Smart City Privacy in Canada

By **KERI GRIEMAN**

JANUARY 2019

This report was produced by CIPPIC as a part of the "The Privacy Implications of Smart Cities" project. This project is led by Sara Bannerman, Canada Research Chair in Communications Policy and Governance, McMaster University and Angela Orasch, PhD Candidate, McMaster University.

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

cippic

CIPPIC is the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, and is a legal clinic based at the Centre for Law, Technology & Society (CLTS) at the University of Ottawa, Faculty of Law. Its core mandate is to ensure that the public interest is accounted for in decision-making on issues that arise at the intersection of law and technology. It has the additional mandate of providing legal assistance to under-represented organizations and individuals on law and technology issues, as well as a teaching mandate focused on providing law students practical training in a law and technology setting.

CIPPIC website: cippic.ca (The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic)

Project website: smartcityprivacy.ca/ (The Privacy Implications of Smart Cities)

With Contributions by:

David Fewer

Sara Bannerman

Pam Dheri

Matt Westwell

Michael Kemberhouse

Serguei Tabatchenko

With thanks to:

Angela Orsach

Reem Said

Morgan Lee

Amir Shafie

Design by:

Nathan Hoo

Cover Photo by:

Johann Kwan

CONTENTS

INTRODUCTION

The term 'smart city' encompasses a range of technological applications in urban environments. These range from a single application, such as a smart electricity grid usage tool for reducing energy costs, to a section of a city integrating numerous smart city technologies, such as Sidewalk Labs' Waterfront Toronto project. Smart city technology producers promise many things: more efficient transportation and travel, reduced resource use, and better access to facilities for residents, to name a few. Cities are eager to embrace this vision of the 'smart city,' both to better inhabitants' lives and to improve efficiency. However, smart city technologies raise social and privacy concerns.

The core of smart city technologies is data. Companies that sell smart city technologies suggest that cities can become "smart" by analyzing data on how people interact with the city, services, objects, and each other. This view on how to make cities "smart" is contested. As Rob Kitchin, author of *The Data Revolution* (2014), suggests, urban problems are complex and do not necessarily have technological solutions.[1] Rather, they may require political and social solutions. Introducing networked urban infrastructure has profound consequences that could add to, rather than reduce, the social, ethical and political problems of municipal governance. Privacy is at the forefront of these concerns.

Data has many uses. These include beneficial public uses, such as understanding traffic flows for the purposes of road planning. They also include commercial uses, such as the collection of personal information to help target advertisements by customer interests or location. Such uses may compromise individuals' privacy. Some privacy trade-offs may appear to be straightforward and beneficial, such as allowing emergency services access your location to know where to provide assistance. Others are more complicated: should a taxi app have access to your location and transportation habits in order to offer you ride deals? Should it be able to share your location and ride habits with advertisers?

An average day of interaction with smart technologies can produce a great deal of data. Imagine waking up in the morning: your smart power-integrated thermostat raises the temperature in your home when you get out of bed. You start your coffee machine through its app as you get into the shower so you'll have a fresh cup ready to go. You get on the bus with your metro pass, but your traffic app lets you know part way through your commute that the bus will be stopped in traffic at an accident, so you hop off and continue to work with a ride-sharing app. Your ID tag lets you into your office. You digitally exchange contact information with someone you meet through work. After work, you stop by the mall to redeem some shopping credit points. The weather is nice, so you take a bike-share cycle home. On the way you notice that a planter on your boulevard has been knocked over, so you report it with a 311 app. After supper, you throw the refuse into a single bin, and the bin's RFID tag alerts a collection service that the bin is full. These are just a few examples of the hundreds of data interactions that individuals experience in a day. Each of these interactions leaves a data trail, and each of these trails leads back to you.

Data analytics have evolved to the point that smaller and smaller bits of information can be used to create a profile of an individual. For example, an individual using a streaming service may not realize that their age, gender, and nationality can be predicted from their music choice.[2] Moreover, information collected from a variety of sources can make that profile increasingly accurate. This becomes increasingly important when expanded to smart cities,

1 Rob Kitchin, *The data revolution: Big data, open data, data infrastructures and their consequences* (Sage, 2014) at chapter 10.

2 Thomas Krismayer et al, "Prediction of User Demographics from Music Listening" (Paper delivered at 15th International Workshop on Content-Based Multimedia Indexing, Florence, 19-21 June 2017) [unpublished], online (pdf): *ACM Digital Library* <dl.acm.org/citation.cfm?id=3095722> [https://perma.cc/96TE-6S33].

where mass amounts of data may be collected, including concrete data such as current location. This data is valuable to companies for purposes such as marketing and behavioural targeting, and also potentially to those intending to infringe privacy directly. Data can also be used in ethically questionable ways, such as discriminatory pricing based on consumer attributes, or the use of racial profiling in advertisements.[3]

There are four main entities in the smart city space: municipal and government agencies; businesses and private organizations; communities as a whole; and individuals. However, the reality is that the lines between these groups are often blurred. There can be public-private partnerships between government and private actors, private actors undertaking activities usually undertaken by governments, communities working with either government or private actors to meet the needs of resident individuals, and many other possible combinations. While smart cities are intended to better the experience of communities and individuals, they typically purport to do so by improving some aspect of how a public or private entity functions, in order to provide a better or more efficient service. Government entities are increasingly partnering with private sector entities to provide smart services, and can do so in a variety of ways: services created by a government entity may be transferred to a private entity; a service might be privately-owned but government operated; or it might be government-owned and privately operated. There are also different levels of cooperation within these types. The Ontario highway 400, for example, has both privately leased segments and publicly-owned segments, while the city of Toronto has contracted with Sidewalk Labs to deliver city services in the area of Quayside West, with a level of integration with the rest of the city.

Outline

This report examines the interplay between privacy legislation and smart cities. It asks how Canadian privacy legislation applies in the context of smart cities, and how municipalities aiming to incorporate smart city technologies can navigate applicable laws, focusing on federal privacy laws. Part one examines the jurisdiction and applicability of federal privacy law to smart city contexts. Part two reviews key principles of Canadian federal privacy law that are particularly salient in a smart city context, asking how personal information can be used, and what exceptions exist to privacy legislation that are particularly important in the smart city context. Part three examines specific examples of smart city activities and technologies, and considers the applicability of federal privacy regimes to each. The report concludes with a summary of potential approaches to privacy problems in smart cities.

3 Office of the Privacy Commissioner of Canada, *Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*, by the Policy and Research Group of the Office of the Privacy Commissioner of Canada (Gatineau: OPC, May 2016), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/> [https://perma.cc/Z645-3CST] [OPC, "Consent"].

PART 1: Jurisdiction

Federal Privacy Law and Smart Cities

The division of powers set out in the Canadian Constitution allows for both provincial and federal governments to enact laws over their realms of competence. Indeed, both levels of government have enacted privacy laws. Federal privacy laws set overarching standards, to which provincial privacy laws must conform if addressing concurrent areas. When do federal privacy laws apply to smart city technologies and activities?

Privacy legislation in Canada seeks to defend the privacy rights of those in Canada by settings standards and practices that businesses and organizations interacting with Canadians must follow. For the private sector, this is largely federal – harmonizing requirements and expectations across the country. Where provincial laws apply, they must be substantially similar to federal requirements (see Annex 3).

Which privacy laws have jurisdiction over an activity depends on many things: what data is being collected, who is collecting it, how it is being collected, and where it is being collected. Privacy legislation focuses on two distinct points: personal information, and consent to use it.

There are two federal privacy laws: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The *Privacy Act* governs the handling of personal information by federal government institutions. The *Privacy Act* has jurisdiction over federal institutions listed in the act, such as the Canada Revenue Agency and the Department of Health. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is the federal privacy law for private-sector organizations, laying out how businesses must handle personal information. This includes large chains such as supermarkets, but also small businesses.

Commercial Activity

PIPEDA broadly applies to commercial activities across Canada, except in Alberta, British Columbia, and Quebec. These three provinces have privacy legislation that is officially deemed substantially similar to PIPEDA. In these cases, provincial legislation has exclusive jurisdiction over the collection, use, and disclosure of information in that particular province.

