order to Enforce the Act on the Protection of Personal Information*. The reason that these books and registers on the market are excluded from personal information database etc. is that they have little possibility of harming an individual's rights and interests and furthermore that although

APPI imposes various duties on a person possessing a personal information database etc. (see Table 4-3, p. 93), it is considered excessive for even an owner of a database which is available for everyone on the general market to have imposed upon them duties to ensure control of the security of the database, such as that the owner must keep their phone book in a strong locker. A person providing a personal information database etc. for use in business is called a "personal information handling business operator" (PIHBO) in *APPI* (art. 2 (5)). *APPI* imposes only upon PIHBOs. Therefore, a person who possesses only personal information but not a personal information database etc. is not subject to *APPI*. Also, personal information constituting a personal information database etc. is called "personal data" in *APPI* (art. 2 (6)).

4.2.1.2.2 Retained Personal Data

In some cases, personal data may be categorized as "retained personal data." Retained personal data refers to "personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of" (art. 2 (7)). For example, if the principal demands of a PIHBO disclosure of retained personal data that can identify him or her, the PIHBO having the authority to disclose has an obligation to disclose the retained personal data related to the principal.

However, there is a possibility that public or other interests would be harmed if the presence or absence of retained personal data is made known, and duties related to retained personal data (disclosure of retained personal data, correction, addition and deletion in regard to the contents of the retained personal data, cessation of utilization and third-party provision and deletion of the retained personal data) would be burdensome for PIHBOs; therefore, *APPI* dictates that two types of personal data are excluded from retained personal data. The first type is personal data that is likely to harm public or other interests (See Table 4-2). The second type is personal data which will be deleted in the near future. It is considered an excessive burden upon PIHBOs to be obligated

to abide by the duty of disclosure and correction etc. of personal data that will be deleted in the near future. Therefore, personal data which will be deleted within six months is not subject to the duties required for retained personal data, in order to decrease the burden upon PIHBOs (See Table 4-2).

Table 4-2 Personal Data Excluded from Retained Personal Data (Article 4 and 5 of Cabinet Order to Enforce the Act on the Protection of Personal Information)

Art.	Category	Example
4 (i)	Personal data which would harm a principal or third party's life, body or fortune	Personal data of a domestic violence sufferer running away from an assailant
4 (ii)	Personal data which would encourage or induce an illegal or unjust act	Personal data of a suspicious person or a vicious complainer
4 (iii)	Personal data which would undermine national security, destroy a trust relationship with a foreign country or international organization, or suffer disadvantage in negotiations with a foreign country or international organization	Personal data of a designer or developer of weapons, facilities, devices, software related to national defense.
4 (iv)	Personal data which would hinder the maintenance of public safety and order such as the prevention, suppression or investigation of a crime	Personal data which includes information related to a bank account used for bank transfer fraud
5	Personal data which is deleted within a period of no longer than six months	Personal data which is deleted within six months

4.2.1.3 Comparative Considerations

When the definitions of information related to individuals are compared between Canada and Japan, there are some notable differences.

First Difference: Business Contact Information

Firstly, business contact information is subject to *APPI* of Japan, but it is exempted in *PIPEDA* of Canada. Why is there this discrepancy? The reason is because of the difference of purpose and meaning of business between *PIPEDA* and *APPI*. The main purpose of *PIPEDA* is to control personal information in the course of commercial activities and to facilitate commerce, and business contact information is essential for trading any products and services.[402] Furthermore, if collection, use, and disclosure of business contact information is restricted "solely for the purpose of communicating or facilitating communication with the individual in relation to their employment,

[402] *PIPEDA*, *supra* note 18 ss 2—3.

business or profession" (s. 4.01), *PIPEDA* considers that there would be little risk of harming the privacy of individuals. On the other hand, the structure of *APPI* does not only consist of sections related to PIHBOs in the private sector but also sections applied to the public and private sectors. Furthermore, although *APPI* regulates PIHBOs, the scope of business consists of activity carried out repeatedly and continuously regardless of whether it is for profit or non-profit. The scope of business within *APPI* includes activities of residents' associations and alumni associations. Thus according to the definition of business in *APPI*, handling of business contact information may in some cases affect the privacy of individuals, and therefore needs to be regulated. The scope of business within *PIPEDA* also applies regardless of whether commercial activity is for profit or non-profit, and *PIPEDA* defines that "commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." (s. 2 (1)). However, most non-profits are not subject to *PIPEDA* because they do not engage in commercial activities, and collecting membership fees, organizing club activities, compiling lists of members' names and addresses, and mailing out newsletters are not considered commercial activities.[403]

Second Difference: Definition of Personal Information

Secondly, personal information within *APPI* is defined in more detail than within *PIPEDA*. Before *APPI* was amended in 2015, the definition of personal information was simpler than it is in the current version of *APPI*. The previous version states:

> The term "personal information" as used in this Act shall mean information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy

[403] See Office of the Privacy Commissioner of Canada, "The Application of PIPEDA to Charitable and Non-Profit Organizations", (June 2019), online: *Office of the Privacy Commissioner of Canada* <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_19/>.

reference to other information and will thereby enable the identification of the specific individual)[404]

The more detailed definition in the current version of *APPI* (see section 4.2.1.2.1) has since arisen from the development of information and communication technologies and the intention of the Cabinet and the industrial field. As information and communication technologies were developed, new utilizations of "personal data"[405] were considered, including the use of Bigdata that had not been foreseen by many businesspeople at the time when *APPI* was initially enacted in 2003. Many businesspeople felt that it was difficult for them to judge which information was not covered under the definition of personal information in *APPI* and was free to use without the regulation of *APPI*. The industrial field considered that the difficulty to judge these matters was a hindrance which caused some businesspeople to hesitate to start a new service with "personal data." The Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) under the Cabinet understood the demands of the industrial field, and it moved to clarify the definition of personal information (see 4.2.3.3 for more background on this clarification).

Third Difference: Multiple Types of Personal Information

Thirdly, *APPI* defines multiple types of personal information. While *PIPEDA* only defines personal information, *APPI* defines personal information, personal data, and retained personal data. The reason that *APPI* has some subtypes of personal information is that *APPI* aims to maintain the balance of protection of personal information by PIHBOs by imposing increased or decreased duties according to the type of personal information they use (In *EU GDPR*, there are cases that

---

[404] *APPI*, *supra* note 19 at art 2 (1).

[405] The meaning of "personal data" enclosed within double quotation marks and used in sections 4.2.1.3 and 4.2.3.3 is not the definition personal data defined in *APPI*. This "personal data" means the information related to a person including that which cannot be clearly judged as information that can identify a specific person. In short, this "personal data" covers a wider range than personal information defined in *APPI*.

duties depend on the type of person (for example, a "controller" or a "processor") using personal information). Table 4-3 shows that the relationship between duty of a PIHBO and the types of personal information. In the case where a PIHBO deals with personal data, the PIHBO has more duties than in the case where it deals only with personal information which is not personal data. One reason for this increased responsibility is that when personal data are compiled in a database, there is a higher risk of a larger leakage of personal data, and such a breach of privacy could be more harmful because the compiled database can connect with information on another database more easily. Furthermore, PIHBOs dealing with retained personal data require more duties than those dealing with personal data. In other words, whether a PIHBO has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of personal data or not determines the increase or decrease of duties of the PIHBO. For example, in the case that an online retailer entrusts data analysis to a consulting firm in order to determine the correlation between products and customer stratum and provides consumer data including purchase history to the firm, if the firm, which only has the authority to analyze data, must cope with requests for disclosure or deletion from consumers, the duties imposed on the firm may be too excessive and irrational.

Table 4-3 The Relationship between Duties of a Personal Information Handling Business Operator and Type of Personal Information[406]

Art.	Duty of personal information handling business operator	Personal information	Personal data	Retained personal data
35	Personal Information Handling Business Operator's Dealing with a Complaint	✓	✓	✓
15	Specifying a Utilization Purpose	✓	✓	✓
16	Restriction due to a Utilization Purpose	✓	✓	✓
17	Proper Acquisition	✓	✓	✓
18	Notification etc. of a Utilization Purpose when Acquiring	✓	✓	✓
19	Assurance etc. about the Accuracy of Data Contents		✓	✓
20	Security Control Action		✓	✓
21	Supervision over Employees		✓	✓
22	Supervision over a Trustee		✓	✓
23	Restriction on Third Party Provision		✓	✓
24	Restriction on Provision to a Third Party in a Foreign Country		✓	✓

[406] See arts 15—35 of *APPI*.

25	Keeping etc. of a Record on a Third-party Provision		✓	✓
26	Confirmation etc. when receiving a Third-party Provision		✓	✓
27	Public Disclosure etc. on Matters relating to Retained Personal Data			✓
28	Disclosure			✓
29	Correction etc.			✓
30	Utilization Cessation etc.			✓
31	Explanation of Reason for denying demand			✓
32	Procedure for Responding to a Demand etc.			✓
33	Fee			✓

4.2.2 Sensitive Information

4.2.2.1 Canada

PIPEDA of Canada does not define sensitive information. However, clause 4.3.4 of Schedule 1 (the *Model Code*) of *PIPEDA* does mention sensitive information, suggesting that whether or not information is sensitive is decided depending on the context. In most cases, information related to medical care and finances would be classified as sensitive information. However, even normal information could become sensitive information, depending on the context. "For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive." (cl. 4.3.4)

4.2.2.2 Japan

APPI clearly defines "special care-required personal information" (art. 2 (3)). In particular, a principal's race, creed, social status, medical history, criminal record, and status of having suffered damage are special care-required personal information. *Guidelines to the Act on the Protection of Personal Information (General)* by the PPC describes special care-required personal information (n. 2-3).

4.2.2.3 Comparative Considerations

Why does *PIPEDA* suggest that sensitive information depends on the context, and avoid defining it? On the other hand, why did *APPI* define special care-required personal information when *APPI* was amended, although it had not defined any sensitive information before?

First of all, *PIPEDA* and *APPI* have slightly different approaches to privacy and personal information protection. Both of them consider whether information is sensitive information or not based on the type of information and the effect on privacy. However, according to *PIPEDA*, the effect on privacy is more meaningful to personal information protection, while *APPI* takes another approach more strictly focusing on the type of information.

Secondly, the decision as to whether sensitive information depends on the context might be affected by the Principle of Consent. *PIPEDA* includes the Principle of Consent, while *APPI* does not have it. Inclusion of this principle means that an organization in Canada needs the consent of individuals when it collects, uses and discloses personal information. Why should the difference between normal personal information and sensitive information be distinguished at all? The reason is that sensitive information must be specially cared for when an organization collects, uses, discloses and safeguards it because if exposed, sensitive information has the risk of leading to unfair discrimination, prejudice, and other detriments to the principal. *PIPEDA* requires an organization to gain consent from individuals when it collects, uses and discloses personal information, whether it is normal personal information or sensitive information (cl. 4.3). Therefore, when an organization requires an individual's consent, the individual can judge how sensitive the information is and whether he or she should provide the information or not. Nevertheless, there are exceptional cases in which an organization can collect, use and disclose personal information without consent (s. 7), and *PIPEDA* requires organizations to get express consent (cl. 4.3.6) and to safeguard information at a higher level of protection (cl. 4.7.2) when the information is likely to be considered sensitive. Although *PIPEDA* does not have a detailed definition of sensitive information, it specifically protects sensitive information based on express consent and the higher level of protection, in a similar way to countries having both the Principle of Consent and the definition of sensitive information.

By contrast, the Japanese *APPI* has not adopted the Principle of Consent. The reason *APPI* does not have this principle may be that Japan – unlike Canada – mainly followed the recommendations of *OECD Guidelines*.[407] The *OECD Guidelines* do not always require consent.[408] *APPI* has only four cases in which consent is required: utilization of personal information other than for intended purposes (art. 16), acquisition of special care-required personal information (art. 17 (2)), provision of personal data to a third party (art. 23), and provision of personal data to a third party in a foreign country (art. 24). Therefore, if a PIHBO informs a principal of, or discloses to the public, the purpose for the utilization of the information, it can acquire personal information without the principal's consent from another person[409] (art. 18 (1)). Also, when a PIHBO provides personal data to a third party, it needs consent of the principal, but if the PIHBO sets rules to stop providing to the third party personal data that can identify the principal upon request of the principal, the PIHBO may provide the said personal data to a third party (art. 23 (2)) if it satisfies some requirements based on the rules of the PPC. The requirements are threefold: firstly, the PIHBO must notify the PPC that it provides personal data to third party without consent, and detail some matters related the provision (art. 23 (2)); secondly, when the PIHBO changes any matters in the provision, it must notify the PPC of the change (art. 23 (3)); and thirdly, the PIHBO must keep a record of a third party provision (art. 25). A PIHBO who receives personal data from the third party needs to confirm the identity of the third party, providing

---

[407] *PIPEDA* also includes the idea of the EU Privacy Directive. See Article 7 of EU Privacy Directive: "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent".

[408] OECD Privacy Guidelines has the Collection Limitation Principle, "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

[409] Theoretically, a personal information handling business operator may be able to acquire personal information from a principal directly without the principal's consent as long as it explicitly states the purpose for data utilization to the principal. However, after the principal is informed of the purpose, if he or she does not consent, he or she may choose not to provide the operator with his or her personal information.

information such as the name or appellation and address of the third party and how the third-party acquired the personal data (art. 26).

In other words, it is possible to have data brokers who act lawfully because the data brokers may collect, use and disclose personal data without consent in a way allowed by *APPI*. If a company uses a law-abiding data broker, sending direct mail is lawful. There are also law-abiding data brokers in Canada, for example, Cornerstone Group of Companies and InfoCanada.[410] According to the record of the OPC these data brokers make lists based on the personal information that *PIPEDA* allows them to collect, use and disclose without consent, for example, the information that is publicly available and is specified by the regulations (s. 7), and they use and disclose these lists as business.[411] Moreover, the data brokers recognize that the lists are subject to *PIPEDA* and insist that they comply with *PIPEDA*.[412]

A third reason that Japan introduced and defined in detail the idea of special care-required personal information when *APPI* was amended is that Japan intended that *APPI* would become an adequate legislation according to the *EU GDPR*.[413] In such a case, transfer of personal information between the EU and Japan would be able to proceed freely. The *EU GDPR* requires that member states should have rules to appropriately protect sensitive information.[414] In response, *APPI* added protection for sensitive information, as special care-required personal information, as there had not been any rules related to sensitive information in the prior version.[415]

---

[410] Office of the Privacy Commissioner, *Data Brokers: A Look at the Canadian and American Landscape* (2014) at 7.

[411] *Ibid* at 7—8.

[412] *Ibid*.