Provinces that do not have 'substantially similar' legislation are subject to PIPEDA, but are also subject to their own local privacy legislation as well. In Ontario, for example, this would include the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

What is, and what is not, a commercial activity? The answer to this question is not always simple. Definitions of commercial activity vary. PIPEDA's definition of commercial activity includes whether there is commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists. This is not particularly demonstrative. In surveying other legislation that defines commercial activity, the general characteristics include reference to its 'commercial character,' having the purpose of making a profit, and considerations of the purpose and nature of the activity (See Annex 2).[4] Case law states that

4 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2(1); *Ontario (Regional Assessment Commissioner) v Caisse populaire de Hearst Ltée*, [1983] SCJ No 8, [1983] 1 SCR 57; see also, *Re Windsor-Essex County Real Estate Board and City of Windsor*, [1974] OJ No 2135, 6 OR (2d) 21 (Ont CA); *State Immunity Act*, RSC 1985, c S-18, s 2; *Canada-European Union Comprehensive Economic and Trade Agreement*, 30 October 2016(entered into force 21 September 2017); *Harmonized Sales Tax Act*, SNB 1997, c H-1.01; *Act respecting the Québec sales tax*, CQLR c T-0.1, s 1; *State Immunity Act*, RSC, 1985, c S-18; *Re Canada Labour Code*, [1992] SCJ No 49, 91 DLR (4th) 449 (SCC); *University of Calgary v Colorado School of Mines*, [1995] AJ No 1026, [1996] 2 WWR 596 at 608 (Alta QB); *Ferguson v Arctic Transportation Ltd* (1995), 101 FTR 16 (FCTD); *Butcher v Saint Lucia*, [1998] OJ No 2026 (Ont Div Ct); *Sarafi v Iran Afzal* (The), [1996] FCJ

commercial activity must be more than mere exchange of consideration. The question of what constitutes commercial activity is also fact-specific. A landlord collecting, using or disclosing a tenant's personal information to administer a lease is engaged in commercial activity, but a membership in a non-profit bike-share program is likely not.

Commercial activity includes activity that is not of direct commercial benefit. This can include something that makes the company better and thus more attractive to consumers. If a business installed canopies that retracted in nice weather and expanded in the rain, any information collected in relation to such canopies could still be considered associated commercial activity, as it makes the company more likely to attract customers in rainy weather. In 2008, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a complaint with the Federal Privacy Commissioner over several of Facebook's practices, resulting in the OPC stating that collection, use and disclosure of personal information for the purpose of enhancing the experience of users indirectly contributes to the success of the site as a commercial enterprise. In that sense, collection, use and disclosure of personal information in relation to a feature, without an obvious direct commercial link, can still be characterized as a commercial activity:

It is reasonable to assume that those features of the site that do not have an obvious link to its business model are included to enhance the user's experience on Facebook. Enhancing the experience likely encourages existing members to continue to use the site and presumably encourages others to join as well – thereby indirectly contributing to the success of Facebook as a commercial enterprise. In that sense, collection, use and disclosure of personal information in relation to a feature without an apparent direct commercial link can still be characterized as occurring "in the course of commercial activity" in the sense required under the Act.[5]

Non-profit or membership-based organizations such as car-share programs or homelessness charities may also be involved in smart city designs. The fact that an organization is non-profit or membership-based does not exclude it from commercial activity. If an activity "were found to serve, primarily, the administrative and organizational needs of its members and not educational or other public purposes," it would be found to have commercial activity.[6] Subsidy by a provincial or municipal government also does not mean there is no commercial activity – a daycare organization subsidized by a municipal government was found to be engaged in commercial activity.[7] On the other hand, a collection of membership fees in exchange for services and benefits of membership may constitute an exchange of consideration, but does not necessarily constitute commercial activity for the purposes of PIPEDA.[8] For non-profits,

---

No 519, 111 FTR 256 (FCTD); *El Ansari v Maroc*, [2003] JQ no 13913, JE 2003-1973 (Qc CA); *Accurso v Royaume du Maroc*, [2003] JQ no 18660, JE 2004-289 (CQ); *Alberta Personal Information Protection Act*, SA 2003, c P-6.5, s 56(1)(a); Vern Krishna, *Halsbury's Laws of Canada - Income Tax (General)* (Toronto: LexisNexis Canada, 2017); Ronald J Maddock & Brian C Pel, *Halsbury's Laws of Canada - Taxation (Goods and Services)* (Toronto: LexisNexis Canada, 2015); *Governor in Council Education Act Regulations*, NS Reg 74/1997, s 86; *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, s 1(1); *Excise Tax Act*, RSC 1985, c E-15, s 123(1); Halsbury's Laws of Canada (online), *Public International Law*, "Jurisdictional Immunities: State Immunity: Exceptions From Immunity" (VII.1.(2)) at HPI-81 "Commercial activity exception." (2014 Reissue); *Rodgers v Calvert* (2004), 244 DLR (4th) 479, 49 BLR (3d) 53 (Ont Sup Ct).

5 Office of the Privacy Commissioner of Canada, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, by Elizabeth Denham (Ottawa: OPC, 16 July 2009), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> [https://perma.cc/L88J-QRK7].

6 Office of the Privacy Commissioner of Canada, *Law School Admission Council Investigation* (Report of Findings) (Ottawa: OPC, 29 May 2008), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/389_rep_080529/> [https://perma.cc/LH4U-VZL9].

7 Office of the Privacy Commissioner of Canada, *Daycare denied parent access to his personal information* (Case summary) (Ottawa: OPC, 4 August 2005), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-309/> [https://perma.cc/9XSK-CEH7].

8 *Rodgers v Calvert* (2004), 244 DLR (4th) 479, 49 BLR (3d) 53 (Ont Sup Ct).

the key concern seems to be whether they were directly engaged in their core mandate – such as, for a university, education – or engaged in activity outside of that purpose that could be construed as commercial. For membership organizations, commercial activity analysis is more likely to hinge on whether compensation was received for a specific purpose rather than general benefits.

Jurisdiction over collection of information by a quasi-governmental provincial or municipal entity varies according to whether or not the activity is considered commercial. PIPEDA generally does not apply to organizations that do not engage in commercial activity, and thus does not generally apply to not-for-profit and charity groups; municipalities; universities; schools; hospitals; and political parties and associations.[9] However, PIPEDA will apply (in a province without substantially similar legislation) if the organization engages in a commercial activity outside its core activity, but that still involves personal information, such as a university selling an alumni list.

Federal works, undertakings, and businesses

PIPEDA applies to all federal works, undertakings, and businesses (FWUBs) such as banks, telecommunications, radio and television broadcasting, and airports. FWUBs are those that are under the legislative authority of Parliament. All private organizations in the territories are also considered FWUBs, and as such are subject to PIPEDA.[10]

If the organization is a FWUB, such as a telecommunications provider of an internet hotspot or internet booth, PIPEDA applies regardless of whether there is commercial activity.[11] If the organization is not a FWUB, there needs to be commercial activity for PIPEDA to apply.

There are many examples of FWUBs that operate in the context of smart cities. Not only are internet service providers FWUBs, but so are airports - where airport apps and kiosks are used for passport processing and traveler guidance.

Health sector

Ontario, Nova Scotia, New Brunswick, and Newfoundland have legislation that is deemed substantially similar to PIPEDA, but only in the health sector (see Annex 3). These four provinces have exclusive jurisdiction over personal information collected, used, or disclosed by health information custodians such as doctors and pharmacists. The definition of what constitutes a health information custodian varies with provincial legislation, but broadly speaking applies to health care professionals who are in direct contact with personal information about an identifiable individual. There are exceptions to this rule; for example, a doctor performing an independent medical examination (such as for insurance purposes) is not considered a health custodian in Ontario, and thus the personal information produced from such an examination will fall under PIPEDA rather than Ontarian health legislation (the *Personal Health Information Protection Act*).[12]

A growing number of smart city initiatives are taking place in the health sector. Cities have

---

9 Office of the Privacy Commissioner of Canada, *Summary of privacy laws in Canada* (Ottawa: OPC, January 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/> [https://perma.cc/YYG5-6PET] [OPC, "Summary"].

10 *Ibid*.

11 Office of the Privacy Commissioner of Canada, *Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts* (Ottawa: OPC, November 2004), online: *Office of the Privacy Commissioner of Canada* <https://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/> [https://perma.cc/W7ZR-C7RF] [OPC, "Questions and Answers"].

12 *Wyndowe v Rousseau*, [2008] FCJ No 151, 71 Admin LR (4th) 58 (FCA).

adopted apps, data systems, and health education initiatives as part of their smart city strategies.

Trans-border information transfers

Where information pertaining to commercial activity crosses a provincial, territorial, or national border, the transfer will be subject to PIPEDA – even if it is being transferred from or to a province with substantially similar legislation. This is also true if it is being transferred to another country.

Transfers of information further complicate jurisdictional analysis. Sub-contracting, or even sharing information between different parts of an entity, can involve different legislation. Broadly speaking, the initial application of jurisdiction will 'follow' information – if a bank, as a FWUB, subcontracts processing of information to a non-FWUB, then PIPEDA will still apply to that information, and the bank will still be responsible for ensuring that the data is treated properly. If an entity subject exclusively to provincial legislation contracts out to an entity subject to PIPEDA, then the contractor will have to comply with provincial legislation for the treatment of the information being transferred. There are instances where jurisdiction will not 'follow.' For example, if a non-FWUB entity engaged in commercial activity in Quebec transferred information to a non-FWUB entity in Alberta, then Quebec legislation would apply to the information before the transfer, PIPEDA to the transfer itself, then Albertan legislation after the transfer.