[413] Soichiro Fujiwara, Hironobu Tsukamoto & Akemi Suzuki, *Nichibeiō kojin jōhō hogo dēta purotekushon no kokusai jitsumu* [International Practice of Personal Information Protection and Data Protection in Japan, the U.S. and EU], Oki Mori, ed. (Tokyo: Shojihoumu, 2017) at 12.

[414] EC, *supra* note 305 at art 9.

[415] Hiroshi Miyake & Ikuko Komachiya, *Kojin jōhō hogo hō no hōritsu sōdan* [Legal Counseling for Personal Information Protection] (Tokyo: Seirin Shoin, 2017) at 124.

4.2.3 Anonymously Processed Information

Nowadays, because of the development of information and communication technology and artificial intelligence, de-identified or anonymized personal information can be provided to facilitate business, decreasing the risk of privacy breaches. There are now many instances where anonymized personal information is used. One example is the service providing more detailed traffic jam prediction and weather information on roads, which is based on probe information collected from car navigation systems and includes the history of positions of driving cars. Other examples include the development of drug discovery and clinical research based on medical information retained by health care centers and medical institutions, and the creation of new services and innovations using the history of purchases from loyalty cards and the loading history from IC card train passes. Such data are used by multiple companies regardless of industrial sector.[416]

4.2.3.1 Canada

The OPC has not yet announced its official view on whether organizations can de-identify personal information without individuals' consent and then freely use and disclose the de-identified information.

In 2015, the OPC decided on four privacy priorities that it would primarily seek to address through 2020. These four points are the Economics of personal information, Government surveillance, Reputation and privacy, and the Body as information.[417] As of 2019, the Privacy Commissioner has stated that much has been accomplished so far.[418] Among various actions, under

---

[416] Personal Information Protection Commission, "Tokumei kakō jōhō [Anonymously Processed Information]", (10 February 2019), online: *Personal Information Protection Commission* <https://www.ppc.go.jp/personalinfo/tokumeikakouInfo/>.

[417] Office of the Privacy Commissioner, "Consultation on consent under PIPEDA", (24 May 2018), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.

[418] Office of the Privacy Commissioner, "2019-20 Departmental Plan", (11 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2019-2020/dp_2019-20/>.

the Economics of personal information priority, the OPC published a discussion paper exploring potential enhancements to consent[419] including de-identification, with the goal of receiving opinions on the paper from various fields. There were 51 replies submitted in response to the discussion paper. For instance, "several business submissions, and some submissions from the legal community, argued that de-identified information is not personal information and thus does not fall within *PIPEDA*'s framework, and that consent is therefore not required,"[420] and the Information Technology Association of Canada sought "recognition from the OPC that the process of anonymizing/de-identifying personal information is not a "use""[421]. This means that although *PIPEDA* requires organizations to obtain consent from individuals in advance when the organizations use personal information other than for intended purposes, if anonymizing/de-identifying personal information is not considered as "use" in *PIPEDA*, the organizations can anonymize and de-identify any personal information without consent and then can freely use, disclose and sell the anonymized or de-identified information without consent because the anonymized or de-identified information is not personal information and is not subject to *PIPEDA*. In a report published on May 2018, the OPC wrote:

> we intend to issue guidance on de-identification... The guidance will help organizations assess and reduce risk of re-identification to a sufficiently low level where it may reasonably be used without consent... We encourage Parliament to examine this emerging issue, which has the potential to provide the flexibility needed to achieve a better balance between

---

[419] Office of the Privacy Commissioner, *Consent and privacy - A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (2016).

[420] Office of the Privacy Commissioner, "Overview of Consent Submissions", (5 October 2016), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_intro/>.

[421] Office of the Privacy Commissioner, "Submission: Modernizing Consent and Privacy in PIPEDA", (5 October 2016), online: *Office of the Privacy Commissioner of* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_35/>.

privacy protection and economic value of data.[422]

However, the OPC has not issued guidance on this matter.

4.2.3.2 Japan

The idea of "anonymously processed information" was added to *APPI* when it was amended in 2015. Anonymously processed information means information produced from processing personal information so as neither to be able to identify a specific individual nor to be able to restore the personal information (art. 2 (8)). A collective body of information comprising anonymously processed information which has been systematically organized so as to be able to search easily for specific anonymously processed information is called an "anonymously processed information database etc." (art. 2 (10)), and a person who provides an anonymously processed information database etc. for use in business is called an "anonymously processed information handling business operator" (art. 2 (10)).

APPI has established rules related to anonymously processed information. PIHBOs and anonymously processed information handling business operators can freely use anonymously processed information if they comply with the rules of *APPI*.

These rules are classified into two types; the first type is rules for a person who makes anonymously processed information, and the second type is rules for a person who uses anonymously processed information. The duties of a PIHBO who makes anonymously processed information are subdivided into three categories: the duties to produce, the duties to provide, and the duties to control. When a PIHBO produces anonymously processed information, it has three duties involved in production of the information: first of all, it shall process personal information in accordance with standards prescribed by the rules of *APPI* (art. 36 (1)); secondly, it shall prevent

---

[422] Office of the Privacy Commissioner, *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (2017).

the leakage of information relating to a processing method (art. 36 (2)); and thirdly, it shall disclose to the public the categories of information contained in the anonymously processed information (art. 36 (3)). When a PIHBO provides anonymously processed information to third party, it has two duties involved in provision of the information: firstly, it shall disclose to the public the categories of information contained in anonymously processed information and the method of provision to a third party (art. 36 (4)); and secondly, it shall state to the third party that the information is anonymously processed information (art. 36 (4)). When a PIHBO retains anonymously processed information after production, it has two duties involved in controlling the information: firstly, it must not re-identify the information (art. 36 (5)); and secondly, it shall strive to take necessary and appropriate actions for the security control of the anonymously processed information (art. 36 (6)). An anonymously processed information handling business operator is required to uphold the duties to provide and the duties to control.

4.2.3.3 Comparative Considerations

Currently Canada is considering issuing guidance for de-identification of personal information. By contrast, *APPI* already has a structured system to use anonymously processed information. Why did Japan introduce the idea of anonymously processed information earlier than Canada? The reasons are in part due to the intentions of the government and industries, and also due to the occurrence of an incident related to use of anonymously processed information in Japan.

Before *APPI* was amended, there was a legal interpretation that *APPI* might allow for anonymized or de-identified information to be used freely. However, the way that personal information should be anonymized or de-identified in order to freely use it without a major risk to privacy was obscure. In other words, the border between information and personal information was

unclear. The Japanese government thought that using "personal data"[423] with advanced information and communication technology would boost convenience for individuals and would support creation of new businesses and stimulation of existing business. Thus, in 2013 the government instituted the "Study Group on Personal Data" in the IT Strategic Headquarters to discuss the amendment of *APPI*, including resolution of the ambiguous definition of personal information and development of rules related to anonymously processed information.

Around the time that the study group was established, an incident occurred related to use of de-identified information. Passengers of the East Japan Railway Company (JR-East) may buy "Suica", which are IC card train passes that function as electronic money for train use and ride purchases. Every time a possessor of Suica uses it, JR-East stores information such as history of getting on and off the train and purchase history. If the stored information is analyzed, the stations passengers use and the ways they use trains can be recognized. The analyzed information can be used to support not only railroad operation but also local development near the stations and business in various fields. JR-East believed that the stored information could be beneficial for societal development, including for passengers. JR-East sold the stored information to Hitachi, Ltd., which has experience in data analysis, after it had removed names, telephone numbers and purchase history, erased the date from date of birth, and converted the identifier of each IC card to a new identifier which was not able to be used to restore the original identifier. Furthermore, they had a contract prohibiting identification any specific person. However, some legal experts and technologists voiced their concern that if the processed data were continually provided to the third party, a person could be identified through collation of the provided information with other information. Moreover, many users of the IC cards were against this third-party provision, and in

[423] See footnote 405.

fact about 30,000 people requested that JR-East cease to process their personal information and provide the processed information to a third party. After emergence of these concerns, JR-East stopped selling the processed information.[424]

Because of the problems mentioned above, demand in the Study Group meeting for amendment of *APPI* increased for the development of rules to facilitate the appropriate use of anonymized personal information, not only from the industrial field but also from legal experts and technologists.

4.3 Duties of Organizations Holding Personal Information

4.3.1 Overview and Comparative Considerations

In Canada, the main duties of organizations dealing with personal information are written in Schedule 1 of *PIPEDA*, which is the same as the *Model Code* drawn up by the Canadian Standards Association. Therefore, *PIPEDA* needs to be interpreted based on the history of its development using the CSA's *Model Code*. The case of *Englander v. Telus Communications Inc.*[425] makes reference to this history in its interpretation of Part 1 and Schedule 1 of the Act.[426] The court made note of the inherent challenges of incorporating legislations of the *Model Code* into *PIPEDA*, as expressed by the authors of the Annotated Guide[427] to *PIPEDA*. For example, the *Model Code* was a mix of recommendations and requirements,[428] and the court concluded that "even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this

---

[424] *Suica ni kansuru dēta no shagai heno teikyō ni tsuite chūkan torimatome* [The provision on the outside of data related to Suica: Interim Report], by Expert Committee on the provision on the outside of data related to Suica, Zotero (2014).

[425] 2004 FCA 387.

[426] Michel W Drapeau & Marc-Aurèle Racicot, *Federal Access to Information and Privacy Legislation Annotated 2013* (Toronto: Thomson Reuters Canada Ltd, 2012) at 9–18.

[427] Stephanie Perrin & Canada, *The Personal Information Protection and Electronic Documents Act: an annotated guide* (Toronto: Irwin Law, 2001).

[428] *Englander v. Telus Communications Inc.*, *supra* note 425 at para 44.

legislation, the Court must strike a balance between two competing interests. Furthermore, because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction. In these circumstances, flexibility, common sense and pragmatism will best guide the Court."[429]

In Japan, the main duties of PIHBOs are outlined from Article 15 to Article 35 (see Table 4-3). These articles are complemented by the *Cabinet Order to Enforce the Act on the Protection of Personal Information*, the *Enforcement Rules for the Act on the Protection of Personal Information*, and the *Guidelines to the Act on the Protection of Personal Information (General)*.Table 4-4 shows the corresponding relationship of duties for organizations having personal information between *PIPEDA* and *APPI* from the standpoint of *PIPEDA*, and Table 4-5 shows the corresponding relationship of duties for organizations having personal information between *PIPEDA* and *APPI* from the standpoint of *APPI*. As the result of comparing the duties required by these two laws, it can be observed that the two countries impose fairly similar duties, although there are some modest differentials. The reason for their similarity is that both Canada and Japan referred to the *OECD Guidelines* when they enacted these legislations. On the other hand, differences arise due to the fact that Canada introduced ideas of the *EU Privacy Directive*.

As showing Table 4-4 and Table 4-5, each country's law has some unique points. These points are explained within the following sections. It is helpful for Canadian and Japanese companies to recognize these points when they do business in the other respective markets. When Japanese companies advance into the Canadian market, they must ensure that they make provisions to comply with the unique Canadian duties described in section 4.3.2, and likewise for Canadian companies with respect to the unique Japanese duties described in section 4.3.3. For example, *APPI* does not have a provision of the withdrawal of consent (see section 4.3.2.3), so a Japanese company

[429] *Ibid* at para 46.

working in a Canadian market should include this provision within its privacy policy. On the other hand, the company must be careful about expecting that it could implement unique Japanese duties in Canada or another country. For example, in Japan, if a company satisfies some requirements, it may provide personal information to a third party without consent of the individuals, but there is no such provision in Canada.

Table 4-4 Table of Corresponding Relationship of Duties for Organizations Having Personal Information between in *PIPEDA* and *APPI* (from the Standpoint of *PIPEDA*)

PIPEDA	APPI
Principle 1 — Accountability	
Shall designate a person having responsibility for principals of personal information protection (4.1)	art. 20; n. 8-3 (1)
Accountability of privacy officer (4.1.1)	-
Shall disclose the information of the person having responsibility for principals (4.1.2)	art. 27 (1)
Shall supervise a third party (cl. 4.1.3)	art. 22
Shall implement policies and practices (Accountability for Safeguards, respond to complaints, training staff, and developing privacy policies) (4.1.4)	art. 20; n. 8-1, 8-2; art. 35 (1), (2); n. 3-6
Principle 2 — Identifying Purposes	
Shall identify the purposes for collecting personal information (4.2)	art. 15 (1)
Shall document the identified purposes (4.2.1)	art. 18 (1), (2)
Determination of the information collected for purposes (4.2.2)	-
Shall specify the identified purposes (4.2.3)	art. 18 (1)
Shall identify the new purpose (4.2.4)	art. 15 (2), 18 (3)
Should explain the purposes for which the information is being collected (4.2.5)	art. 18 (2)
Linkage between Identifying Purposes principle and other principles (4.2.6)	-
Principle 3 - Consent	
Shall obtain consent of individual (4.3)	None (opt-out methods)
Under certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. (4.3)	art. 17 (2), 27 (3)
Shall obtain consent for collection and disclosure (4.3.1)	art. 23 (1) (Only disclosure)
Shall make an effort to let individual know the purpose (4.3.2)	art. 27 (1), (2)
Do not require an individual to consent, as a condition of the supply of a product or service, beyond that required to fulfil the explicitly specified, and legitimate purposes. (4.3.3)	art. 16 (1), 17 (1)
Shall take into account the sensitivity of the information for obtaining consent (4.3.4)	art. 17 (2)
Do not obtain consent through deception (4.3.5)	art. 17 (1)
Should seek express consent for sensitive information (4.3.6)	art. 17 (2)
Examples to obtain consent (4.3.7)	-
Shall inform the individual of the implications of withdrawal (4.3.8)	None (art. 29 (1), 30 (1))
Principle 4 — Limiting Collection	
Shall collect personal information within only identified purposes (4.4)	art. 16 (1)
Shall collect personal information by fair and lawful means (4.4)	art. 17 (1)
Do not collect personal information indiscriminately (4.4.1)	art. 17 (1)
Shall limit the amount and the type of information to what is required within the identified purposes (4.4.1)	art. 16 (1)
Shall specify the type of information collected (4.4.1)	None (only disclosure, n. 8-3 (3))
Explanation of fair and lawful means (4.4.2)	-
Linkage between Limiting Collection principle and other principles (4.4.3)	-
Principle 5 —Limiting Use, Disclosure, and Retention	
Do not use or disclose information other than for the identified purposes. (4.5)	art. 16 (1)
Shall retain personal information for as long as is necessary for purposes (4.5)	art. 19
Shall document any new purpose for the use of personal information (See, 4.2.1) (4.5.1)	art. 18 (3)