Transfer of information can also be considered incidental, in which case PIPEDA may not apply. If a complaint is made about the treatment of information in a province, and transfer across provincial lines is incidental, then PIPEDA may not be invoked. The substance and character of the interaction will be considered in such cases. If, for example, a customer in a province with 'substantially similar' legislation were to use a retail store credit card, which the store checked against their records in an office in another province, and the customer subsequently made a complaint about the collection of a phone number during the transaction, then the transfer of information (requesting information about the store credit card) was incidental to the actual cause for complaint, and thus the substantially similar provincial legislation would apply and not PIPEDA.[13]

Cross-border information transfers are significant to smart cities. Many smart city technologies are part of the 'internet of things,' and so transfer collected data via the internet. Due to the hub nature of the internet, information may in fact pass international borders through a large hub in another country before returning to Canada, even if the destination is relatively geographically close to the original collecting tool. A municipal bike counter, for example, may collect information locally in a city, but transmit its count through the internet, and thus across borders, before reaching its destination in the same city.

Employment

PIPEDA does not apply to personal information of employees in areas of provincial jurisdiction. For example, personal information about customers collected by a provincial adult education app in Saskatchewan would be subject to PIPEDA if the app involved commercial activity. However, personal information regarding employees of that same provincial app would not be subject to PIPEDA, as education is a provincial matter.

13 OPC, "Questions and Answers", *supra* note 11.

Dual jurisdiction

Some entities can be subject to both a provincial privacy law and PIPEDA. In this case, the federal Office of the Privacy Commissioner recommends that the organization in question look at the differences between the laws, and follow the more stringent requirements. For example:

> Alberta's and British Columbia's [privacy legislation deemed substantially similar to PIPEDA] have "grandfathering clauses" that deem information collected before January 1, 2004 to have been collected with consent. PIPEDA however, may require that organizations obtain consent to use and disclose information collected before PIPEDA came into force. If your organization has to comply with both pieces of legislation, you could ensure that you communicate with your customers to confirm their continued consent for the collection, use and disclosure of that information. You would be going further than required by [provincial legislation], but would not be contravening it.

Jurisdiction as a Whole

There are some straightforward applications of privacy legislation to public and private activities in Canada. Federal government activity is governed the the *Privacy Act*. Federally regulated activities such as aviation are under PIPEDA. Provincial government activity is governed by provincial privacy laws, which in Ontario are FIPPA and MFIPPA. Commercial activity in provinces other than British Columbia, Quebec, and Alberta is governed by PIPEDA. There are certain sector-specific carve-outs for health related information. So a smart city company operating commercially in Ontario that does not deal with health information would *prima facie* be governed by PIPEDA.

Determining jurisdiction becomes more difficult when the lines between these activities are less distinct. For example, municipal activity is not covered by PIPEDA, while commercial activity by a private company is. So information collected by the city in the course of regular municipal activity, such as using a sensor to count vehicles as part of road maintenance detection, is not covered by PIPEDA, whereas a privately owned mall tracking customers is covered by PIPEDA.[14] What if the city hires an independent contractor to do their counting? The privacy obligations of the city are likely to attach to the contractor, who is in effect stepping into the shoes of the city. But those specific legislative obligations blur, the further the contractor's activities range from core municipal services. What if the contractor is a private company carrying out additional activities of a commercial nature that are nonetheless related to the government activity? For example, a company may display ads while it is counting bikes. While additional activities can be built into the contract between the city and private party, there is no defined line as to where an activity's nature slips from municipal to commercial, particularly where the activity is shared between public and private actors. Partnerships may have clearly defined responsibilities in terms of actions to be performed, such as data control activities, but these actions, particularly in the smart city context, do not fit in perfect jurisdictional boxes.

Where the applicable privacy law is unclear, regulatory uncertainty becomes a barrier to innovation in the provision of public services. The restrictions and obligations of public and private parties differ. Smart city applications highlight the growing difficulty of extricating defining characteristics for the purposes of jurisdiction when public/private partnerships are formed.

14 Adam Toy, "Alberta Privacy Commissioner investigating use of facial recognition software in Calgary malls", *Global News* (3 August 2018), online: <https://globalnews.ca/news/4370735/alberta-privacy-commissioner-investigating-facial-recognition-software-calgary-mall/> [https://perma.cc/5C2K-4LF6].

PART 2: Key Principles

Privacy Principles

While determining which privacy law applies in a particular situation can be complicated, Canadian privacy legislation as a whole attempts to ensure that individual privacy is protected according to certain standard principles. PIPEDA and substantially similar legislation are based on ten principles of fair information: that entities be held accountable for the data they collect; that the purpose for collection be identified; that consent be obtained before collection; that collection be limited to only what is necessary for the identified purpose; that use, disclosure, and retention be limited to only what is necessary; that data collected be accurate; that there are safeguards in place to protect the data; that there is an air of openness around the collection process at all levels; that individuals be able to access data collected; and that the compliance of entities collecting, using, or disclosing information can be challenged. Provincial legislation such as Ontario's FIPPA and MFIPPA also emphasize safeguards - the question of whether reasonable steps have been taken to protect the "privacy and security of the records in its custody and control."[15] This is particularly important for smart city entities that contend to run on such data.

What is personal information?

While definitions of what is considered personal information may vary slightly, personal information generally refers to, as PIPEDA states, "information about an identifiable individual."[16] This includes obvious information such as a name or address, but also information such as an email address or pupillary patterns.

Consent

Consent is the cornerstone of privacy legislation.[17] While there are specific exceptions, generally consent must be obtained for organizations to collect, use, or disclose personal information. Consent is a way for individuals "to protect their privacy by exercising control over their personal information – what personal information organizations can collect, how they can use it, and to whom they can disclose it."[18] The consent requirement is intended to protect individual autonomy by letting individuals decide the sensitivity of their own information and determine when they choose to share it. Consent is intended to be granular – particularized to a situation and set of circumstances.

Consent is particularly important in terms of collecting information. Privacy legislation attempts to ensure that entities are obtaining proper consent for collecting information. Closely tied to this is whether the consent is obtained for what the information is actually being used for; otherwise the consent is meaningless. An individual consenting to a government entity acquiring their personal information for a survey is not inherently consenting to having the information tied to them and disclosed publicly. Concerns such as 'scope creep' refer to the issue of entities obtaining meaningful consent for a particular use, but using the information for additional or more expansive purposes.

---

15 Information and Privacy Commissioner of Ontario, *Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions* (Toronto: IPC, February 2016) at 10, online (pdf): *Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/2016/08/thinking-about-clouds-1.pdf> [perma.cc/FKH3-QSPA].

16 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2(1) [*PIPEDA*].

17 *Ibid*.

18 OPC, "Consent", *supra* note 3 at 2.

Challenges to the concepts of personal information and consent

The concepts of 'personal information' and 'consent' are challenged in the smart-city context. The Privacy Commissioner of Canada points out that while data that is not personally identifiable does not meet the legal definition of 'personal information' and is thus generally not covered by privacy regulation, the "purpose of big data algorithms is to draw correlations between individual pieces of data. While each disparate piece of data on its own may be non-personal... Big data analytics has the ability to reconstitute identities that have been stripped away."[19] Large amounts of data collected in a smart-city context also challenges notions of consent; while individual collection may have received consent, the amalgamation of data may go beyond what was consented to.

Obtaining meaningful consent for collection of data will be a challenge for smart cities, as will limiting the use of that information. It may be necessary to ascertain new modes of ascertaining consent in a smart city context. Going forward, it will be important to reconcile these aims and approaches in order to achieve a balance between the potential benefits of smart cities and the need to protect individual privacy, particularly in regard to transparency of collection and use.

Reasonable uses

Section 5(3) of PIPEDA states that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances,"[20] even if the collector has consent.[21] Analysis of what is appropriate is evaluated contextually, and courts have considered whether "1) the collection, use or disclosure of personal information is directed to a bona fide business interest, and 2) whether the loss of privacy is proportional to any benefit gained."[22] The Federal Court of Appeal has affirmed that the following factors will be used in evaluating whether an organization's purpose is in compliance with 5(3):

- The degree of sensitivity of the personal information at issue;
- Whether the organization's purpose represents a legitimate need / bona fide business interest;
- Whether the collection, use and disclosure would be effective in meeting the organization's need;
- Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- Whether the loss of privacy is proportional to the benefits[23]

Reasonable use in the smart city space will be fact specific. Consider a smartwatch with a pulse rate monitor. A bike-share app could try to ensure that the only person using the bike was the person who is registered with the app by recording pulse rate averages and whether the

---

19 *Ibid* at 7.

20 *PIPEDA*, *supra* note 16, s 5(3).

21 Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* (OPC: Ottawa, May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/> [perma.cc/96V9-D5N7].

22 *AT v Globe24h.com*, 2017 FC 114 at para 74 [*AT*].

23 *Turner v Telus Communications Inc*, 2005 FC 1601 at para 48. See also *AT*, *supra* note 22 at para 74; *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at paras 127, 177, 179–181; *Penny Lane Entertainment Group v Alberta (Information and Privacy Commissioner)*, 2009 ABQB 140 at paras 58–61; *Leon's Furniture Limited v Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94 at paras 58–62.

watch was removed, but it is not reasonable to use a pulse tracker to ensure this. It is sensitive information that is particularly invasive compared to the proportionate benefit.