PIPEDA	APPI
Should develop guidelines including minimum and maximum retention periods. (4.5.2)	art. 19; n. 3-3-1
Shall retain personal information used to make a decision about an individual long enough to allow the individual access (4.5.2)	art. 19; n. 3-3-1
Should destroy unnecessary personal information. (4.5.3)	art. 19
Shall develop guidelines to govern the destruction of personal information (4.5.3)	art. 20; n. 8-3 (2)
Linkage between Limiting Use, Disclosure, and Retention principle and other principles (4.5.4)	-
Principle 6 — Accuracy	
Shall keep personal information accurate, complete, and up-to-date (4.6)	art. 19
Shall keep personal information accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about an individual (4.6.1)	art. 19
Do not routinely update personal information other than for fulfilling the purposes (4.6.2)	art. 19
Should keep personal information generally accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out (4.6.3)	art. 19
Principle 7 — Safeguards	
Shall protect personal information by security safeguards (4.7)	art. 20
Shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification regardless of the format (4.7.1)	art. 20
Should safeguard sensitive information by a higher level of protection (4.7.2)	art. 20
Example of protection methods (4.7.3)	-
Shall make their employees aware of the importance of maintaining the confidentiality of personal information (4.7.4)	art. 21
Shall take care in the disposal or destruction of personal information to prevent unauthorized access (4.7.5)	art. 20; n. 8-5 (4)
Principle 8 — Openness	
Shall make known to individuals specific information about its policies and practices relating to the management of personal information (4.8)	art. 35 (2); n. 3-6
Shall make known the policies and practices in a way which is understandable and make it easy for individuals to acquire (4.8.1)	art. 35 (2); n. 3-6
Shall include the policies with the contact information of the privacy officer, the means of gaining access to personal information, the description of the type of personal information held by the organization etc. (4.8.2)	art. 27 (1), (2); n. 3-5-1; art. 35 (2); n. 3-6
Examples of making information on the policies available in variety of ways (4.8.3)	-
Principle 9 — Individual Access	
Shall give individuals access to their information (4.9)	art. 28 (1), (2), (3), (4)
Shall inform an individual as to whether or not the organization holds personal information about the individual. (4.9.1)	art. 28 (1), (2), (3)
Should indicate the source of this information. (4.9.1)	art. 28; n. 3-5-2
Shall allow the individual access to this information. (4.9.1)	art. 28 (1)
Shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed (4.9.1)	art. 18, 25 (1), (2), 35
May require individuals to provide sufficient information in order that an organization can provide an account of their personal information (4.9.2)	art. 32 (2)
Should provide an account of third parties to which it has disclosed personal information as specifically as possible. (4.9.3)	art. 25 (1), (2)
Shall provide a list of organizations to which it may have disclosed information when it is not possible to provide a list of the organizations to which it may have disclosed information about the individual. (4.9.3)	art. 25 (1), (2) (must provide a list)
Shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual (4.9.4)	art. 28 (2), 33 (1), (2)
Shall provide the requested information in an understandable form. (4.9.4)	art. 28 (2), n. 3-5-2
Shall amend the information as required. Amendment involves the correction, deletion, or addition of information (4.9.5)	art. 29 (1), (2), 30 (1), (2), (3), (4)
(Where appropriate) Shall transmit amended information to third parties having access to the information (4.9.5)	art. 19 (transmit to trustee and a jointly utilizing person)
Shall record the substance of any unresolved challenge when the challenge is not resolved to the satisfaction of the individual. (4.9.6)	None (notification of denying demand; art. 28 (3), 29 (3), 30 (5), 31)

PIPEDA	APPI
(When appropriate) Shall transmit the existence of the unresolved challenge to third parties having access to the information (4.9.6)	None (notification of denying demand; art. 28 (3), 29 (3), 30 (5), 31)
Principle 10 — Challenging Compliance	
An individual shall be able to address a challenge concerning compliance with the principles (4.10)	art. 35 (1) (2)
Explanation of privacy officer (See, 4.1.1) (4.10.1)	-
Shall put procedures in place to receive and respond to complaints (4.10.2)	art. 35 (2), 32 (1), (4)
The complaint procedures should be easily accessible and simple to use. (4.10.2)	art. 35 (2); n. 3-6
Shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. (4.10.3)	art. 35 (2); n. 3-6
Shall investigate all complaints. (4.10.4)	art. 35 (1), 29 (3), 30(2) (4)
Shall take appropriate measures including, if necessary, amending its policies and practices. (4.10.4)	art. 35 (1), 29 (3), 30(2) (4)

* The mark (-) means that the point is not comparable as an explanation, not as a duty, and does not necessarily mean that there is no similar duty in *APPI*.

Table 4-5 Table of Corresponding Relationship of Duties for Organizations Having Personal Information between *PIPEDA* and *APPI* (from the Standpoint of *APPI*)

Art	APPI	PIPEDA
15 (1)	Specifying a Utilization Purpose	4.2
(2)	Altering a Utilization Purpose	4.2.4
16 (1)	Restriction due to a Utilization Purpose	4.3.3, 4.4, 4.4.1, 4.5
(2)	Restriction due to a Utilization Purpose in case of merger	
(3)	Exceptions of Restriction due to a Utilization Purpose	4.2.4
17 (1)	Proper Acquisition	4.3.3, 4.3.5, 4.4, 4.4.1
(2)	Acquisition for Special Care-required Personal Information	4.3, 4.3.4, 4.3.6
18 (1)	Notification etc. of a Utilization Purpose when Acquiring	4.2.1, 4.2.3
(2)	State of a Utilization Purpose when Acquiring in a Written Contract or Other Document	4.2.1, 4.2.5
(3)	Duty to Inform a Principal of or Disclose to the Public a Post-altered Utilization Purpose	4.2.4, 4.5.1
(4)	Exceptions of Notification etc. of a Utilization Purpose when Acquiring	4.1 Note
19	Assurance etc. about the Accuracy of Data Contents	4.5, 4.5.2, 4.5.3, 4.6, 4.6.1, 4.6.2, 4.6.3
20	Security Control Action	4.1, 4.1.4, 4.7, 4.7.1, 4.7.2, 4.7.5
21	Supervision over Employees	4.7.4
22	Supervision over a Trustee	4.1.3
23 (1)	Restriction on Third Party Provision	4.3.1
(2)	Third Party Provision based on Opt-out Method	None
(3)	Altering Matters informed by Opt-out Method	None
(4)	Disclosure to the Public altered Matters by the Personal Information Protection Commission	None
(5)	Exceptions of Third Party	None
(6)	Altering Matters related to Joint Utilization	None
24	Restriction on Provision to a Third Party in a Foreign Country	4.1.3
25 (1)	Keeping etc. of a Record on a Third-party Provision	4.9.1, 4.9.3
(2)	Retention Period of the Provision Record	4.9.1, 4.9.3
26 (1)	Confirmation etc. when Receiving a Third-party Provision	None
(2)	Prohibition for Deception on Matters relating to the Confirmation	None
(3)	Keeping etc. of a Record related to Information received from a Third Party	None
(4)	Retention Period of the Receipt Record	None
27 (1)	Public Disclosure etc. on Matters relating to Retained Personal Data	4.1.2, 4.3.2, 4.8.2
(2)	Request by a Principal to be Informed of a Utilization Purpose of Retained Personal Data	4.3.2, 4.8.2
(3)	Notification of Denial for Request of the Utilization Purpose of Retained Personal Data	4.3
28 (1)	Demand for Disclosure	4.9, 4.9.1
(2)	Exemption of Duty for Disclosure	4.9, 4.9.1, 4.9.4
(3)	Notification of Denying Demand for Disclosure	4.9, 4.9.1
(4)	Other Laws related to Disclosure	4.9
29 (1)	Request for Correction etc.	(4.3.8), 4.9.5

Art	APPI	PIPEDA
(2)	Duty for Correction etc.	4.9.5
(3)	Notification of Denying Demand for Correction etc.	4.10.4
30 (1)	Demand for Cessation of Utilization etc.	(4.3.8), 4.9.5
(2)	Duty for Cessation of Utilization etc. and Exemption	4.9.5, 4.10.4
(3)	Demand for ceasing a Third-party Provision	4.9.5
(4)	Duty for ceasing a Third-party Provision and Exemption	4.9.5, 4.10.4
(5)	Notification of Denying Demand for Ceasing Correction etc. and Third-party Provision	
31	Explanation of Reason for Denying a Demand	
32 (1)	Procedure for Responding to a Demand etc. for Disclosure etc.	4.10.2
(2)	Requesting a Principal to Present a Matter Sufficient to Specify Retained Personal Data Subject to the Demand etc.	4.9.2
(3)	A Demand etc. for Disclosure etc. by an Agent	S7 (3) (d.4)
(4)	Consideration of Principal's Burden related to a Demand etc. for Disclosure etc.	4.10.2
33 (1)	Fee	4.9.4
(2)	Consideration for Reasonable Fee	4.9.4
34	Advance Demand	-
35 (1)	Personal Information Handling Business Operator's Dealing with a Complaint	4.1.4, 4.10, 4.10.4
(2)	Establishment of a System Necessary to Achieve a Purpose to Deal with a Complaint.	4.1.4, 4.8, 4.8.1, 4.8.2, 4.10, 4.10.2, 4.10.3

4.3.2 Duties Unique to Canadian Law

4.3.2.1 Accountability of Organization

PIPEDA requires organizations to designate an individual who is accountable for personal information protection (cl. 4.1). *APPI* does not require such designation, but in the Guidelines of *APPI*, a PIHBO shall organize organizational frameworks as systematic security control measures, and one of the examples of organizational frameworks is establishment of a responsible person and clarification of their role and responsibility (n. 8-3 (1)). Also, *PIPEDA* requires organizations to implement policies and practices to give effect to the principles (cl. 4.1.4). *APPI* does not require making of such policies, but the Guidelines of *APPI* explains the importance of establishment of a basic policy on the protection of personal information, and it requires a PIHBO to provide a declaration of compliance with *APPI* and other related legislation and guidelines in the basic policy (n. 8-1 and 8-2).

4.3.2.2 Consent Principle

PIPEDA requires organizations to obtain consent from individuals in principle when it collects, uses and discloses personal information (cl. 4.3). Japan does not have the Principle of Consent (the

reason for this is explained in more detail in 4.2.2.3), but in its place, *APPI* legislates opt-out (art. 18, 23 (2), 25, 26 and 27).

4.3.2.3 Withdrawal of Consent

In *PIPEDA*, an individual may withdraw consent at any time, and organizations shall inform individuals of the implications of withdrawal (cl. 4.3.8). *APPI* does not provide legislation concerning the withdrawal of consent because it does not have the Principle of Consent. However, an individual may request that a PIHBO delete, erase, or cease the utilization or the third-party provision of their retained personal data. These requests have almost same effect as *PIPEDA*'s legislation.

4.3.2.4 Specification of Category of Collected Data

PIPEDA requires that organizations shall specify the type of information collected as part of their information-handling policies and practices (cl. 4.4.1). *APPI* does not require specification of the type of information when a PIHBO collects personal information. However, *APPI* requires PIHBOs to specify the type of information when the PIHBOs provide the collected information to a third party (art. 23 (2)). Why is there a difference in the responsibility of the PIHBO between the collection and the third-party provision in *APPI*? When a PIHBO collects personal information from an individual directly, the individual can understand what type of information is collected because the individual himself gives the personal information. On the other hand, when the PIHBO provides the personal information to a third party, the individual is not aware of which type of information is provided. Thus, when personal information is provided to a third party, *APPI* requires that the PIHBO specify the type of information. However, there are some cases in which an individual does not understand what type of information is collected when the operator collects the information from the individual. For instance, individuals provide their name, date of birth and

sex when they register for a social networking service. They understand that their name, date of birth and sex are collected by the company, but they are not notified that their posting and browsing history are also collected. Therefore, it is better that individuals can easily know what type of information is collected and used. The guidelines of *APPI* require a PIHBO to clarify the type of personal data collected and used in advance (n. 8-3 (3)).

4.3.2.5 Understandable and Alternative Format

PIPEDA requires that an organization shall provide an individual with information in an understandable form if the individual requests that the organization disclose his or her personal information to him or her (cl. 4.9.4). Also, an organization is required to prepare information in an alternative format[430] if an individual with a sensory disability requests it (s. 10). *PIPEDA* prohibits an organization from providing an explanation of information for an individual with information which is written using unintelligible and gibberish wording, or is readable only with a specific software, and it also does not allow an organization to explain to a deaf person his or her personal information by phone. Although *APPI* of Japan does not have such rules, *APPI* also requires a PIHBO to disclose retained personal data if a principal demands the data (art. 28). Although Article 28 only requires the PIHBO to disclose the data to the principal as a duty and does not state the appropriate method of disclosure, if the PIHBO discloses unintelligible or gibberish data, it cannot be interpreted legally that the PIHBO has completed its duty of disclosure. *APPI* permits a PIHBO to deny an individual's request to disclose retained personal data in the case that such disclosure could potentially seriously interfere with the PIHBO implementing its business properly (art. 28 (2) (ii)). However, if a PIHBO refuses to disclose retained personal data in an alternative format pursuant to the provisions of Article 28, paragraph (2), item (ii), such denial is against the spirit of

[430] *Alternative format*, with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information. (s. 2)

the duty of disclosure according to *APPI*, and is not acceptable from the viewpoints of Article 4 of the *Basic Act for Persons with Disabilities*[431] and Article 8 of the *Act for Eliminating Discrimination against Persons with Disabilities*.[432] Thus the PIHBO should prepare the personal information in an alternative format at the request of principal. The guidelines of *APPI* assume that appropriate methods of disclosure can include not only written documentation but also e-mail or telephone, so the guidelines do accept flexible methods.

4.3.2.6 Submitting of Amended, Erased and Added Personal Information to a Third Party

PIPEDA requires that an organization shall amend, delete or add some information to an individual's information by request of the individual, and where appropriate, the amended information shall be transmitted to third parties having access to the information in question (cl. 4.9.5). In Japan, if a PIHBO entrusts, in whole or in part, the handling of personal data to others or uses the personal data jointly with others, the PIHBO needs to transmit amended personal data to others to which it is entrusted or jointly used in order to ensure the personal data contents. However, a PIHBO does not have the duty to transmit the amended information to a third party to which it had provided the information in the past. Also, *PIPEDA* requires an organization to record the substance of any unresolved challenge and transmit the record of the unresolved challenge to third parties having access to the information in question (cl. 4.9.6). *APPI* does not have any rules requiring a PIHBO to record the substance of an unresolved challenge or to transmit such a record to a third party. However, if the PIHBO rejects a request from an individual, the PIHBO shall

---

[431] Article 4 (1): No person may commit an act of discrimination or any other act which violates interests or rights against a person with a disability on the basis of the disability. *Shogaisha kihon ho* [Basic Act for Persons with Disabilities], Amendment of Act No. 90 of 2011Amendment of Act No. 90 of 2011. [translated by Ministry of Justice of Japan]

[432] Article 8 (1): When carrying out its business, a company must not violate the rights or interests of persons with disabilities through disparate and unfair discriminatory treatment on the basis of disability comparing to persons without disability. *Shogai wo riyu to suru sabetsu no kaisho no suishin ni kansuru horitsu* [Act for Eliminating Discrimination against Persons with Disabilities], Act No. 65 of 2013. [translated by Ministry of Justice of Japan]

inform the principal to that effect without delay in order to resolve the problem between the PIHBO and the individual.

4.3.3 Duties Unique to Japanese Law

4.3.3.1 Opt-out

One of the unique elements included in *APPI* of Japan is the opt-out method (art. 23 (2) ~ (6)). If a PIHBO complies with this method as dictated by *APPI*, the PIHBO can disclose personal data to a third party without consent from the principal (see 4.2.2.3). There is no similar method in Canada.

4.3.3.2 Limitation for Disclosure to a Third Party in a Foreign Country

APPI restricts the provision of personal data to a third party in a foreign country (art. 24). This article was newly added to the revised version of *APPI* to deal with the increase in transmission of information including personal data beyond borders, and to satisfy the adequacy requirements of the *EU GDPR*. As mentioned in section 4.3.3.1, *APPI* permits a PIHBO to provide personal data to a third party without an individual's consent if the PIHBO complies with the opt-out method. However, *APPI* does not permit the PIHBO to provide personal data to a third party in a foreign country with the opt-out method. The PIHBO needs to obtain an individual's consent that he or she approves the provision to a third party in a foreign country before the PIHBO transfers the personal data to the third party (art. 24). However, there are two exceptional cases in which the PIHBO can provide personal data to a third party in a foreign country without consent. The first case is that the third party which is provided personal data is placed in a foreign country which is recognized by the PPC as a country having an equivalent personal information protection system to Japan. Any foreign countries having an equivalent personal information protection system to Japan and being recognized as such by the PPC are not subject to the restrictions upon disclosure to a third party in a foreign country in Article 24 of *APPI*. The standard to judge whether or not a country has an equivalent personal information protection system to Japan can be found in Article 11 of

Enforcement Rules for the Act on the Protection of Personal Information.[433] However, the PPC has not yet recognized any countries as having an equivalent personal information protection system to Japan.

The second case is that the third party in a foreign country which is being provided with personal data establishes an appropriate system for personal information protection. The standard dictating whether the third party's system is appropriate or not is recorded in Article 11-2 of *Enforcement Rules for the Act on the Protection of Personal Information*.[434] For example, if the third party or the PIHBO which provides information to the third party has the Certification of APEC CBPR, the standard will be satisfied.

No Canadian acts related to privacy, whether for the public sector or the private sector, prohibit transfer of personal information to other countries.[435] However, *PIPEDA* dictates that, "the organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party" (cl. 4.1.3). Although Canadian acts do not prohibit transfer of personal information to other countries, *PIPEDA* regulates organizations which outsource the processing of information, including to countries outside of Canada. Moreover, there are guidelines for processing personal data across borders.[436]

4.3.3.3 Duty of a Person who Receives Personal Information from a Third Party

APPI imposes three duties on a PIHBO which receives personal data from a third party. The first duty is to confirm the identity of the third party using information such as a name and address, and

---

[433] Article 11 (i): a personal information handling business operator and a person who receives the provision of personal data have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method. [translated by Ministry of Justice of Japan]

[434] Article 11 (ii): a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information. [translated by Ministry of Justice of Japan]

[435] Office of the Privacy Commissioner, "Personal information transferred across borders", (14 December 2018), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/>.

[436] Office of the Privacy Commissioner, *Guidelines for Processing Personal Data Across Borders* (2009).

to confirm how the third party acquired the personal data (art. 26 (1)). The second duty is to keep a record of when it received the provision of personal data and of matters concerning the fulfillment of the first duties (art. 26 (3)). The third duty is to maintain a record (art. 26 (4)).

These requirements were added when *APPI* was amended to confront data brokers trading personal data illegally. Before the amendment, legal experts and consumers had begun to express the need for countermeasures against the potential breach of *APPI* by data brokers.

One incident[437] significantly enhanced the realization of this need. Benesse Corporation is a company devoted to correspondence education as its primary business field. It has the largest share, around 80 per cent, of the market in correspondence education in Japan. In 2014, Benesse customer information was copied without any permission by a worker of the trustee of the company which Benesse had entrusted with system development and operation. The worker sold the list of customers to a data broker, and the list was purchased by software developers, English conversation schools, and tutoring schools through some other data brokers. The list included names, sexes, dates of birth, postal codes, addresses, telephone numbers, e-mail addresses, and even in some records on the list the expected date of birth of an individual's baby. About 216,390,000 pieces of data were leaked in total, and the data included the personal information of over 48,580,000 individuals.[438]

This incident was one of the drivers stimulating the preparation of new duties to counter the illegal trade of personal data.[439] After *APPI* was amended, data brokers were required to check the identity of a person who sells personal data and the channel of acquisition of the personal data (see 4.2.2.3). Because of this duty, data brokers cannot buy personal data that a third party had

---

[437] Benesse Holdings, *Kojin jōhō rōei jiko chōsa iinkai ni yoru chōsa hōkoku* [Report by Personal Information Leakage Incident Investigation Committee] (2014).

[438] See Report by Personal Information Leakage Incident Investigation Committee, *Ibid*.

[439] Miyake & Komachiya, *supra* note 415 at 220.

acquired in an illegal way, and also a PIHBO needs to check with a data broker to ensure that the personal data were legally acquired. These duties, which were uniquely implemented due to the Benesse incident in Japan, are not included within *PIPEDA* of Canada. However, although *PIPEDA* does not mandate the same duties as *APPI*, such as that a receiver of personal information shall check how the personal information be acquired by a data broker and keep a record of the transfer from the data broker to the receiver, Canadian companies which buy personal information from a third party must still comply with some rules.[440]

4.3.3.4 Agent

APPI allows an agent to request that a PIHBO disclose, amend, and cease use of retained personal data etc. instead of a principal (art. 32 (3)). This means that an agent according to the legislation of *APPI* has broader authority than a representative according to *PIPEDA*. *PIPEDA* allows for a legal guardian or a representative to act instead of an individual in some cases, and in such cases the representative must give evidence that they are authorized to act in this capacity.[441] Such representatives may give consent instead of an individual (cl. 4.3.6) and receive the disclosure. Those who may be authorized as representatives are "legal guardians for incapable minors, personal representatives in the administration of a deceased person's estate, and an attorney with relevant power of attorney."[441]

4.3.3.5 Duty of Anonymously Processed Information

APPI of Japan includes duties for dealing with anonymously processed information. The explanation of these duties is found in section 4.2.3.2. Canada has no special rules related to

---

[440] Office of the Privacy Commissioner, *supra* note 410 at 6.

[441] Office of the Privacy Commissioner of Canada, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts", (5 November 2004), 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/>.

anonymized or de-identified information, but OPC is in the process of preparing guidance on de-identification (see 4.2.3.1).

4.4 Securing the Enforceability of Rules

PIPEDA of Canada and *APPI* of Japan have rules and duties which apply to organizations and PIHBOs, and they have systems to secure the enforceability of the rules and duties. The systems to secure the enforceability of rules are subdivided into three classifications: settlement of complaint by party, authority of Commissioner/Commission, and application of penalty. Both *PIPEDA* and *APPI* essentially recommend that an individual and an organization engaged in a private dispute should first attempt to resolve the issue between themselves. If the problems are not settled, the Commissioner can be enlisted to help resolve them, or the organization may be subject to punishment by law.

4.4.1 Settlement of Complaint

4.4.1.1 Settlement of Complaint by Party

4.4.1.1.1 Canada

Organizations in Canada must comply with the 10 principles written in Schedule 1 of *PIPEDA*. Based on these 10 principles, organizations shall consider and deal with any request from an individual in a systematic way if he or she demands that the organization disclose, amend or delete his or her personal information or lodges a complaint. *PIPEDA* prescribes the specific procedure that must be implemented concerning a request for amending etc. Firstly, an individual requests an organization to disclose, amend or delete his or her personal information. in writing (s. 8 (1)). The organization shall respond to the request within thirty days (s. 8 (3)). If the organization refuses to grant the request, it shall inform the individual of the refusal with the rationale (s. 8 (7)). If the individual is not satisfied by the organization's response, he or she can complain to Commissioner.

Section 8 of *PIPEDA* also provides prescriptions for other matters including extension of the time limit (s. 8 (4)) and charging of fees (s. 8 (6)).

4.4.1.1.2 Japan

APPI expresses that a PIHBO shall strive to deal appropriately and promptly with a complaint about the handling of personal information (art. 35 (1)) and endeavor to establish a system necessary to accomplish suitable handling of complaints (art. 35 (2)). However, these rules are not mandatory duties but obligations to make efforts. Therefore, unlike *PIPEDA*, *APPI* does not prescribe the specific procedure concerning the request for amending etc. and the settlement of complaints. If a principal is not satisfied by the response of a PIHBO, he or she can complain to an APIPO or to the PPC.

4.4.1.2 Settlement of a Complaint by an Accredited Personal Information Protection Organization

In Japan, APIPOs exist as a legal system to protect personal information.[442] Canada does not have this system. *APPI* of Japan assumes not only regulation by public institutions but also compliance with and promotion of personal information protection voluntarily by business companies and private bodies.[443] *APPI* of Japan prescribes general rules that will ensure the minimum acceptable level of personal information protection, because it applies to all private bodies handling personal information regardless of their business field and profitability. It is considered better that self-regulation and self-resolution are enhanced by private bodies in order to maintain the appropriate handling of personal information according to the nature of and the way of use of personal

---

[442] There is a list of accredited personal information protection organizations in Japan. See Personal Information Protection Commission, "The List of Accredited Personal Information Protection Organizations", (1 April 2020), online: *Personal Information Protection Commission* <https://www.ppc.go.jp/personalinfo/nintei/list/>.

[443] Tomomi Hioki & Yoichiro Itakura, *Kojin jōhō hogohō no shikumi* [Mechanism of Personal Information Protection Law] (Tokyo: Shojihoumu, 2017) at 136—139.

information, the actual conditions of its handling, and the circumstances of each business field.[444] APIPOs are private corporate bodies having the purpose of enhancing personal information protection and are established in each business field, and they are accredited by the PPC based on certain criteria (art. 47, 48, and 49). A PIHBO may register with an APIPO as a "covered business operator," that is, a PIHBO covered by the services of an APIPO. An APIPO has five main works: the first work is dealing with any complaints concerning the handling of personal information etc. by a covered business operator (art. 47 (1) (i)); the second work is providing a covered business operator with information concerning matters related to ensuring the proper handling of personal information etc. (art. 47 (1) (ii));[445] the third work is rendering necessary services related to ensuring the proper handling of personal information etc. by a covered business operator (art. 47 (1) (iii)); the fourth work is developing personal information protection guidelines and notifying the PPC of these guidelines (art. 53 (1) and (2));[446] and the fifth work is taking action in connection with a covered business operator such as providing guidance or recommendations to comply with the personal information protection guidelines (art. 53 (4)). Because these five works require neutrality, industry groups or business associations tend to become APIPOs.

In some cases, a principal may not be satisfied with the response of a PIHBO even after the PIHBO addresses a complaint concerning the handling of his or her personal information by the PIHBO. If the PIHBO is a covered business operator under an APIPO, the principal may petition the APIPO to resolve the complaint. The APIPO which receives the complaint shall hold

---

[444] Daini Tokyo Bar Association, *Kaisei kojin jōhō hogohō* [Revised Act on the Protection of Personal Information] (Tokyo: Shin Nippon Hoki, 2015) at 136—140.

[445] The accredited personal information protection organizations provide covered business operators information to ensure security and to deal with personal information appropriately as a proactive activity. See Uga, *supra* note 348 at 282. Some of them facilitate the covered business operators to obtain a certification for personal information protection. For example, JIPDEC holds consultation for the covered business operators to get a certification like APEC CBPR. See JIPDEC, "Nintei kojin jōhō hogo dantai [Accredited Personal Information Protection Organization]", (13 May 2020), online: *JIPDEC* <www.jipdec.or.jp/protection_org/about.html>.

[446] All accredited personal information protection organizations open personal information protection guidelines. Personal Information Protection Commission, *supra* note 442.

consultation, give necessary advice, and investigate the circumstances surrounding the complaint, and furthermore, it shall inform the covered business operator of the substance of the complaint and request its prompt resolution (art. 52 (1)). The APIPO may request that the covered business operator provide a written or oral explanation and submit a referential material (art. 52 (2)). The covered business operator must not refuse this request without a justifiable reason (art. 52 (3)). If the covered business operator deals with the complaint in a manner contradictory to the personal information protection guideline developed by the APIPO, the APIPO shall give the covered business operator notification and guidance to compel the covered business operator to follow the personal information protection guideline (art. 53 (4)).

4.4.1.3 Comparative Considerations

Canada prescribes in detail the procedure to handle a complaint in *PIPEDA*. However, Japan does not prescribe such a procedure in *APPI*.

In *APPI*, the settlement of a complaint is not a mandatory duty of PIHBOs but an obligation to make efforts; thus, *APPI* does not prescribe a complaint processing procedure. There are two reasons that a procedure to handle a complaint by PIHBO is not prescribed. The first is the rationale of lawmakers that the settlement of a complaint should be a private matter between a PIHBO and a principal; therefore, as the complaint should ideally be resolved promptly between the parties, a flexible processing procedure should optimally facilitate this.[447] The second is due to the multi-layered mechanism for resolving a complaint in *APPI*. *APPI* assumes the presence of a unique existence, that is, the APIPO.[448] If a PIHBO does not deal with complaint, a principal may ask an APIPO to take action against the PIHBO such as providing guidance or recommendations.

---

[447] Uga, *supra* note 348 at 233.

[448] *Ibid*.

The background of the establishment of this unique existence is an economic structure peculiar to Japan. There are many industry groups and business associations in Japan, and they have powerful political influence.[449] Representatives of industry groups attended the meeting to discussed the draft of *APPI*,[450] and argued for the importance of their self-regulation. Conclusively, in the *Basic Policy on the Protection of Personal Information*[451] established by the Cabinet on April 2, 2004, the importance of APIPOs was stipulated:

> The accredited personal information protection organization is expected to fulfill key roles in the effort to solve problems in the private sector through complementing the personal information handling business operator's own efforts to field complaints, facilitating the resolution of problems voluntarily and practically, and supporting the personal information handling business operator's efforts through the development of personal information protection guidelines unique to each business field. Accredited personal information protection organizations should sufficiently use the mechanisms available to them.[452]

When *APPI* was amended, representatives of industrial groups again joined as members of the committee to discuss the amendment.[453] At the committee, the importance of APIPOs was highlighted, and the procedure to handle a complaint by the APIPO was enhanced, making it a mandatory duty, from an obligation to make efforts.[454] Even now, industry groups and business associations are primarily in charge of the works of APIPOs.[455]

---

[449] Isao Niwa, "Rieki dantai no kyōryoku kankei to eikyōryoku [Coalition and Influence of Interest Groups]" (2006) 53:3 L Rev of Kinki U 298.