Exceptions for research, journalistic, artistic and literary uses

Research, journalistic, artistic, and literary activities are exempt from the requirement to obtain consent for data use and disclosure under PIPEDA. Smart city technology companies may assume that they can rely on the research exemption with the expectation that their collection of large amounts of data will inherently qualify as research. This is not necessarily the case. PIPEDA and jurisdictions with 'substantially similar' legislation each have slightly different requirements for the research consent exemption, but in general, legislation requires using the information in a way that maintains confidentiality, that consent be impracticable to obtain, and that the organization inform the Privacy Commission *before* personal information is used for the research purpose.[24] A more thorough examination of the research exception requirements contained in legislation deemed substantially similar to PIPEDA can be found in Annex 1.

PART 3: Privacy and Smart City Technologies

Introduction

Different technologies present different concerns and jurisdictional questions. Case studies of specific technologies help to illustrate their place in the smart city ecosystem, some of the challenges in determining which level of jurisdiction applies, and some of the privacy problems they raise.

1) Bike-sharing programs

A bike-share program can help to combat automobile congestion, reducing environmental impact. Typical bike-share programs will have trackers placed on the bikes in order to locate lost bikes, to keep track of the number of bikes per area, and to charge users. Generally such programs will not be FWUBs. Often, bike sharing programs will constitute commercial activity, as users tend to pay for either time used or pre-set time blocks. If the bike share program is in Alberta, British Columbia, or Quebec, it will be governed by the provincial legislation. If it is in a territory, PIPEDA will apply by default. If it is in a province other than Alberta, British Columbia, or Quebec, then PIPEDA will apply. If the bike-share program is a city project, then employee personal information may not be subject to PIPEDA. If it is a non-government project, then PIPEDA will apply to all personal information.

If the bike-share organization is in more than one province, then PIPEDA will apply to the transfer of information over provincial, territorial, or national lines. The organization must receive consent from a user to collect their information. It must also restrict itself only to what information would be reasonably suspected for operating such a program: location of the bike in use, name, and billing information, for example.

If the bikes had a heart-rate monitor, then the collection of this information might not be considered appropriate by a reasonable person under the circumstances, particularly if they were unaware of the monitor. In provinces with 'substantially similar' health legislation – Ontario, Newfoundland, Nova Scotia, and New Brunswick – the organization is unlikely to be considered a health (information) custodian, so PIPEDA is likely to apply. Complaints could

24 Éloïse Gratton, "The Consent Exception for Research Purposes" (3 June 2016), online (blog): *Éloïse Gratton* <https://www.eloisegratton.com/blog/2016/06/03/the-consent-exception-for-research-purposes/> [perma.cc/858M-8TGV].

potentially be raised to the Office of the Privacy Commissioner of Canada if information was disclosed that included the heart-rate monitor, as a consumer would not necessarily consider it reasonable under the circumstances, and PIPEDA would apply.

Bike-sharing programs raise several privacy concerns, particularly involving consent and limiting collection under PIPEDA. A user who voluntarily accepts terms of service in a bike-sharing may not understand what data is collected or even what cross-analyses are possible with the data collected.[25] For instance, credit card information used to purchase time on a bike can be combined with electronic IDs on a bike-sharing app, card, or key. Data on where a person travels, when, and how regularly, combined with other private information is incredibly valuable for targeted advertising. Business and urban planning academics say this is precisely how bike-shares make most of their money: selling their data on users, combined with data from private companies that invest in bike-shares.[26] This issue is amplified in situations where, as some bike-sharing services implement in their terms of service, there is a possibility of tracking users when they aren't currently using a bike.[27]

Privacy concerns also arise under PIPEDA for disclosure to third parties, particularly the government. For planning purposes, many North American cities have started asking bike-sharing and scooter companies to share data with them up-front.[28] The cities of Ottawa and Gatineau even signed a data-sharing agreement with Strava, which tracks users' GPS location while cycling.[29] As noted by Professor Teresa Scassa, given the data is still owned by Strava, it is not open data and is thus immune to access to information requests.[30] This increasingly common type of data-sharing has transparency concerns, and in turn prevents an adequate assessment of privacy concerns.

Under PIPEDA, safeguards are also a large concern for bike-sharing programs. First, some bike-sharing programs are more vulnerable to breaches. For bikes that do not have a docking station and are instead left where convenient, hackers can more easily decode the anonymous identities companies assign to users, as well as their trips.[31] Second, data localization issues may make large swathes of personal and group data accessible to foreign governments. For instance, certain Chinese companies like Ofo and Mobike operating in the US both reserve the right to process data collected outside the US, where it is not subject to the same data-protection rules.[32] In both instances, absent adequate safeguards, individuals may be subject to huge intrusions upon their private data.

---

25 Fábio Duarte, "Disassembling Bike-Sharing Systems: Surveillance, Advertising, and the Social Inequalities of a Global Technological Assemblage" (2016) 23:2 J of Urban Technology 103.

26 Stephanie Gardiner, "How Your Personal Information Funds Share Bike Schemes", *Sydney Morning Herald* (14 November 2017), online: <https://www.smh.com.au/business/consumer-affairs/how-your-personal-information-funds-share-bike-schemes-20171110-gzj05d.html> [perma.cc/HY6X-JA2A].

27 Naaman Zhou, "Dockless Bike Share: Privacy and Safety Concerns Voiced Ahead of Sydney Launch", *The Guardian* (25 June 2017), online: <https://www.theguardian.com/australia-news/2017/jun/25/dockless-bike-share-privacy-and-safety-concerns-voiced-ahead-of-sydney-launch> [perma.cc/3EWS-4M3E].

28 Aarian Marshall, "Still Smarting from Uber, Cities Wise Up About Scooter Data", *Wired* (18 September 2018), online: <https://www.wired.com/story/cities-scooter-data-remix-uber-lyft/> [perma.cc/F7T6-7QJ9].

29 Trevor Pritchard, "Ottawa-Gatineau Cyclists Urged to Map Their Journeys", CBC (22 April 2016), online: <https://www.cbc.ca/news/canada/ottawa/strava-app-ottawa-1.3546513> [perma.cc/CR7W-KG86].

30 Teresa Scassa, "Sourcing Cycling Data From the Private Sector: Some Questions About Data Analytics and City Planning" (25 April 2016), online (blog): *Teresa Scassa* <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=213:sourcing-cycling-data-from-the-private-sector-some-questions-about-data-analytics-and-city-planning&Itemid=81> [perma.cc/S2K3-MJ9T].

31 Elizabeth Woyke, "The Secret Data Collected by Dockless Bikes is Helping Cities Map Your Movement", *MIT Technology Review* (28 September 2018), online: <https://www.technologyreview.com/s/612123/the-secret-data-collected-by-dockless-bikes-is-helping-cities-map-your-movement/> [perma.cc/5QAZ-FMLG].

32 Laura Bliss, "Are Dockless Bikes a Cybersecurity Threat?", Citylab (15 February 2018), online: <https://www.citylab.com/transportation/2018/02/are-dockless-bikes-a-cybersecurity-threat/552206/> [perma.cc/ES74-9M4C].

2) Drones

Drones or unmanned air vehicles (UAVs) both refer to vehicles that can operate in the air without an onboard pilot, though they can vary in size, shape, form, and speed.[33] They fall into two broad categories: those that require a land-based pilot, and those than can operate with pre-set instructions. Drones are used for a variety of applications including surveillance, construction, agriculture, resource exploration, meteorology, mapping, and photography.

The *Aeronautics Act* regulations are the primary legislation governing drones, commercial or otherwise. For non-recreational uses where the drone is either over 35 kg or is used for purposes such as survey work, agricultural work, inspections, academic research, police work, aerial photography or aerial videography, a Special Flight Operations Certificate must be obtained by submitting an application to the local Civil Aviation regional office.[34] Criminal Code provisions also inform unsafe or illegal drone use, though Transport Canada has jurisdiction to investigate reports of unauthorized drone use.[35] Historically, the Supreme Court of Canada has been reluctant to expand the federal government's exclusive authority over aeronautic activities to the provinces.[36]

Consent for drone use varies. There are "no drone zones" where it is unsafe or illegal to fly at all, including airports and aerodromes; busy, populated areas; national parks; and border crossing. Transport Canada has pre-set conditions for use generally (such as 'lower than 90m above ground' and 'within sight at all times'), and permission is generally not required for drones flown for fun that weigh less than 35 kg.[37] Private organizations using drones for commercial purposes are regulated by PIPEDA, as drone footage can include personal information of an individual is capable of being identified, even if only in combination with other data.[38] This could include vehicle tracking with "persistent UAV surveillance."[39] Federal government departments are subject to the *Privacy Act*.[40] Typical data collection from drones includes photo, video, and audio footage, as well as geographic location.

Privacy concerns arise at distinct two stages: when drones are collecting data in the air and the drone owner's post-collection activities.[41] Aerial surveillance of people, either by governments or private actors, runs up against secrecy, autonomy, and anonymity conceptions of privacy.

If drones capture information about individuals in public spaces, it raises the question of whether people can have a reasonable expectation of privacy to data collected by drones. Privacy issues compound where drone data can be combined with other data to reveal new personal information about the individual. Where data is collected by the state, the additional question that arises is whether this constitutes unreasonable search and seizure under the

---

33 Office of the Privacy Commissioner of Canada, *Drones in Canada: Will the proliferation of domestic drone use in Canada cause new concerns for privacy?* (Ottawa: OPC, March 2013) at 2 [OPC, "Drones"]; Canada, Library of Parliament, *Civilian Drone Use in Canada*, by Jed Chong & Nicole Sweeney, Publication No 2017-23-E (Ottawa: Library of Parliament, 16 October 2017) at 1.