[450] The Study Group on Personal Information Protection, which was established on July 1999, was composed of representatives of industry groups, scholars, and lawyers. See Sonobe & Fujiwara, *supra* note 399 at 22.

[451] *Kojin joho no hogo ni kansuru kihon hoshin* [Basic Policy on the Protection of Personal Information], Cabinet Decision of April 2, 2004.

[452] *Ibid*. [translated by author]

[453] Keiichiro Seki, *Kojin jōhō hogo hō* [Personal Information Protection Law] (Tokyo: Gyosei, 2015) at 114.

[454] *Ibid* at 115.

[455] See Personal Information Protection Commission, *supra* note 389 at 36—42.

4.4.2 Authority of Commissioner/Commission

4.4.2.1 Canada

If a complaint is not settled between an individual and an organization, the individual may file a written complaint with the Commissioner (s. 11 (1)), and the Commissioner also may initiate a complaint (s. 11 (2)). The Commissioner must give the organization in question a notice of the complaint (s. 11 (4)). The Commissioner must examine the complaint. If the Commissioner decides not to conduct an investigation for the complaint, it must give notification of its decision and provide reasons (s. 12 (3)). If the individual gives the Commissioner compelling reasons for the Commissioner to investigate the organization, the Commissioner may consider whether or not the investigation should be conducted (s. 12 (4)). If the Commissioner decides to conduct the investigation, the Commissioner may call forth people to appear before the Commissioner, compel people to provide evidence, enter certain types of premises, converse with any person in such premises, and obtain relevant records found within such premises (s. 12.1 (1)). If the organization obstructs the investigation, it is subject to punishment (s. 28). After the investigation, the Commissioner may resolve the complaint with dispute resolution mechanisms (s. 12.1 (2)). If the Commissioner decides to discontinue the investigation (s. 12.2 (1)), the Commissioner must provide notification to both the individual and the organization that the investigation was discontinued, along with reasons (s. 12.2 (3)). If the complaint was not resolved with the dispute resolution mechanisms and the investigation was completed, the Commissioner shall prepare a report (s. 13 (1)). The report should include the opinion and recommendation of the Commissioner, so that both the individual and the organization can comply with the report. However, this report does not have any legal enforcement;[456] therefore, if the organization does not comply with the

[456] Office of the Privacy Commissioner, "Statement: Remarks by Privacy Commissioner of Canada regarding his 2018-2019 Annual Report to Parliament", (10 December 2019), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20191210/>, Last Modified: 2019-12-10.

report, it is not punished. If the organization does not comply with the report or the individual is not satisfied with the report, he or she may apply to the Court to request a hearing in order to address any matter relevant to the initial complaint or referenced within the Commissioner's report (s. 14 (1)).

Although the powers of the Commissioner are broad, case law indicates that they are not unlimited. In *Privacy Commissioner v. Blood Tribe Department of Health*,[457] the SCC confirmed that the Privacy Commissioner does not have the power to interfere with solicitor-client privilege. Annette Soup, who was laid off from Blood Tribe Department of Health (BTDH), requested BTDH to provide her access to her personnel file because she suspected that her employer had justified her dismissal based on erroneous and improperly acquired information. The employer denied her request and would not provide a rationale for denial. Ms. Soup filed a complaint with the Privacy Commissioner. The Privacy Commissioner requested that BTDH submit Ms. Soup's complete employment record. BTDH partially complied with the Commissioner's request, but would not provide certain documents, invoking solicitor-client privilege. The Commissioner ordered that BTDH released the privileged documents based on s. 12 of *PIPEDA* at the time (which moved to s. 12.1 in a later amendment), but the employer applied for judicial review to challenge the legality of the Privacy Commissioner's order. In a unanimous judgement, Binnie J. concluding that if the court entertained a challenge to the claim of privilege, it would violate the privilege. Binnie J. identified that the solicitor-client privilege has fundamental importance for a well-functioning legal system[458] and explained that open-textured language governing production of documents would be read not to include solicitor-client documents, referring to *Lavallee, Rackel & Heintz v. Canada*

[457] [2008] 2 SCR 574.

[458] *Ibid* at para 9.

(Attorney General)[459] and *Pritchard v. Ontario (Human Rights Commission)*[460].[461] Binnie J. also stated that "[the Commissioner] is an administrative investigator not an adjudicator."[462] Similarly, in *Privacy Commissioner of Canada v. Air Canada*,[463] the Court declared that the Privacy Commissioner had no jurisdiction in her administration of *PIPEDA* to rule on an assertion of privilege and that the Commissioner was not entitled to require a party to provide with affidavit evidence in support of its claim of privilege.

4.4.2.2 Japan

The affairs of the PPC include supervision of the handling of personal information, any necessary mediation of a lodged complaint and cooperation offered to the PIHBO who deals with the complaint (art. 61 (ii)). The PPC may investigate the PIHBO based on the lodged complaint or the authority of the PPC. In the investigation, the PPC may require the PIHBO to submit necessary information or material and may have the PPC'S officials enter a business office, inquire about the handling of personal information, and inspect a book, document or other property (art. 40 (1)). The PIHBO shall cooperate during the investigation, and if the PIHBO refuses, obstructs or evades the inspection, the PIHBO will be subject to punishment (art. 85). After the investigation, the PPC may select one of three options: the first choice is guidance or advice; the second choice is a recommendation or order; the third choice is an urgent order. The PPC may provide a PIHBO which has breached duties with necessary guidance or advice on the handling of personal information (art. 41). The breach of duties includes mandatory duties and obligations to make efforts, so the guidance and advice can apply both to mandatory duties and to obligations to make

---

459 2002 SCC 61.

460 *Pritchard v Ontario (Human Rights Commission)*, 2004 SCC 31.

461 *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, *supra* note 457 at para 11.

462 *Ibid* at para 20.

463 2010 FC 429.

efforts. The PPC may recommend that the PIHBO cease the act of violating or take other necessary action to rectify the violation if the PPC judges that the PIHBO violates its duties and that there is a need for protecting an individual's rights and interests (art. 42 (1)). If the PIHBO does not take action in line with the recommendation without legitimate ground, the PPC may order the PIHBO to take action in line with the recommendation (art. 42 (2)). If the PIHBO does not obey the order, it is subject to punishment (art. 84). If the PPC judges that the PIHBO violates its duties and that there is a need to take "urgent" action due to an issue that "seriously" harms an individual's rights and interests, the PPC may order the PIHBO to take necessary action to rectify the violation such as suspending the act of violation (art. 42 (3)). If the PIHBO does not obey this urgent order, it is subject to punishment (art. 84).

If a principal feels that a PIHBO has handled his or her personal information in a manner contrary to *APPI*, he or she will firstly need to lodge a complaint with the PPC. The PIHBO will be punished if it ignores an order from the PPC. However, the principal may file a lawsuit in connection with a demand pursuant to seeking disclosure, correction, and cessation of utilization etc. (art. 34). In one case, *Disclosure Request for Retained Personal Data*,[464] a principal sued a clinic directly seeking for provision of his health record without lodging a complaint to a competent minister, who was in charge of dealing with problems related to personal information before the PPC was established, on the basis of duty of disclosure by the principal in the previous version of *APPI*. The Japanese court rejected his claim because the previous version of *APPI* assumed that settlement of a complaint by a party or by a competent minister would proceed without involving the courts. When *APPI* was amended, the Japanese government proposed to expand the right of the principal. Therefore, principals now have the right to request disclosure, correction, and utilization

[464] *Kojin joho hogoho ni motozuku hoyu kojin deta kaiji seikyu [Disclosure Request for Retained Personal Data according to Act on the Protection of Personal Information]*, *supra* note 384.

cease etc. in under the current version of *APPI*. However, as of yet there are no case laws related to the exercise of this right.

4.4.2.3 Comparative Considerations

The authority of the Commissioners of both Canada and Japan is similar. Both may conduct an investigation and recommend rectification of violation of duties. However, the report which includes the opinions and recommendations of the Commissioner of Canada does not have any legal enforcement. Therefore, even if an organization ignores the Commissioner's recommendations, the organization is not punished. On the other hand, if a PIHBO in Japan ignores the PPC's order, it is punished. The reason for this difference is that *PIPEDA* prescribes a redress awarded by the Court (see 4.4.3.1). *APPI* of Japan does not prescribe a redress awarded by the court. However, this does not mean that a principal cannot seek legal remedy by the court; he or she is still permitted to bring a suit to the court.

4.4.3 Penalty

4.4.3.1 Canada

Penalty is stipulated in Section 28 of *PIPEDA*. If an organization contravenes its duty for retention of information related to a request by an individual, dismisses, demotes, disciplines, or harasses etc. an employee who discloses infringement of *PIPEDA* to the Commissioner, or obstructs the Commissioner in the investigation of a complaint, it is prescribed a fine of up to a maximum of $100,000 (s. 28). The organization will not have a fine imposed even if it contravenes the duties concerning the handling of personal information. However, the Court may order an organization to correct its practices (s. 16 (a)) and may award damages to the complainant, including damages for any humiliation (s. 16 (c)).

4.4.3.2 Japan

Penalties which apply to a PIHBO are provided in Chapter 7 of *APPI*. If a PIHBO and its employee, including a former employee, provided or used by stealth a personal information database etc. for the purpose of seeking their own or a third party's illegal profits, they shall be punished by imprisonment with labor for not more than one year or a fine of not more than 500,000 yen (art. 83). If a PIHBO receives personal data from another person, it is required to check how the data was acquired (art. 26 (1)). The person who provides the personal data shall not deceive the PIHBO on a matter relating to the confirmation (art. 26 (2)). If the person deceives the PIHBO, he or she shall be punished with a non-criminal fine of not more than 100,000 yen (art. 88 (1)). If a person fails to submit a report or material which was requested under an investigation by the PPC, or falsely submits a report or material, or fails to answer a question posed by the staff of the PPC or falsely answers a question, or refuses, obstructs or evades an inspection, he or she shall be punished with a fine of not more than 300,000 yen (art. 85 (1)).

If a PIHBO violates an order given by the PPC, it shall be punished by imprisonment with labor for not more than six months or a fine of not more than 300,000 yen (art. 84).

4.4.3.3 Comparative Considerations

Obstruction of an investigation by the Commissioner is subject to punishment in both Canada and Japan. If an organization contravenes duties related to handling of personal information, there are no penalties dictated in *PIPEDA*, but the problem is resolved by recommendation of the Commissioner and order and remedy of the Court. In the same situation in Japan, a PIHBO shall be punished if it ignores an order given by the PPC.

4.5 Comparative Analysis for Notable Differences between *PIPEDA* and *APPI*

In this Section, *PIPEDA* and *APPI* were compared from three aspects.

First Aspect: Definition of Personal Information

The first is the definition of personal information in the two laws. Both of the laws protect personal information. However, *APPI* defines personal information in more detail than *PIPEDA* and provides four classifications of personal information (see Fig 4-2). One reason that *APPI* has a more detailed definition is that there was an opinion that the obscurity of the definition of personal information caused stagnation in the Japanese economy (see 4.2.1.3). Also, unlike Canada, Japan did not have a supervisory authority to examine and judge personal information problems. The absence of such an authority meant that without a detailed definition, the boundary between information that is personal or not could be blurred, whereas in Canada, assessment of information as personal or not can be assessed by the supervisory authority as needed.

APPI subdivides personal information into personal data and retained personal data. These subdivisions are not seen in the laws of other countries including Canada. Personal data and retained personal data dictate what type of duties are imposed on a PIHBO (see Table 4-3). In other words, the duties of the PIHBO depend on what type of personal information the PIHBO has. The reason that personal data and retained personal data are defined in *APPI* is in order that the rigorousness of the personal information protection duties required of PIHBOs can be balanced according to the type of personal information they use. This method of regulation was developed through circumstances unique to Japan (see 4.2.1.3). When enactment of *APPI* was discussed, the Japanese government considered the concerns of business companies, hoping that they would smoothly agree to the legislations for protection of personal information. The government thought that it would an excessive burden upon trustees which only process personal information, without responsibilities of the control of personal information, or upon small and medium sized companies

which have little personal information, if all of the duties were required of them.[465] The definition of retained personal data thus exempts trustees from some duties depending on the level of authority they have over the information they deal with.

PIPEDA does not define sensitive information, but it assumes that organizations take special care of such information. On the other hand, *APPI* defines special care-required personal information. The reason that *APPI* defines this information is that it had a slightly different legal approach to privacy and personal information protection and considered international harmonization with other laws such as *EU GDPR* (see 4.2.2.3).

While *PIPEDA* does not have provisions related to de-identified information, *APPI* has special rules concerning anonymously processed information. The reason for the earlier establishment of rules on anonymously processed information in Japan versus Canada is that while the Japanese industrial field hoped to use de-identified information freely, an incident related to use of de-identified information occurred (see 4.2.3.3). This incident hastened the development of provisions for de-identified information in Japan. However, the OPC is now also preparing guidance for de-identification.

Second Aspect: Duties for Organizations Having Personal Information

The second aspect of comparison is concerning duties for organizations having personal information. Provisions of both *PIPEDA* and *APPI* were established referring to *OECD Guidelines*, so their duties are similar. However, there are notable differences. *PIPEDA* has the principle of consent, but *APPI* does not. On the other hand, opt-out methods are developed in *APPI*. The reason for this difference is that Japan made the legal framework for personal information protection

[465] Before the amendment of *APPI*, companies which had fewer than 5,000 units of personal information were not subject to *APPI*. This exception has been repealed for the sake of international harmonization to suit the *EU GDPR*.

focusing on the *OECD Guidelines*, but Canada introduced the principle of consent through consideration of the *EU Privacy Directive* (see 4.3.2.2).

APPI has duties for organizations which receive personal information from a third party which *PIPEDA* does not have. The reason that *APPI* regulates not only senders of personal information but also receivers is because of the occurrence of a serious incident related to data brokers (see 4.3.3.3).

Third Aspect: Enforcement

The third aspect of comparison is enforcement. *PIPEDA* and *APPI* both prescribe some methods to resolve personal information problems such as by settlement of complaints by the involved party, by authority of Commissioner/Commission, and through penalties. Additionally, *APPI* outlines another method whereby an APIPO supports the individual and organization in order to settle the problems. This system is unique to Japan and was created because of the Japanese economic structure (see 4.4.1.3). In Japan, industry groups have many roles and strong power. When *APPI* was enacted, Japan did not have a supervisory authority. On the other hand, the government expected flexible protection for consumers and companies by the industry groups, which have the potential authority to regulate members and promote the interests of the whole industrial field.