34 Transport Canada, *Applying for a Special flight Operations Certificate* (Ottawa: Transport Canada, 19 June 2018), online: <https://www.tc.gc.ca/eng/civilaviation/opssvs/applying-special-flight-operations-certificate.html> [perma.cc/29N7-S33S].

35 Transport Canada, *Flying your drone safely and legally* (Ottawa: Transport Canada, 19 June 2018), online: <http://www.tc.gc.ca/eng/civilaviation/opssvs/flying-drone-safely-legally.html> [perma.cc/C3WF-7B88] [Transport Canada, "Flying your drone"].

36 *Johannesson v Rural Municipality of West St Paul* (1951), [1952] 1 SCR 292, 4 DLR 609.

37 Transport Canada, "Flying your drone", *supra* note 35.

38 Ciara Bracken-Roche et al, "Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada: A Report to the Office of the Privacy Commissioner of Canada under the 2013-2014 Contributions Program" (30 April 2014) at 51, online (pdf): <https://www.sscqueens.org/sites/sscqueens.org/files/Surveillance_Drones_Report.pdf> [perma.cc/DZN7-D8RY].

39 *Ibid*.

40 OPC, "Drones", *supra* note 33.

41 United States of America, Congressional Research Service, *Domestic Drones and Privacy: A Primer*, by Richard M Thompson (Washington: CRS, 30 March 2015), online (pdf): <https://fas.org/sgp/crs/misc/R43965.pdf> [perma.cc/Q5NZ-MK4Z].

Charter.

Drone technology may also interfere with individuals' sense of personal autonomy. Some argue drone surveillance has the potential to alter individual behaviour when individuals know that their day-to-day activities may be surveilled.[42]

Depending on the data gathered, drones can infringe on the right to public anonymity. Drone surveillance over urban centres or large public events (e.g. sports venues, concerts, etc.) appear to pose a low risk for anonymity because the individual remains undifferentiated from the crowd. However, coupling drones with sensors such as automated licence plate readers and facial recognition technology has the potential to target surveillance to specific individuals and hinder one's anonymity in public spaces.[43]

3) Smart Utilities

Smart utilities include smart gas, electricity, and water technologies. Such technologies are integrated with a communication system that allows them to reduce pollutants and costs to consumers. While traditional utilities send power, water or gas in one direction, smart utility services can monitor and respond to consumer activity based on real-time usage. In the case of smart electrical grids, these can sometimes divert energy back to the grid when unneeded. Smart grids can also be integrated with smart appliances, such as smart refrigerators, light fixtures, and washer and dryers to further maximize energy efficiency.[44]

PIPEDA is well-suited to regulate smart utilities. Smart utilities generate a great deal of commercial data flow; consumers use private sector products to manage utility consumption; commercial activity occurs between utility provision and user; and information has the potential to cross provincial or national boundaries.[45] In terms of current utility companies, both Toronto Hydro and Hydro One refer to PIPEDA in data privacy management.

Consent for smart utility use is typically acquired when setting up a smart meter in a house or business. Consent, however, can be difficult to withdraw if, for example, there is a change of tenant, since withdrawal of consent may require dismantling the smart meter and replacing it with a non-smart meter.[46]

Data collection from smart grids covers electricity use. This can include which individual appliances are used and when. Experts note that data that may be harmless on its own can be a privacy threat when combined with other data, potentially including "how many people live in a household, their presence and absence at home, their schedules for taking showers, watching TV, frequency of microwave use, [and] their sleeping patterns."[47]

Smart utilities present numerous concerns under PIPEDA, particularly related to information disclosure. As noted by the federal Privacy Commissioner, sharing data from smart meter

---

42 John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (Chicago: University of Chicago Press, 2001); Julie E Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan L Rev 1373 at 1426.

43 Andrew Conte, "Drones with Facial Recognition Technology Will End Anonymity, Everywhere", *Business Insider* (27 May 2013), online: <http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5> [perma.cc/7C5J-3G2F].

44 Avner Levin & Colin Rogers, "Applying PIPEDA to the Smart Grid" (March 2011) at 22, online (pdf): <https://www.ryerson.ca/content/dam/tedrogersschool/privacy/documents/Applying_PIPEDA_to_the_Smart_Grid.pdf> [perma.cc/3QQP-JVSV].

45 *Ibid* at 26–27.

46 "FAQ: Changing a Meter", online: *Stop Smart Meters* <https://stopsmartmeters.org/frequently-asked-questions/changing-a-meter/#howchange> [perma.cc/2XKB-5SBN].

47 Farhan Siddiqui et al, "Smart Grid Privacy: Issues and Solutions" (delivered at the 21st International Conference on Computer Communications and Networks, July 2012) [unpublished], online: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6289304> [perma.cc/82JU-TND4].

usage with third parties is a common practice in North American jurisdictions.[48] Given the detailed information discernable from a household's energy usage, stakeholders, government, utility companies, law enforcement, researchers, and third-party service providers may have an interest in this information.[49] Clear disclosure practices are necessary to address concerns around information being disclosed potentially beyond the scope to which individuals consent, to avoid issues like price discrimination by landlords[50] or potentially invasive forms of targeted advertising.[51]

A large privacy issue for smart utilities relates to the whether information they collect is defined as personal information. Former Information and Privacy Commissioner of Ontario Ann Cavoukian, along with other academics, have highlighted the lack of a consistent definition for personally identifiable information in the context of smart grid technology.[52] Whether information is considered personal determines whether it garners any protection under PIPEDA. In the law enforcement context, the Supreme Court of Canada did not find that data from a police-installed ammeter measuring electricity use had a reasonable expectation of privacy.[53] In the commercial context, the definition is even less clear. This definition issue is compounded by the fact that utility companies' privacy policies may not adequately address new technologies.[54]

Another concern for smart grids under PIPEDA is ensuring adequate safeguards are in place. Smart utility technologies are susceptible to network attacks, data tampering and fabrication, and private information breaches, which may put a person's private information at risk to hackers.[55] Despite calls for closing vulnerability gaps in smart meter technology,[56] PIPEDA still offers little protection for private data from smart devices.[57] Data from smart-meters can potentially reveal what time a person leaves or arrives at their residence, whether a security system is activated, or whether a television is in use.[58] In the wrong hands, this information could result in significantly damaging breaches.

---

48 Office of the Privacy Commissioner of Canada, *The Internet of Things: An Introduction to Privacy Issues with a Focus on the Retail and Home Environments* (Ottawa: OPC, February 2016) at 8, online (pdf): *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/1808/iot_201602_e.pdf> [https://perma.cc/C5F5-ZE28] [OPC, "Internet of Things"].

49 Astrid Kalkbrenner, "Climate Change, Big Data Revolution and Data Privacy Rights" (2018) 32 J Envtl L & Pract 1 at 6 (WL).

50 Giovanni Buttarelli, "Opinion of the European Data Protection Supervisor on the Commission Recommendation on Preparations for the Roll-Out of Smart Metering Systems" (June 2012) at 6, online (pdf): <https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf> [https://perma.cc/YR3N-65NB].

51 Antonella Artuso, "Privacy Violation at Heart of City's Potential Plan to 'Mine' Smart Meters: Expert", *Toronto Sun* (30 April 2017), online: <https://torontosun.com/2017/04/30/privacy-violation-at-heart-of-citys-potential-plan-to-mine-smart-meters-expert-2/wcm/5e552184-4646-43cb-87fb-b8e8cf6229fe> [https://perma.cc/RT25-QLUM].

52 Ann Cavoukian et al, "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation" (2010) 3:2 Identity in the Information Society 275 at 284.

53 *R v Gomboc*, 2010 SCC 55 at para 1.

54 Samuel J Harvey, "Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid" (2014) 61 UCLA L Rev 2068 at 2078.

55 Asmaa Abdallah & Xuemin Shen, "Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks" (2017) 8:3 IEEE Transactions on Smart Grid 1064 at 1064.

56 Ashley Csanady, "Ontario's Smart Meters Vulnerable to Hacking and Present a Threat to the Grid, New Democrat Warns", *National Post* (10 November 2015), online: <https://nationalpost.com/news/politics/smart-meters-are-vulnerable-to-hacking-and-present-a-threat-to-personal-privacy-ontario-new-democrat-warns> [https://perma.cc/4XDT-4BFQ].

57 Rahul Kalvapalle, "Smart Devices Can Share Your Private Date, but Canada's Privacy Laws Offer Little Protection: Report", Global News (7 October 2017), online: <https://globalnews.ca/news/3791571/canada-privacy-laws-internet-of-things/> [https://perma.cc/9BEW-9PSB].