5 Conclusion

A comparison between the Canadian and Japanese processes of developing privacy and personal information protection, including past and more recent political and social perspectives, had not yet been undertaken. This thesis set out to close this gap in the literature and to contribute to the fields of comparative law and legal history.

Section 2 of this thesis has considered the right of privacy in constitutional law and tort law in Canada and Japan. It has explored various possible meanings of "privacy" and of the right of privacy, and has identified a theory on the right of privacy which can assist in examining the protection of personal information in the Canadian and Japanese contexts.[466]

Section 3 has outlined the process of developing personal information protection in Canada and Japan. As the comparative research has demonstrated, the process can be divided into five periods:[467] a first period characterized by the establishment of the right of privacy, a second period when laws for protecting personal information in the public sector were enacted, a third period, characterized by voluntary efforts to protect personal information being made in the private sector, a fourth period during which laws for protecting personal information in private sector were enacted, and a fifth period that saw the implementation of certification systems.

Section 4 has focused on a comparison of *PIPEDA* and *APPI*, the personal information protection laws for the private sector for Canada and Japan. The comparison has been guided by three main questions: 1) what is protected by laws concerning personal information, 2) how do the laws protect personal information, and 3) how do the laws secure enforceability?[468] The inquiry identified similarities and differences between *PIPEDA* and *APPI*, and considered possible reasons

---

[466] See section 2.4.

[467] See section 3.4.

[468] See section 4.2, section 4.3, and section 4.4, respectively.

and explanations. Notable differences were found in the attitudes regarding anonymously processed information, the consent principle, the opt-out procedure, and the settlement of complaints by APIPOs.[469] Various reasons for these differences have been considered, related to the political and economic structures and circumstances in the respective countries, the surrounding legal frameworks and underlying legislative intentions.

In a final evaluation of the similarities and differences between Canadian and Japanese personal information protection regimes, the role of the APIPOs in Japan, which do not have a comparable entity in Canada, appears particularly noteworthy.[470] While both Canada and Japan have a Privacy Commissioner/Commission who can receive complaints from individuals, conduct investigations and give recommendations to the organization or PIHBO, Japan's 43 APIPOs allow for a more customized and flexible personal information protection system, because they can establish personal information protection guidelines for each business field (medical, financial, etc.), which handle different types of personal information and have varying levels of desired security.

APPI offers a baseline level of personal information protection and gives more freedom to the APIPOs in individual sectors to self-regulate according to various sectoral needs and to enlist the input of companies as well as consumer representatives or other concerned parties in order to decide the level of personal information protection that is most appropriate for them.[471] This also allows individual companies and consumers to have an alternative way to resolve problems besides through the court or legal system, which tends to be a more difficult, time consuming, and expensive process for all involved parties, and puts less stress on the legal system.

---

[469] See section 4.2.3.3, section 4.2.2.3, section 4.2.2.3, section 4.4.1.3, respectively

[470] See section 4.4.1.2

[471] See *APPI*, *supra* note 13 at art 53.

Additionally, APIPOs are more adept at dealing with issues which involve the certification systems which are outside the realm of the law, and furthermore, they are more likely to work proactively to approach companies and encourage them in protecting personal information.[472] On the other hand, the court system tends to handle personal information protection problems on a retroactive basis.[473] Once personal information is leaked, the damage to the consumer has already occurred, so all things being considered, it is preferable to approach personal information protection on a proactive basis. Given these considerations, the concept of APIPOs could be a valuable model to consider for the legal systems of other countries, such as Canada.

In the future, particularly as the digital environment continues to change and new privacy issues arise, this research hopes to be of use for Canadian and Japanese researchers who continue to survey these processes. This thesis thus aims to contribute to the laying of a foundation for the continued examination and discussion of these matters. The legal similarities and differences between *PIPEDA* and *APPI* examined within this thesis highlight the particular characteristics of both statutes, information that may be useful in situations in which lawmakers need to review privacy and personal information law. Additionally, these comparisons can provide an improved understanding for Canadian and Japanese companies doing business in each other's respective countries.

This thesis focuses primarily on the comparison of personal information protection laws as hard law. However, of course, soft laws protecting privacy and personal information, such as certification systems, exist as well and are increasingly important. In recent years, certification systems have been considered by many countries and international organizations to be effective tools for privacy and personal information protection, because, unlike hard law, they can be revised

---

[472] See footnote 445.

[473] See section 3.3.1.

quickly in order to cope with the emergence of new technologies. Since certification systems supplement hard law, further research of soft law is needed in order to pursue more effective and efficient international cooperation on privacy and personal information protection.

Bibliography

Legislation

Canada

Act respecting the protection of personal information in the private sector, RSQ c P-39.1.
Bill C–29, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 3rd Sess, 40th Parl, 2010.
Bill C–12, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess, 41th Parl, 2011.
Bill S-4, *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*.
Bank of Canada Act, RSC 1985 c B-2.
Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
Canadian Human Rights Act, SC 1976-77, c 33.
Charter of Human Rights and Freedoms, CQLR c C-12.
Civil Code of Québec.
Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.
Criminal Code, RSC 1985, c C-46.
Local Authority Freedom of Information and Protection of Privacy Act, SS 1990-91, c L-27.1.
Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56.
Municipal Government Act, SNS 1998, c 18.
Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
Privacy Act, RSC 1985, c P-21.
Privacy Act, RSBC 1996, c 373.
Privacy Act, CCSM, c P125.
Privacy Act, RSS 1978, c P-24.
Privacy Act, RSNL1990, c P-22.

Japan

Denshi keisan soshiki no unei ni kansuru jorei [Ordinance on the Management of Data Processing Systems], Promulgated on 26 March, 1975.
Denshi keisanki shori ni kakaru kojin joho nohogo ni kansuru jorei [Ordinance on the Protection of Personal Information Pertaining to Electronic Data Processing], Promulgated on 28 June, 1973.
Dokuritsu gyosei hojin to no hoyu suru kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc], Amendment of Act No. 89 of 2016, Amendment of Act No. 89 of 2016.
Gaikokujin toroku ho [Alien Registration Act], Amendment of Act No. 95 of 1981.
Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs], Act No. 95 of 1988.
Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information Electronically Processed and Held by Administrative Organs], Amendment of Act No. 51 of 2016.

Cabinet's 82nd Bill, *Gyosei kikan no hoyu suru denshi keisanki shori ni kakaru kojin joho no hogo ni kansuru horitsu an* [Bill on the Protection of Personal Information Electronically Processed and Held by Administrative Organs].
Gyosei tetsuzuki ni okeru tokutei no kojin wo shikibetsu suru tame no bango no riyo to ni kansuru horitsu [Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures], Amendment of Act No. 63 of 2013.
Kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information], Amendment of Act No. 65 of 2015.
Kojin joho no hogo ni kansuru horitsu [Act on the Protection of Personal Information], Act No. 57 of 2003.
Kojin joho no hogo ni kansuru horitsu shiko kisoku [Enforcement Rules for the Act on the Protection of Personal Information], Rules of the Personal Information Protection Commission No. 3 of 2016.
Kojin joho no hogo ni kansuru horitsu shiko rei [Cabinet Order to Enforce the Act on the Protection of Personal Information], Amendment of Cabinet Order No. 324 of 2016.
Kojin joho no hogo ni kansuru kihon hoshin [Basic Policy on the Protection of Personal Information], Cabinet Decision of April 2, 2004.
Mimpō [Civil Code of Japan], Amendment of Act No. 78 of 2006.
Nihonkoku kempō [Constitution of Japan], Constitution 1946.
Shogai wo riyu to suru sabetsu no kaisho no suishin ni kansuru horitsu [Act for Eliminating Discrimination against Persons with Disabilities], Act No. 65 of 2013.
Shogaisha kihon ho [Basic Act for Persons with Disabilities], Amendment of Act No. 90 of 2011.

Others

Datalagen [Data Act].
Datenschutzgesetz [Data Protection Act], 1970, Gesetz- und Verordnungsblatt für das Land Hessen Teil I, Seite 625.
Fair Credit Reporting Act of 1970, Pub L No 91-508, 84 Stat 1127.
Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, Journal Officiel du Grand-Duché de Luxembourg, 11 avril 1979, N° 29.
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, JO, 7 January 1978, 227.
Lov om offentlige myndigheders registre [Public Authorities Registers Act], 8 juni 1978, Lov nr 294.
Lov om personregistre mm av 9 juni 1978 [Personal Data Registers Act of 1978], 1978, Norsk Lovtidend Avd. 1, Nr. 48, 402.
Lov om private registre m. v. [Private Registers Act], 8 juni 1978, Lov nr 293.
Privacy Act of 1974, Pub L No 93-579, 88 Stat 1896.
Right to Financial Privacy Act of 1978, Pub L No 95–630, 92 Stat 3641.

Jurisprudence

Canada

Application under s 8328 of the Criminal Code (Re), 2004 SCC 42.
Athans v Canadian Adventure Camps Ltd et al (1977), 17 OR (2d) 425, 80 DLR (3d) 583 (Ont H Ct J).
Aubry v Éditions Vice-Versa inc, [1998] 1 SCR 591, 157 DLR (4th) 577.

Brasserie Labatt ltée v. Villa, 1944 CarswellQue 144 (WL Can), [1994] JQ No 1002 (QL) (QCCA)
Canada (Privacy Commissioner) v Air Canada, 2010 FC 429.
Canada (Privacy Commissioner) v Blood Tribe Department of Health, [2008] 2 SCR 574, 294 DLR (4th) 385.
CanadianOxy Chemicals Ltd v Canada (Attorney General), [1999] 1 SCR 743, 171 DLR (4th) 733.
Davis v McArthur (1969), 10 DLR (3d) 250, 1969 CarswellBC 230 (WL Can) (BCSC).
Demcak v Vo, 2013 BCSC 899.
Doe 464533 v ND, 2016 ONSC 541.
Englander v Telus Communications Inc, 2004 FCA 387.
Godbout v Longueuil (City), [1997] 3 SCR 844, 152 DLR (4th) 577.
Grant v Winnipeg Regional Health Authority et al, 2015 MBCA 44.
Hill v Church of Scientology of Toronto, [1995] 2 SCR 1130, 126 DLR (4th) 129.
Hunter et al v Southam Inc, [1984] 2 SCR 145, 11 DLR (4th) 641.
Jones v Tsige, 2011 ONSC 1475.
Jones v Tsige, 2012 ONCA 32.
Joseph v Daniels, 1986 CarswellBC 172 (WL Can), [1986] BCJ No 3231 (QL) (BCSC).
Krouse v Chrysler Canada Ltd et al (1970), 12 DLR (3d) 463, 3 OR 135 (Ont H Ct J).
Krouse v Chrysler Canada Ltd et al (1973), 40 DLR (3d) 15, 1 OR (2d) 225 (Ont CA).
Lavallee, Rackel & Heintz v Canada (Attorney General); White, Ottenheimer & Baker v Canada (Attorney General); R v Fink, 2002 SCC 61.
Motherwell v Motherwell (1976), 73 DLR (3d) 62, 1976 CarswellAlta 129 (WL Can) (Alta SC (AD)).
Palad v Pantaleon, 1989 CarswellOnt 2794 (WL Can), [1989] OJ No 985 (QL) (Ont Dist Ct).
Parasiuk v Can Newspapers Co, [1988] 2 WWR 737, 1988 CarswellMan 108 (WL Can) (Man QB).
Pritchard v Ontario (Human Rights Commission), 2004 SCC 31.
Privacy Commissioner of Canada v Air Canada, 2010 FC 429.
Provincial Partitions Inc v Ashcor Inplant Structures Ltd, 1993 CarswellOnt 1119 (WL Can), [1993] OJ No 4685 (QL) (Ont Ct (Gen Div)).
R v Dyment, [1988] 2 SCR 417, 1988 CarswellPEI 7 (WL Can).
R v Evans, [1996] 1 SCR 8, 131 DLR (4th) 654.
R v Gomboc, 2010 SCC 55.
R v Jarvis, 2019 SCC 10.
R v Marakah, 2017 SCC 59.
R v Morgentaler, [1988] 1 SCR 30, 44 DLR (4th) 385.
R v O'Connor, [1995] 4 SCR 411, 130 DLR (4th) 235.
R v Plant, [1993] 3 SCR 281, 84 CCC (3d) 203.
R v Salituro, [1991] 3 SCR 654, 68 CCC (3d) 289.
R v Tessling, 2004 SCC 67.
Robbins v Canadian Broadcasting Corp (1957), 12 DLR (2d) 35, 1957 CarswellQue 135 (WL Can) (Qc Sup Ct).
Roth v Roth, 1991 CarswellOnt 44 (WL Can), [1991] OJ No 1301 (QL) (Ont Ct J (Gen Div)).
Rousseau v Wyndowe, 2006 FC 1312.
Ruby v Canada (Solicitor General), [2000] 3 FC 589.
Saccone v Orr, 1981 CarswellOnt 586 (WL Can), [1981] OJ No 3132 (QL) (Ont Co Ct).

Trout Point Lodge Ltd v Handsho, 2012 NSSC 245.

Japan

Erosu purasu gyakusatsu [Eros plus Massacre] (1970), 23 Koto Saibansho Minji Hanreishu 172, 246 Hanrei Taimuzu 129 (Tokyo High Court).
Kojin joho hogoho ni motozuku hoyu kojin deta kaiji seikyu [Disclosure Request for Retained Personal Data according to Act on the Protection of Personal Information] (2007), 1275 Hanrei Taimuzu 323, 1978 Hanrei Jiho 27 (Tokyo District Court).
Kyoto fu gakuren [Kyoto League of Student Self-Government] (1969), 23 Saikou Saibansho Keiji Hanreishu 1625, 242 Hanrei Taimuzu 119 (Grand Bench of Supreme Court).
Osaka shoken roso ampo soshi demo [Demonstration for deterring the Japan-US Security Treaty by Labour Union of Osaka Stock Exchange] (1964), 17 Koutou Saibansho Keiji Hanreishu 384, 165 Hanrei Taimuzu 106 (Osaka Hish Court).
Shimon onatsu kyosei [Enforcement for fingerprinting], 1986 Koto Saibansho Keiji Saiban Sokuhoshu 160 (Tokyo High Court).
Shimon onatsu kyohi [Rejection for fingerprinting] (1995), 49 Saiko Saibansho Keiji Hanreishu 842, 900 Hanrei Taimuzu 167 (3rd Petty Bench of Supreme Court).
Utage no ato [After the Banquet] (1964), 15 Kakyu Saibansho Minji Hanreishu 2317, 385 Hanrei Jiho 12 (Tokyo District Court).