58 Cheryl Dancey Balough, "Privacy Implications of Smart Meters" (2011) 86 Chicago-Kent L Rev 161 at 167.

4) Cloud computing

Cloud servers are physical or virtual infrastructure that enable cloud computing.[59] Cloud servers have the same information storage function as traditional servers; however, the information is stored and accessed remotely over the internet from a cloud service provider rather than on one's physical device.[60] This can include running programs through the cloud rather than on the individual's device. Common cloud computing activities include storing photos or videos online; using online applications such as social media or email; or paying to store backup files online.[61]

Cloud computing has risen in popularity because it eliminates the need to invest in storage infrastructure, provides scalability, and connects to multiple devices to avoid storage duplication. The Pew Internet Survey "suggests that ease, convenience, and flexibility are at the root of this [considerable] uptake."[62] However, because information stored in cloud servers is often located physically outside Canada, it raises important jurisdictional questions about privacy and data protection.

The Privacy Commissioner of Canada oversees cloud computing through the lenses of both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[63] Government of Canada bodies are dealt with under the *Privacy Act*, whereas PIPEDA covers the "collection, use and disclosure of personal information by private sector organizations in the course of commercial activities," here under the federal government's trade and commerce powers.[64] The Federal Court of Canada has determined that the Privacy Commissioner also holds jurisdiction over the investigation of complaints related to the flow of information over national borders.[65]

The Office of the Privacy Commissioner has noted concerns around consent to cloud computing practices and a tendency towards "function creep," where data is used for purposes other than the original stated purpose consented to.[66] Additionally, there is often little room to negotiate privacy, with many cloud services integrated with other products and are necessary or largely integral to their use, such as the Apple iCloud. Data collected from cloud computing services can include all information uploaded or backed up, but also the way in which the data is used – location data, name, phone, email, time of usage, identity of multiple users, etc.

Cloud computing raises two broad privacy concerns, which include loss of user control over data and dependence on the cloud computing provider.[67]

When users store their data on someone else's hardware, users lose a degree of control over their sensitive information. For consumers, there is a lack of transparency in how, when, why, and where their data is accessed and processed by hosts. As well, it is not always clear whether other third parties are also able to access and use this data. The OPC notes that the aggregation

---

59 "What is a Cloud Server: Infrastructure for Cloud Computing", online: *IBM* <https://www.ibm.com/cloud/learn/what-is-a-cloud-server> [https://perma.cc/28YZ-U8AT].

60 Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing* (Ottawa: OPC, March 2010), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/cc_201003/> [https://perma.cc/2CZC-QN6D] [OPC, "Cloud Computing"].

61 *Ibid*.

62 John B Horrigan, "Data Memo: Use of Cloud Computing Applications and Services" (September 2008), online: *Pew Internet and American Life Project* <http://www.pewinternet.org/files/old-media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf> [https://perma.cc/4CLD-Y95Z].

63 OPC, "Cloud Computing", *supra* note 60.

64 *Ibid*.

65 *Lawson v Accusearch Inc*, 2007 FC 125 at para 51.

66 OPC, "Cloud Computing", *supra* note 60.

67 Marko Hölbl, "Cloud Computing Security and Privacy Issues" (15 March 2011), online (pdf): *Council of European Professional Informatics Societies* <http://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf> [https://perma.cc/2436-UYDX].

of large amounts of data creates a potential for the misuse of personal data.[68] Where hosts mine the data entrusted to them to generate secondary data, issues of data ownership can also arise.[69]

Relatedly, the concept of storing data with another company worries people because responsibility for security now shifts from the hands of the user to the hosting company. From a privacy standpoint, consumers would want to know how the host protects user data. If hosts do not adequately invest in security, cloud computing increases the risk of a security breach.

5) CCTV

CCTV stands for closed-circuit television – a system of recording cameras that does not broadcast outside of its internal monitoring system. Recordings can either be kept or discarded, depending on the policies of the operating body. CCTV is frequently used by private actors such as retail stores in an attempt to reduce theft and other illegal activity. It is used by public entities such as law enforcement for similar reasons.

The Privacy Commissioner has jurisdiction over federal privacy complaints. Recorded or captured images on CCTV constitute a collection of personal information within the meaning of the *Act*.[70] The Commissioner stated in an open letter that "wholesale monitoring or recording certainly runs afoul of the requirement to collect only the minimum amount of personal information required for the intended purpose."[71]

Complaints have been filed and addressed regarding CCTV surveillance use by the RCMP, Correctional Services Canada, and Port Authority, among other public bodies.[72] Employers that constitute a "federal work, undertaking or business" have also been the subject of complaints to the Privacy commissioner under PIPEDA for their use of CCTV.[73] Entities subject to PIPEDA are required to ascertain "knowledge and consent" to "collection, use and disclosure of an individual's personal information."[74] CCTV can be accepted as a reasonable intrusion to privacy in specific cases for specific needs, particularly where other methods are difficult or impossible.

The Office of the Federal Privacy Commission notes that "[i]n order for the organization's purpose to be considered appropriate under PIPEDA, there must be a demonstrable, evidentiary need for the collection… it would not be enough for the organization to be acting on a mere suspicion."[75] Personal information collected must have a clear, limited, and legitimate business purpose, loss of privacy must be proportional to the benefit gained, and less intrusive measures must be taken before resorting to CCTV.[76] While CCTV use generally occurs without consent, to do so legally under PIPEDA an organization must be able to reasonably ensure that:

---

68 OPC, "Cloud Computing", *supra* note 60.

69 *Ibid*.

70 *Ibid*.

71 *Ibid*.

72 Office of the Privacy Commissioner of Canada, *Investigations into federal institutions* (Ottawa: OPC, 20 June 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/?q[0]=59&Page=1> [https://perma.cc/EE7L-AT6M].

73 Office of the Privacy Commissioner of Canada, *Employers subject to PIPEDA should inform their employees about the existence of, and purpose for, video surveillance in the workplace* (Ottawa: OPC, 9 September 2015), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/ser/2015/s2015-001_0909/> [https://perma.cc/PZN2-HWBC].

74 *Ibid*.

75 Office of the Privacy Commissioner of Canada, *Guidance on Covert Video Surveillance in the Private Sector* (Ottawa: OPC, May 2009), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gd_cvs_20090527/> [https://perma.cc/J23D-NT6Y].

76 *Ibid*.

1. collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information; and

2. the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province[77]

Data collected by CCTV typically includes audio, video, and still images. Additional software can be applied to CCTV footage to track individuals and recall all footage they can be found in.

The primary privacy issue for CCTV under PIPEDA is consent. Most surveillance cameras pointed at publicly accessible spaces are commercially run and operated.[78] For individuals to adequately consent to being recorded, for the most part they may need to know they are being recorded, why, and who is recording them.[79] Professor Andrew Clement from the Faculty of Information at University of Toronto has said that most companies using surveillance cameras fall afoul of PIPEDA in their lack of signage posted.[80]

Appropriate use under PIPEDA is also an issue for CCTV cameras. In Canada, private sector compliance with CCTV guidelines established by the Privacy Commissioner is poor.[81] The private nature of CCTV recordings makes it difficult for individuals to know and therefore bring complaints when their privacy rights have been infringed. The result is that noncompliance can continue unremedied. Recent developments in technology have combined facial recognition and AI with CCTV cameras,[82] which could pose greater issues for what constitutes appropriate use under PIPEDA. Therefore appropriate use, along with individuals consenting to that use, are areas with large potential privacy intrusions for CCTV cameras.

6) Smart Trucks

"Smart truck" is a broad term describing a truck that has qualities beyond a driver's capabilities and the vehicle's "driving only" capacity. This term can describe a vehicle that has a level of automation, such as auto-braking; cargo-monitoring capabilities; a system of transport management over a fleet of trucks; and, importantly, trucks that are designed to have reduced environmental impact. Intelligent transportation systems are predicted to eventually connect "smart emergency vehicles, trucks, trains, traffic signals, and other devices."[83]

Smart trucks and other vehicles produce a great deal of data even now, including information that can be used for geolocation, data mining, and market research.[84] Experts have pointed out that not only are many connected-vehicle drivers unaware of the data they're generating, but

77 *Ibid*.

78 Brenda MacPhail et al, "I'll Be Watching You", *IEEE Technology and Society Magazine* 33:2 (2014) 53 at 55.

79 Colin D'Mello, "How Many Cameras Are Watching You? Toronto Professor Concerned About Privacy", *CTV Toronto* (26 February 2015), online: <https://toronto.ctvnews.ca/how-many-cameras-are-watching-you-toronto-professor-concerned-about-privacy-1.2255985> [https://perma.cc/M8UL-4HDH].

80 Canadian Civil Liberties Association, "An Interview with Professor Andrew Clement", *CCLA* (19 May, 2015), online: <https://ccla.org/an-interview-with-andrew-clement/> [https://perma.cc/55S3-J36T].

81 Macphail, *supra* note 78.

82 Patricia Nilsson, "How UK Police Are Using Facial Recognition Software", *Financial Times* (11 October 2018), online: <https://www.ft.com/content/06c46942-cc7d-11e8-b276-b9069bde0956> [https://perma.cc/Y4YK-J275]; Jennifer Kite-Power, "Making Facial Recognition Smarter with Artificial Intelligence", *Forbes* (30 September 2018), online: <https://www.forbes.com/sites/jenniferhicks/2018/09/30/making-facial-recognition-smarter-with-artificial-intelligence/#797901a5c8f1> [https://perma.cc/JM2W-Z7JP].

83 Office of the Privacy Commissioner of Canada, *Protecting Privacy Rights through Innovative Research* (Ottawa: OPC, May 2016), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/real-results/p_res_2016/> [https://perma.cc/HFS4-QKHK] [OPC, "Innovative Research"].

84 *Ibid*.

that opting out of collection is rarely an option.[85] Collected data can also be very personal – who one is with, how they're driving, etc.[86]

Interprovincial and international trucking services are a federal concern,[87] as are inter-provincial and international trade and commerce generally.[88] All federal works, undertakings or businesses are subject to PIPEDA.[89] PIPEDA applies to "inter-provincial and international transactions involving personal information in the course of commercial activities," and the Office of the Privacy Commissioner specifically indicates inter-provincial trucking as an area of commercial activity subject to PIPEDA.

Data collection for smart vehicles can includes a wide range of data types: not just location of the car itself, but potentially where the user goes; who they are with; how they drive; voice and video recording in the car; and biometric scanning for driver identification, to name a few.[90] Experts such as Philippa Lawson have voiced concerns that content tends to be "all or nothing," with no opt-out option for non-essential uses. Lawson also notes that one of her study's "key findings is "that if you want the service, you are forced to agree to an often open-ended array of unnecessary collection, use, or disclosure of your personal information."[91] Concern is amplified when end use of the data is unstated and not in the individual's best interests, such as the manufacturer selling data to the owner's insurer.

Trucking companies are increasingly installing on-board monitoring systems in their trucks to improve safety and to boost driver productivity. There are numerous types of monitoring systems, including gauges that assist with fuel management and devices that report on engine health. However, the systems that generate the greatest privacy concerns are operator monitoring systems. These systems allow managers to detect whether drivers are following other vehicles too closely, hitting the brakes too hard, or engaging in other unsafe practices.[92] They also identify drivers who are 'slacking' or making unauthorized stops. Some of these systems even include driver-facing cameras.

Smart trucks raise the same workplace privacy concerns for drivers as for employees in other employment contexts. Drivers spend hours at length on the road and engage in many activities that can reveal core biographical data, such as listening to radio stations of preference; speaking to family, friends, and associates on the phone; or stopping at particular rest stops. Pervasive video surveillance may impact negatively on the democratic rights of drivers to freely express their thoughts and to associate freely to share those thoughts if they know records of their conversations and radio show preferences are kept by employers.[93]

---

85 Philippa Lawson, "The Connected Car: Who's in the Driver's Seat?" (20 March 2015), online (pdf): *BC Freedom of Information and Privacy Association* <https://fipa.bc.ca/wordpress/wp-content/uploads/2018/01/CC_report_lite.pdf> [https://perma.cc/K78P-QJBV].

86 OPC, "Innovative Research", *supra* note 83.

87 Transport Canada, *Annual Reports: Transportation in Canada 2011: Road Transportation* (Ottawa: Transport Canada, 28 March 2011), online: <https://www.tc.gc.ca/eng/policy/anre-menu-3021.htm> [https://perma.cc/29LF-Q4Q4].

88 Kalkbrenner, *supra* note 49.

89 *PIPEDA*, *supra* note 16, s 4(1)(b).

90 OPC, "Innovative Research", *supra* note 83.

91 Lawson, *supra* note 85.

92 Robert Bowman, "Is New Truck-Monitoring Technology for Safety -- Or for Spying on Drivers?", *Forbes* (11 February 2014), online: <https://www.forbes.com/sites/robertbowman/2014/02/11/is-new-truck-monitoring-technology-for-safety-or-spying-on-drivers/#2b078efe49f8> [https://perma.cc/2CLU-PWL4].

93 Quasim Mahmood Rajpoot & Christian D Jensen, "Video Surveillance: Privacy Issues and Legal Compliance" (2015), online (pdf): *Technical University of Denmark* <http://orbit.dtu.dk/files/110934780/Video_Surveillance_Privacy_issues_and_legal_compliance.pdf> [https://perma.cc/NR2W-6N6R].

7) Transit

It is difficult to determine what constitutes commercial activity in the context of quasi-governmental entities. Metrolinx is a provincial Crown Corporation that manages and provides public transit in Ontario. In Metrolinx's terms of service, it notes that it is governed by the Ontario FIPPA and MFIPPA legislation, and any other relevant legislation. When contacted, Metrolinx has stated that they are not covered by PIPEDA. In a report to the Transit Commission of Ontario, it was stated that "Transit Services is also subject to the Federal Personal Information *Protection and Electronic Documents Act ("PIPEDA")* with respect to employee information."[94] However, this is the inverse of what one might expect – if PIPEDA does apply, it would apply to all information except that relating to employees. This demonstrates some of potential hurdles for Smart City technologies – there are likely to be many entities that are based around local works, but are engaged in commercial activity. Public transit, energy infrastructure, and parking apps are all potential examples.

Adequate safeguards are a privacy concern with transit smart cards. Near-Field Communication (NFC) technology, either on a smart card or a phone app that acts as a smart card, is vulnerable to privacy intrusions. Purchases, train stops, and top-ups are recorded by NFC devices and commuter passes. Because NFC technology often provides unencrypted data to readers within range, this sensitive information, and potentially even credit card information, is possibly at risk.[95] Some studies even demonstrate the ease in calculating an individual's home address through the data exposed by their smart transit cards.[96] Adequate safeguards are needed to ensure individuals' information remains private from nefarious actors, stalkers, and others.

Consent to information collection and disclosure is also a concern for smart transit cards. Some smart card systems, such as PRESTO, tie identity to routes being tracked.[97] As noted by Professors Teresa Scassa, Jennifer Chandler, and Elizabeth Judge, if tied to an individual, smart card records of their movements or activities constitutes personal information.[98] This information can be disclosed to police without a warrant, as has occurred in Winnipeg,[99] Ottawa, and Toronto.[100] Privacy expert Chris Parsons suggests clear consent should be obtained from users by outlining specific circumstances in which this personal information will be disclosed to police. Overall, consent is an issue for transit pass users when they do not clearly understand how their information may be used and disclosed.

8) Ride Sharing

Ride sharing can mean a variety of things. Some ride-sharing is simply between those who know each other, commonly known as carpooling; some can be essentially renting time on an

94 Alain Mercier, "Transferability of Smart Card Bus Passes" (14 September 2011), online: *Ottawa* <https://ottawa.ca/calendar/ottawa/citycouncil/tc/2011/09-21/06%20-%20ACS2011-ICS-TRA-0020%20-%20Transferability%20of%20Smart%20Card%20Bus%20Passes.htm> [https://perma.cc/T3BQ-3FRE].

95 Allan Richarz, "Near-Field Communication Technology: Regulatory and Legal Recommendations for Embracing the NFC Revolution" (2014) 12:1 CJLT 27 at 34 (WL).

96 Jorge Bahamonde et al, "Mining Private Information from Public Data: The Transantiago Case" (2014) 13:2 IEEE Pervasive Computing 37 at 37.

97 Jenny Yuen, "Presto Tracking a Privacy Issue?", *Toronto Sun* (15 February 2017), online: <https://torontosun.com/2017/02/15/presto-tracking-too-close-for-comfort/wcm/4227a5d0-8581-464c-ad62-31c94a078397> [https://perma.cc/WU3Q-FBJV].

98 Teresa Scassa, Jennifer A Chandler, & Elizabeth F Judge, "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and Deployment of Intelligent Transportation Systems" (2011) 74 Sask L Rev 117 at 122.

99 Jeff Keele, "Without Warrants, Winnipeg Police Taking Info from Transit Payment Cards", *CTV News* (7 June 2017), online: <https://www.ctvnews.ca/canada/without-warrants-winnipeg-police-taking-info-from-transit-payment-cards-1.3448736> [https://perma.cc/NU9T-S37V].

100 Ben Spurr, "Metrolinx Has Been Quietly Sharing Presto Users' Information With Police", *Toronto Star* (3 June 2017), online: <https://www.thestar.com/news/gta/2017/06/03/metrolinx-has-been-quietly-sharing-presto-information-with-police.html> [https://perma.cc/937T-H3U9].

individual car through a membership; some can be splitting a hired driver with strangers. There is no fixed definition to ride sharing, but benefits tend to overlap -- less cars on the road, lower energy consumption, and reduced pollution.[101]

Renting time on a vehicle has become a popular form of ride-sharing. Companies such as Car2Go and Zipcar have minimum-amount memberships, but allow members to rent vehicles by either the minute or hour. Some cities have provided designated parking spots in popular areas, while in some cities there will simply be a "home area" in which it is acceptable to leave the car. Rentals include insurance, parking, and gas fees, and membership will typically include an app to help find the vehicles, report issues, and navigate.

Ride sharing with a paid driver is best known to users through companies such as Uber and Lyft. Falling somewhere between taxis and carpooling, apps allow users to choose between the type of vehicle that will pick them up, and whether they are willing to ride with other users in order to lower the price of their ride. Such companies popularized the idea of allowing users to choose their location and drop-off points in an app, rate their drivers, and pay through the app.