Others

Griswold v Connecticut, 381 US 479 (1965).
Hamilton v Lumbermen's Mutual Casualty Co, [1955] 82 So (2d) 61 (La Ct App 1955).
Roe v Wade, 410 US 113 (1973).

Secondary Material

Monographs

Akasaka, Masahiro. *Kempō kōgi: Jinken* [Lecture of Constitutional Law: Human rights] (Tokyo: Shinzansha, 2011).
Altman, Irwin. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Monterey, Cal: Brooks/Cole, 1975).
American Law Institute. *Restatement of the law (2nd) Torts* (St Paul, Minnesota: American Law Institute Publishers, 1977).
Ashibe, Nobuyoshi. *Kempōgaku 2: Jinken sōron* [Study of Constitutional Law (2): General of Human Rights] (Tokyo: Yuhikaku, 1994).
Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca NY: Cornell University Press, 2018).
Bernal-Castillero, Miguel. *Canada's Federal Privacy Laws* (Ottawa: Library of Parliament, 2013).
Beverley-Smith, Huw, Ansgar Ohly & Agnès Lucas-Schloetter. *Privacy, Property and Personality* (Cambridge, UK: Cambridge University Press, 2005).
Cooley, Thomas McIntyre. *Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Chicago: Callaghan & Company, 1880).
Coughlan, Stephen Gerard et al. *Global reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization* (Ottawa: Law Commission of Canada, 2006).
Daini Tokyo Bar Association. *Kaisei kojin jōhō hogohō* [Revised Act on the Protection of

Personal Information] (Tokyo: Shin Nippon Hoki, 2015).
Drapeau, Michel W & Marc-Aurèle Racicot. *Federal Access to Information and Privacy Legislation Annotated 2013* (Toronto: Thomson Reuters Canada Ltd, 2012).
———. *Protection of privacy in the Canadian private and health sectors* (2013).
Ehara, Takeru. *Puraibashī ken no sōgōteki kenkyū* [Comprehensive Research on Privacy Rights] (Kyoto: Horitsu Bunkasha, 1991).
Fischer-Hübner, Simone. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms* (Berlin: Springer-Verlag Berlin Heidelberg, 2001).
Fleming, John G. *The law of torts*, 7th ed (London: Sweet & Maxwel, 1988).
Fujiwara, Shizuo. *Chikujō kojinjōhō hogohō* [Annotations to Act on the Protection of Personal Information] (Tokyo: Kobundo, 2003).
Fujiwara, Soichiro, Hironobu Tsukamoto & Akemi Suzuki. *Nichibeiō kojin jōhō hogo dēta purotekushon no kokusai jitsumu* [International Practice of Personal Information Protection and Data Protection in Japan, the U.S. and EU], Oki Mori, ed. (Tokyo: Shojihoumu, 2017).
Giovanella, Federica. *Copyright and Information Privacy: Conflicting Rights in Balance* (Cheltenham, UK: Edward Elgar Publishing, 2017).
González-Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Germany: Springer, 2014).
Gratton, Eloïse. *Understanding personal information: managing privacy risks* (Markham, Ont: LexisNexis, 2013).
Hioki, Tomomi & Yoichiro Itakura. *Kojin jōhō hogohō no shikumi* [Mechanism of Personal Information Protection Law] (Tokyo: Shojihoumu, 2017).
Horibe, Masao et al. *OECD puraibashī gaidorain - 30 nen no shinka to mirai* [OECD Privacy Guidelines: Advance for 30 Years and Future] (Tokyo: JIPDEC, 2014).
House of Commons. *Privacy and Social Media in the Age of Big Data*, Report of the Standing Committee on Access to Information, Privacy and Ethics (2013).
Ishii, Kaori. *Kojin jōhō hogohō no rinen to gendaiteki kadai* [Philosophy of Personal Information Protection Law and Contemporary Issues] (Tokyo: Keiso Shobou, 2008).
Ito, Masami. *Puraibashi no kenri* [Right of Privacy] (Tokyo: Iwanami Shoten, 1963).
Komukai, Taro. *Jōhōhō nyūmon* [Introduction to Information] (Tokyo: NTT Shuppan, 2015).
Kosta, Eleni. *Consent in European Data Protection Law*, Nijhoff Studies in European Union Law (Leiden: Brill, 2013).
Madsen, Wayne. *Handbook of Personal Data Protection* (New York: Palgrave Macmillan, 1992).
Matsui, Shigenori. *Nihonkoku kempō* [Constitution of Japan] (Tokyo: Yuhikaku, 1999).
McIsaac, Barbara, Rick Shields & Kris Klein. *The law of privacy in Canada*, 2011 Student ed (Toronto: Carswell, 2011).
McNairn, Colin HH & Alexander K Scott. *Privacy Law in Canada* (Toronto: Butterworths, 2001).
Miyake, Hiroshi & Ikuko Komachiya. *Kojin jōhō hogo hō no hōritsu sōdan* [Legal Counseling for Personal Information Protection] (Tokyo: Seirin Shoin, 2017).
Munesue, Toshiyuki. *Jinkenron no shin kōsei* [New Structure of Human Rights] (Tokyo: Shinzansha, 1992).
Nadeau, Alain-Robert. *Vie privée et droits fondamentaux : étude de la protection de la vie privée en droit constitutionnel canadien et américain et en droit international.* (Thesis, University of Ottawa, 2000) [unpublished].
Okamura, Hisamichi. *Kojin jōhō hogoho* [Act on the Protection of Personal Information], 3d ed (Tokyo: Shojihoumu, 2017).

Perrin, Stephanie & Canada. *The Personal Information Protection and Electronic Documents Act: an annotated guide* (Toronto: Irwin Law, 2001).
Powell, Anastasia & Nicola Henry. *Sexual Violence in a Digital Age* (London: Palgrave Macmillan, 2017).
Power, Michael. *The Law of Privacy*, 2d ed (Toronto: LexisNexis Canada, 2017).
Sato, Koji. *Kempō* [Constitutional Law], 3d ed (Tokyo: Seirin Shoin, 1995).
Scassa, Teresa & Michael Eugene Deturbide. *Electronic Commerce and Internet Law in Canada* (Toronto, Ontario: CCH Canadian Limited, 2004).
Seki, Keiichiro. *Kojin jōhō hogo hō* [Personal Information Protection Law] (Tokyo: Gyosei, 2015).
Shimpo, Fumio. *Puraibashī no kenri no seisei to tenkai* [Creation and Development of the Right to Privacy] (Tokyo: Seibundo, 2000).
Sonobe, Itsuo & Shizuo Fujiwara. *Kojin jōhō hogohō no kaisetsu [Commentary on Personal Information Protection Laws]*, 2d ed (Tokyo: Gyosei, 2018).
Suenobu, Sanji. *Eibeihō no kenkyū (Jō)* [Study of Anglo-American Law (1)] (Tokyo: University of Tokyo Press, 1959).
Thompson, Valerie D. *Health and Health Care Delivery in Canada* (Toronto: Elsevier Health Sciences, 2015).
Turnbull, Ian J. *Privacy in the Workplace* (Toronto: CCH Canadian Limited, 2009).
Uga, Katsuya. *Kojin jōhō hogohō no chikujō kaisetsu* [Commentary on Personal Information Protection Laws], 6th ed (Tokyo: Yuhikaku, 2018).
———. *Kojin jōhō hogohō to toriatsukai jitsumu* [Act on the Protection of Personal Information and Practice] (Tokyo: Nihon Horei, 2017).
WEF. *Personal Data: The Emergence of a New Asset Class* (World Economic Forum, 2011).
Westin, Alan F. *Privacy and freedom* (London: Bodley Head, 1970).
Yagi Koji. *Mai nambā hō no subete* [All about My Number Act] (Tokyo: Toyo Keizai Inc., 2013).
Zureik, Elia, Lynda Harling Stalker & Emily Smith. *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (Montréal: McGill-Queen's University Press, 2010).

Articles

Acquisti, Alessandro, Curtis Taylor & Liad Wagman. "The Economics of Privacy" (2016) 52:2 J Econ Lit.
Aikenhead, Moira. "A 'Reasonable' Expectation of Sexual Privacy in the Digital Age" (2018) 41:2 Dal LJ 273.
Alter, Susan, Nancy Holmes & William Young. "Privacy Rights and New Technologies: Consultation Package" in *Privacy: Where Do We Draw the Line?* Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (Ottawa: House of Commons, 1997) Appendix I.
Altman, Irwin. "Privacy Regulation: Culturally Universal or Culturally Specific?" (1977) 33:3 J Soc Issues 66.
Bloustein, Edward J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 NYUL Rev 962.
Bridgeman, Jo & Michael A Jones. "Harassing Conduct and Outrageous Acts: A Cause of Action for Intentionally Inflicted Mental Distress?" (1994) 14:2 LS 180.
British Columbia Law Institute. "Report on the Privacy Act of British Columbia" (2008) 49 BCLI

Rep, online: <www.ssrn.com/abstract=1418205>.
Chaffey, Douglas Camp. “The Right to Privacy in Canada” (1993) 108:1 Political Science Quarterly 117.
Chester, Simon, Jason Murphy & Eric Robb. “Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?” (2003) 27:4 Adv Q 357.
Conroy, Amy M. “Protecting Your Personality Rights in Canada: A Matter of Property or Privacy?” (2012) 1:1 UWOJ Leg Stud, online: <https://ir.lib.uwo.ca/uwojls/vol1/iss1/3>.
Cooke, Elizabeth. “A Development in the Tort of Private Nuisance” (1994) 57:2 Modern L Rev 289.
Craig, John DR. “Invasion of Privacy and Charter Values: The Common-Law Tort Awakens” (1997) 42:2 McGill LJ 355.
Elder, David. “Canada” in Monika Kuschewsky, ed, *Data Protection & Privacy: Jurisdictional Comparisons* (London: Sweet & Maxwell, 2012) 41.
Esayas, Samson Y. “Privacy-as-a-quality parameter of competition” in Björn Lundqvist & Michal S Gal, eds, *Competition Law for the Digital Economy* (Cheltenham, UK: Edward Elgar Publishing, 2019) 126.
Forgó, Nikolaus et al. “The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings” in Marcelo Corrales, Mark Fenwick & Nikolaus Forgó, eds, *New Technology, Big Data and the Law* (Singapore: Springer, 2017) 251.
Hargreaves, Stuart. “Relational Privacy & Tort” (2017) 23:3 Wm & Mary J Women & L 433.
Hokama, Hiroshi. “Puraibashī no kenri (1) [The Right to Privacy]” (1959) 31:6 Horitsujiho 18.
Horibe, Masao. “1980 nen OECD puraibashī gaidorain to nihon [OECD Privacy Guidelines in 1980 and Japan]” in *OECD puraibashī gaidorain - 30 nen no shinka to mirai [OECD Privacy Guidelines: Advance for 30 Years and Future]* (Tokyo: JIPDEC, 2014).
———. “Puraibashī kojin jōhō hogo giron no sekaiteki tenkai to nihon [Global Development of Privacy and Personal Information Protection Discussions and Japan]” (2013) 54:11 IPSJ J 1106.
Hunt, Chris DL. “Privacy in the Common Law: A Critical Appraisal of the Ontario Court of Appeal’s Decision in Jones v. Tsige.” (2012) 37:2 Queen’s LJ 661.
———. “The Common Law’s Hodgepodge Protection of Privacy” (2015) 66 UNBLJ 161.
Igarashi, Kiyoshi. “Tekunorojī to puraibashī [Technology and Privacy]” (1969) 413 Jurist 134.
Itakura Yoichiro. “Kojin jōhō hogo hō ihan wo riyū to suru songai baishō seikyū ni kansuru kōsatsu [Consideration on Claims for Damages Due to Violation ofAct on the Protection of Personal Information]” (2012) 11 Inf Network L Rev 2.
Kaino, Michitaka. “Puraibashīken to sono hoshō [Right of Privacy and Guarantee]” (1959) 39:1.2.3 Minshoho Zasshi 87.
Kakumoto, Kazumasa. “Saibā jidai ni okeru puraibashī no hō riron (2): Shihō jō no mondai wo chūshin ni [Legal Theory of Privacy in Cyber Era (2): Focus on Issues in Private Law]” (2017) 67:5 Hokkaido L Rev 109.
Kardash, Adam & Patricia Kosseim. “Canada” in *The international comparative legal guide to Data Protection 2018*, 5th ed (London: Global legal group, 2018).
Klar, Lewis N. “The Impact of U.S. Tort Law in Canada” (2011) 38:2 Pepp L Rev 359.
Komachiya, Ikuko. “Puraibashī no kenri - kigen to seisei - [Right of Privacy - Origin and Generation -]” (2004) 15 Archives 48.
Koops, Bert-Jaap et al. “A Typology of Privacy” (2017) 38:2 U Pa J Intl L 483.
Krane, Joshua A. “‘Sir’ches and Seizures: Are Supplementary Information Requests Unconstitutional?” (2011) 52:2 Can Community LJ 232.

Larocque, André. “La réforme électorale. L’héritage démocratique du Premier ministre René Lévesque” in *L’éthique gouvernementale: Cahiers de recherche éthique 21* (Montreal: Fides, 1997).
Maki, Misaki. “Jiko ketteiken no ronten [Points at Issue of Right of Self-determination]” (2006) 2006:5 Reference 77.
McCamus, John D. “The Protection of Privacy: The Judicial Role” in Rosalie S Abella & Melvin L Rothman, eds, *Justice beyond Orwell* (Montréal: Éditions Y. Blais, 1985) 168.
McClennan, Jennifer & Vadim Schick. “O, Privacy - Canada’s Importance in the Development of the International Data Privacy Regime” (2007) 38:3 Geo J Intl L 669.
McCorquodale, Susan. “Corporations’ Right to Privacy in Canada and Australia: A Comparative Analysis” (2003) 15:1 Bond L Rev 102.
McKay-Panos, Linda. “The Canadian Charter of Rights and Freedoms: An Integral Part of Our Constitution” 37:3 LNow 20.
Morgan, Charles. “Employer Monitoring of Employee Electronic Mail and Internet Use” (1999) 44:4 McGill LJ 849.
Nigusse, Girma & Bart De Decker. “Capabilities and Limitations of P3P” (2009) Report CW 539.
Niwa, Isao. “Rieki dantai no kyōryoku kankei to eikyōryoku [Coalition and Influence of Interest Groups]” (2006) 53:3 L Rev of Kinki U 298.
Oliphant, Benjamin. “Taking Purposes Seriously: The Purposive Scope and Textual Bounds of Interpretation under the Canadian Charter of Rights and Freedoms” (2015) 65:3 UTLJ 239.
Parent, William A. “A New Definition of Privacy for the Law” (1983) 2:3 Law & Phil 305.
Peck, Richard & Sarah Pringle. “Privacy, Technology and the Rule of Law” (2019) 77:6 Advocate 837.
Post, Robert C. “Three Concepts of Privacy” (2001) 89:6 Geo LJ 2087.
Prosser, William L. “Privacy” (1960) 48:3 Cal L Rev 383.
Reiter, Eric H. “Privacy and the Charter: Protection of People or Places?” (2009) 88:1 Can B Rev 119.
Sato, Koji. “Kenri toshiteno puraibashī [Privacy as Legal Right]” (1981) 742 Jurist 158.
Shinohara, Harumi. “JIS Q 15001 kaisei ni itaru keii [The Background for amending JIS Q 15001]” *Information From JADAC and Experts* (July 2018).
Stoddart, Jennifer & Heather Black. “Message from the Privacy Commissioner of Canada” in *Learning from a decade of experience: Québec’s Private Sector Privacy Act* (Ottawa: Privacy Commissioner of Canada, 2005).
Storr, Christine & Pam Storr. “Internet of Things: Right to Data from a European Perspective” in Marcelo Corrales, Mark Fenwick & Nikolaus Forgó, eds, *New Technology, Big Data and the Law* (Singapore: Springer, 2017) 65.
Suzuki, Masatomo. “kojin jōhō hogohō to puraibashī no kenri [The Act on the Protection of Personal Information and the Right of Privacy]” in Masao Horibe, ed, *Puraibashī kojin jōhō hogo no shin kadai* [New Issues of Protection for Privacy and Personal Information] (Tokyo: Shojihoumu, 2010).
Takahashi, Mikio. “Higisha no shashin satsuei to shōzōken [Photographing of Suspect and Portrait Rights]” (1966) 135 Hanrei Taimuzu 73.
Takasaki, Haruo. “Kojin jōhō hogo ni kakaru hōseido wo meguru EU no jōkyō [EU Situation regarding Legal System for Personal Information Protection]” (2014) 55:12 IPSJ J 1337.
Warren, Samuel D & Louis Dembitz Brandeis. “The Right to Privacy” (1890) 4:5 Harv L Rev 193.
Wedge, Catherine. “Limitations on Alcohol and Drug Testing in Collective Bargaining

Relationships" (1994) 2 CLELJ 461.

Others

APEC. "Business | Cross Border Privacy Rules System", (12 June 2019), online: *Cross Border Privacy Rules System* <cbprs.org/business/>.

Barrass, Rob & Lyndsay Wasser. *Seclusion Intrusion: A Common Law Tort for Invasion of Privacy* (McMillan LLP, 2012).

Benesse Holdings. *Kojin jōhō rōei jiko chōsa iinkai ni yoru chōsa hōkoku* [Report by Personal Information Leakage Incident Investigation Committee] (2014).

Cabinet. *Shōwa 62 nendo ni kōzubeki sochi wo chūshin to suru gyōsei kaikaku no jisshi hōshin ni tsuite* [Implementation Policy for Administrative Reform - Focused on Measures to Be Taken in the Fiscal Year 1987].

Canada (Minister of Innovation, Science and Economic Development). *Government Response to the Twelfth Report of The Standing Committee on Access to Information, Privacy And Ethics* (2018).

Canada, Office of the Privacy Commissioner of. "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts", (5 November 2004), 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/>.

Cavoukian, Ann. *Privacy by Design ... Take the Challenge* (Information and Privacy Commissioner of Ontario, 2009).

———. *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario, 2009).

Debenham, David. *Canada's New Tort of Privacy and Its Impact on Your Fraud Investigation* (2012).

EC. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31.

———. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1.

Employment and Social Development. "Federally Regulated Businesses and Industries", (15 April 2020), online: *Canada.ca* <www.canada.ca/en/employment-social-development/programs/employment-equity/regulated-industries.html>.

Expert Committee on the provision on the outside of data related to Suica. *Suica ni kansuru dēta no shagai heno teikyō ni tsuite chūkan torimatome* [The provision on the outside of data related to Suica: Interim Report], by Expert Committee on the provision on the outside of data related to Suica, Zotero (2014).

Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (2012).

Flaherty, David H. *Reflections on Reform of the Federal Privacy Act* (Office of the Privacy Commissioner of Canada, 2008).

Founded mainly on the materials collected by the Philological Society and edited by Sir James Augustus Henry Murray et al. *The Oxford English dictionary A new English dictionary on*

historical principles (Clarendon Press, 1909).
Gaya, Saad. "R v Jarvis: Carving out a Contextual Approach to Privacy", (7 March 2019), online: *TheCourt.ca* <www.thecourt.ca/r-v-jarvis-carving-out-a-contextual-approach-to-privacy/>.
Government of Canada (Department of Justice). "Charterpedia - General principles for the interpretation and application of the Charter", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/principles-principes.html>.
———. "Charterpedia - Section 7 – Life, liberty and security of the person", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html>.
———. "Charterpedia - Section 8 – Search and seizure", (17 June 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html>.
———. "Modernizing Canada's Privacy Act", (20 August 2019), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.
———. "Where our legal system comes from - About Canada's System of Justice", (16 October 2017), online: *Department of Justice* <www.justice.gc.ca/eng/csj-sjc/just/03.html>.
Government of Canada (Global Affairs Canada). "Canada-Japan Relations", (April 2019), online: *Embassy of Canada to Japan* <www.canadainternational.gc.ca/japan-japon/bilateral_relations_bilaterales/index.aspx?lang=eng>.
Greenleaf, Graham. *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Country Studies – B5 Japan* (2010).
House of Commons. *Privacy and Social Media in the Age of Big Data*, Report of the Standing Committee on Access to Information, Privacy and Ethics (2013).
———. *Towards Privacy by Design : Review of the Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics (2018).
Hunt, Chris DL & Nikta Shirazian. "Canada's Statutory Privacy Torts in Commonwealth Perspective", (2016), online: *Oxford University Comparative Law Forum* <ouclf.iuscomp.org/canadas-statutory-privacy-torts-in-commonwealth-perspective/>.
International Conference of Data Protection and Privacy & Commissioners. *Resolution on Privacy by Design* (2010).
Japanese Industrial Standard (JIS). *Personal Information Protection Management Systems - Requirements (JIS Q 15001: 2017)* (2017).
———. *Requirements for Compliance Program on Personal Information Protection (JIS Q 15001)* (1999).
JETRO. "FY2018 JETRO Survey on Business Conditions for Japanese Companies in Canada (29th annual survey)", (18 March 2019), online: *JETRO - Japan External Trade Organization* <www.jetro.go.jp/en/news/releases/2019/e182395e4fbd1d5b.html>.
———. *FY2018 Survey on the International Operations of Japanese Firms - JETRO Overseas Business Survey* (2019).
JIPDEC. *Minkan bumon ni okeru kojin jōhō hogo no tameno gaidorain* [Guideline for Protection of Personal Information in the Private Sector] (1988).
———. "Nintei kojin jōhō hogo dantai [Accredited Personal Information Protection Organization]", (13 May 2020), online: *JIPDEC* <www.jipdec.or.jp/protection_org/about.html>.
———. "Outline and Objective | PrivacyMark System", (2018), online: *PrivacyMark System* <privacymark.org/about/outline_and_purpose.html>.
———. *The PrivacyMark System* (2017).

Kawai, Rihoko & Consumer Affairs Agency. *Shogaikokuto ni okeru kojin joho hogo seido no kantoku kikan ni kansuru kento iinkai hokokusho* [Report of Study Committee on Supervisory Authority concerning Personal Information Protection Legal System in Other Countries] (2011).
Kuneva, Meglena. *Roundtable on Online Data Collection, Targeting and Profiling* (Brussels, 2009).
Law Reform Commission of Hong Kong. *Civil Liability for Invasion of Privacy* (2004).
Ministry of Economy, Trade and Industry. *Keizai sangyō bun-ya no uchi kojin iden jōhō wo mochiita jigyō bun-ya ni okeru kojin jōhō hogo gaidorain* [Guidelines for Personal Information Protection in the Business Using Individual Genetic Information in the Economy, Trade and Industry Field] (2017).
Ministry of Foreign Affairs of Japan. *Kaigai zairyu hojinsu chosa tokei (Heisei 30 nen yoyaku ban)* [Annual Report of Statistics on Japanese Nationals Overseas (Summary of 2017)] (2017).
Ministry of International Trade and Industry. *Minkan bumon ni okeru denshi keisanki shori ni kakaru kojin jōhō no hogo ni kansuru gaidorain* [Guideline on Protection of Personal Information Pertaining to Electronic Data Processing in the Private Sector] (1997).
Mladen, Caryn. *Privacy in Canada* (2003).
Morikawa, Mitsuo, ed. *Kindai shingo to shakai jōshiki* [Modern New Words and Social Common Knowledge] (kin-ensha, 1965).
Moyse, Pierre-Emmanuel. *Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé* (2018).
OECD. *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(80)58/FINAL (1980).
———. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(80)58/FINAL (1980).
———. *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc No C(2013)79 (2013).
———. *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, Doc No DSTI/ICCP/REG(2010)6/FINAL (2011).
———. *The OECD Privacy Framework* (2013).
Office of the Privacy Commissioner. *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (2017).
———. "2019-20 Departmental Plan", (11 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2019-2020/dp_2019-20/>.
———. *Consent and privacy - A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* (2016).
———. "Consultation on consent under PIPEDA", (24 May 2018), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/>.
———. *Data Brokers: A Look at the Canadian and American Landscape* (2014).
———. *Guidelines for Processing Personal Data Across Borders* (2009).
———. "Overview of Consent Submissions", (5 October 2016), online: *Office of the Privacy Commissioner* <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_intro/>.

———. “Personal information transferred across borders”, (14 December 2018), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/>.
———. “PIPEDA in brief”, (May 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/>.
———. “PIPEDA Report of Findings #2019-001: Investigation into Equifax Inc. and Equifax Canada Co.’s compliance with PIPEDA in light of the 2017 breach of personal information”, (9 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/>.
———. “PIPEDA Report of Findings #2019-002: Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia”, (25 April 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>.
———. “Privacy Law Reform: A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy”, (10 December 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/>.
———. “Provincial and territorial privacy laws and oversight”, (6 November 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/>.
———. “Reforming Canada’s privacy laws: Shifting from the whether to the how”, (23 May 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-news/speeches/2019/sp-d_20190523/>.
———. “Statistics Canada: Invasive data initiatives should be redesigned with privacy in mind”, (9 December 2019), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and- decisions/investigations/investigations-into-federal-institutions/2018-19/pa_20191209_sc/>.
———. “Submission: Modernizing Consent and Privacy in PIPEDA”, (5 October 2016), online: *Office of the Privacy Commissioner of* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_35/>.
———. “Summary of privacy laws in Canada”, (January 2018), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>.
———. “The Application of PIPEDA to Charitable and Non-Profit Organizations”, (June 2019), online: *Office of the Privacy Commissioner of Canada* <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_19/>.
———. *The Case for Reforming the Personal Information Protection and Electronic Documents Act* (2013).
Office of the Privacy Commissioner of Canada & Paul-André Comeau. *Control Authorities: Personal information in the French-speaking world* (2007).
Perlstein, Rick. *Britannica Academic* (2017).
Personal Information Protection Commission. *Kojin jōhō no hogo ni kansuru hōritsu nitsuite*

nogaidorain (tsūsoku hen) [Guidelines to the Act on the Protection of Personal Information (General)] (2016).
———. *Kojin jōhō hogohō seido kaisei taikō* [Reform Proposals of Act on the Protection of Personal Information] (2019).
———. *Kojin jōhō no hogo ni kansuru hōritsu nitsuite nogaidorain (tsūsoku hen)* [Guidelines to the Act on the Protection of Personal Information (General)] (2016).
———. "The List of Accredited Personal Information Protection Organizations", (1 April 2020), online: *Personal Information Protection Commission* <https://www.ppc.go.jp/personalinfo/nintei/list/>.
———. "Tokumei kakō jōhō [Anonymously Processed Information]", (10 February 2019), online: *Personal Information Protection Commission* <https://www.ppc.go.jp/personalinfo/tokumeikakouInfo/>.
Personal Information Protection Commission & Financial Services Agency. *Kin-yū bun-ya ni okeru kojin jōhō hogo ni kansuru gaidorain* [Guidelines for Personal Information Protection in the Financial Field] (2017).
Sato, Nobuyuki & Consumer Affairs Agency. *Shogaikokuto ni okeru kojin joho hogo seido no jittai chosa ni kansuru kento iinkai hokokusho* [Report of Study Committee on Actual Conditions Survey concerning Personal Information Protection Legal System in Other Countries] (2008).
Secretariat, Treasury Board of Canada. "Standard personal information banks", (20 March 2017), online: *Canada.ca* <www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/information-about-programs-information-holdings/standard-personal-information-banks.html>.
Senate of Canada. "Senate banking committee sheds light on Statistics Canada's secretive demand for Canadians' personal banking data", (11 December 2018), online: *Senate of Canada* <sencanada.ca/en/newsroom/banc-senate-banking-committee-statistics-canadas-secretive-demand-canadians-personal-banking-data/>.
Shimmura, Izuru, ed. *Kojien*, 4th ed (Tokyo: Iwanami Shoten, 1991).
———, ed. *Kojien*, 7th ed (Tokyo: Iwanami Shoten, 2018).
Study Group for Protection of Personal Information in National Administrative Bodies. *Gyōsei kikan ni okeru kojin jōhō no hogo taisaku no arikata ni tsuite* [Concept of Protective Measures for Personal Information Protection in Administrative Bodies] (1986).
Study Group on Personal Data. *Dai 7 kai pasonaru deta ni kansuru kentokai shiryo 1-2 (betten)* [Document 1-2 (Appendix) of 7th Meeting of Study Group on Personal Data] (2014).
Study Group on Protection of Privacy. *Kojin dēta shori ni tomonau puraibashī hogo taisaku* [Protective Measures for Privacy with Processing Personal Data] (1982).
TRC Inc. *Nihon sesōgo shiryō jiten: Shōwa sengohen 2 - Dai 4 Kan* [Japanese Word Reflecting Social Condition Encyclopedia; Showa after World War II Series 2 - vol. 4] (Tokyo: TRC Inc, 2008).
TrustArc. "APEC CBPR and APEC PRP Privacy Certifications", (12 June 2019), online: *TrustArc* <www.trustarc.com/products/apec-certification/>.
Vandergrift, Ellen. "Possible expansions to claims for breach of confidence", (29 May 2015), online: *Business Torts in Canada* <businesstorts.ca/blog/2015/5/29/possible-expansions-to-claims-for-breach-of-confidence>.
Wasser, LyndsayA & Mitch Koczerginski. *Can you keep a secret? The courts recognize a new tort for public disclosure of private facts* (2016).
The Oxford English Dictionary Online (Oxford University Press, 2020).