In response to ride sharing applications, traditional taxi companies such as Diamond and Beck Taxi have expanded their access methods to app users. Hailo, for example, promotes itself as "Canada's first licensed app-based taxi company."[102] Other apps such as OneTaxi and TheRide connect users to a local taxi company, enabling them to contact the first available taxi in their area no matter where they are.

Carpooling is typically an informal arrangement between non-commercial entities, and would not generally engage privacy legislation. Carpooling apps, even for private vehicles, typically include a commercial element and are thus likely to engage PIPEDA similar to other types of ride sharing.

App-based ride sharing in general requires a user's starting location, and the ability to pay through the app. App-based ride sharing with a driver typically works by amalgamating data from users phones. This is necessary in order to coordinate between drivers and riders, as well as determining fit for add-on riders in the case of multi-user rides. Renting time on a vehicle requires information from users as to how long the car is used, its location, and the state of the vehicle. Traditional taxi companies using apps also require a user's location.

Beyond provincial and municipal approval as to whether or not ride-share companies are allowed in their jurisdiction, PIPEDA applies to the privacy issues that such commercial activities raise. While provinces with substantially similar legislation will intercede, the requirements are the same. Ride sharing apps are commercial activity that collects personal information. This includes not only the app's obvious uses, such as their current location, but also amalgamation of information such as the user's typical pickup location and their use habits.

Ride-sharing apps raise several privacy concerns, depending on the type of data collected. Since ride-share apps need to know the locations of both drivers and passengers requesting the ride service, the apps collect the GPS coordinates of driver and riders alike. If riders do not turn off location access after they are dropped off at their destination and driver do not turn theirs off after finishing their rounds, the app could potentially track and collect data on where the individual is, where they go, and how long they stay there. Apps have little need to keep rider information once a ride is complete. However, in its privacy policy update in 2015, Uber refused to surrender its right to delete trip information after ride transactions are complete. Uber

101 Adam Connor-Simons, "How Ride-Sharing Can Improve Traffic, Save Money, and Help the Environment", *MIT News* (4 January 2017), online: <http://news.mit.edu/2016/how-ride-sharing-can-improve-traffic-save-money-and-help-environment-0104> [https://perma.cc/S8HL-V794].

102 "Smartphone Taxi Apps Offer an Instant Pick-Me-Up", *The Canadian Press* (26 September 2012), online: <https://www.cbc.ca/news/canada/toronto/smartphone-taxi-apps-offer-an-instant-pick-me-up-1.1152790> [https://perma.cc/5K2Q-P9TV].

failed to put forward a legitimate reason for reserving this right, stating vaguely that riders may benefit from being able to view their ride history. However, the company neglected to elaborate on what these benefits may be.[103]

If the app requires users to authenticate themselves by signing into a social network account, the ride share company may also gain access to personal information in the individual's social media account. Since most app-based ride-share programs are cashless, they also collect and store user's credit card details.[104]

9) Automated Vehicles

There are a range of vehicular features that fall under the heading of 'automated.' These are typically divided into a range: zero being no automation, where the driver performs all necessary 'driving' functions, and five being a completely autonomous vehicle where the machine 'drives' itself, and does not need a steering wheel or brakes. The levels in between add increasingly autonomous features. These include features such as various sensing capabilities that warn the driver of nearby entities.

Ottawa is considering making the leap to being the first Canadian city with a completely autonomous shuttle, to be used at the airport.[105] Other countries have already implemented them - France has a nuclear power station with autonomous shuttles, and has had them for several years.[106] While it has been noted that such shuttles currently work best in a controlled environment, the increasing use of autonomous vehicles in general seems likely.

While the particularities of driving law beyond the criminal realm are under provincial jurisdiction, the privacy aspects of autonomous cars will have a federal element. Commercial applications of autonomous vehicles, such as commercial shuttles or autonomous taxis, will fall under PIPEDA as a federal legislation. User data will likely include profiles, drop off and pick-up points, and payment information. Additionally, cars need not be fully autonomous to fall under PIPEDA: as long as there is a commercial element, such as hiring a vehicle, data collected on the user, particularly on their driving, may constitute personal data and thus fall under PIPEDA.

A major privacy concern for autonomous vehicles is consent. The federal Privacy Commissioner noted that individuals should be aware that information shared with an automated vehicle may be used for many purposes, such as personal information marketing, navigation, vehicle improvement, and more.[107] However, these numerous and complex uses may be overwhelming, and requires automated vehicles provide notes to individuals seeking their consent prior to collection, use, and disclosure of personal information.[108] Philippia Lawson, Barrister and Solicitor for the British Columbia Freedom of Information and Privacy Association, in her submission to the Senate Standing Committee on Transport and Communications, has even suggested that informed consent is an unworkable model given the multiplicity of players

---

103 Justin Bregman, "Uber and Privacy: Should You Be Concerned?" (15 July 2015), online: *The zebra* <https://www.thezebra.com/insurance-news/1747/uber-and-privacy-should-you-be-concerned/> [https://perma.cc/S3GT-ZCUR].

104 Norton, "How Ridesharing Services Can Take Your Privacy for a Ride", online: *Norton* <https://us.norton.com/internetsecurity-privacy-ridesharing-privacy-ride.html> [https://perma.cc/8W9K-2ZKX].

105 Elizabeth Payne, "Ottawa airport looking at driverless shuttle service", *Ottawa Citizen* (14 May 2018), online: <https://ottawacitizen.com/news/local-news/ottawa-airport-looking-at-driverless-shuttle-service> [https://perma.cc/AYX9-ME3U].

106 *Ibid*.

107 Office of the Privacy Commissioner of Canada, *Submission to the Standing Committee on Transport and Communications Regarding Their Study on the Regulatory and Technical Issues Related to the Deployment of Connected and Automated Vehicles* (OPC: Ottawa, 22 November 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_sub_171122/> [https://perma.cc/859Z-KSCS] [OPC, "Automated Vehicles"].

108 Teresa Scassa, Jennifer A Chandler & Elizabeth F Judge, "Privacy by the Wayside: The New Information Superhighway, Data Privacy, and Deployment of Intelligent Transportation Systems" (2011) 74 Sask L Rev 117 at 121.

in the autonomous vehicle ecosystems.[109]

Another major concern for autonomous vehicles is information disclosure and accountability. Data can be sold to third parties who can create user profiles, predict where they will go, and use travel information to market specific products to users.[110] Issues over who controls the data or owns the data, particularly in the context of shared autonomous vehicles or taxis, arise in this context.[111] Given the complexity, the Privacy Commissioner suggests the PIPEDA principle of accountability should take a larger role.[112] Regardless of how data flows are addressed, third parties, both for commercial and law enforcement purposes, will try to seek disclosure of valuable autonomous vehicle data. Ensuring clear corporate and governmental accountability for data ownership or disclosure is essential.

Adequate safeguards are also an issue for autonomous vehicles, both networked and unnetworked. Unnetworked autonomous vehicles contain huge repositories of information on the user, such as where they traveled, stopped, and how the vehicle traveled. Networked vehicles in constant real-time communication with other vehicles and infrastructure have many more potential breach points.[113] In both instances, these vehicles are susceptible to hackers, burglary, and large information breaches. Even anonymized data has the potential to reveal home addresses, income, and movement retracing.[114]

10) Education and Health

While education and health are naturally important in all aspects, and may benefit from data produced by smart city technologies, they fall squarely under provincial jurisdiction in the division of powers. The federal Office of the Privacy Commissioner has stated:

> While municipalities, educational institutions and hospitals may occasionally provide services on a fee basis, they are not, on the whole, engaged in trade and commerce as contemplated by the Canadian Constitution. Furthermore, these institutions are completely or largely dependent on municipally or provincially levied taxes and provincial grants.
>
> As a result, our Office is of the view that, as a general rule, PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals. By core activities we mean those activities that are central to the mandate and responsibilities of these institutions.[115]

Provincial privacy legislation, however, may apply..

---

109 Senate, *Driving Change: Technology and the Future of Automated Vehicles* (January 2018) (Chair: David Tkachuk) at 55.

110 Araz Taeihagh & Hazel Si Min Lim, "Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks" (2018) Transport Reviews 1.

111 Rob Gillies, "Privacy Concerns Mar Sidewalk Labs Plan to Redevelop Toronto Neighbourhood", *CTV News* (2 October 2018), online: <https://www.ctvnews.ca/business/privacy-concerns-mar-sidewalk-labs-plan-to-redevelop-toronto-neighbourhood-1.4117894> [https://perma.cc/RQH7-D69F].

112 OPC, "Automated Vehicles", *supra* note 107.

113 Dorothy J Glancy, "Privacy in Autonomous Vehicles" (2012) 52 Santa Clara L Rev 1171 at 1180.

114 Alex Hern, "New York Taxi Details Can Be Extracted From Anonymised Data, Researchers Say", *The Guardian* (27 June 2014), online: <https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn> [https://perma.cc/Y5VB-4VEJ].

115 Office of the Privacy Commissioner of Canada, *The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals* (OPC: Ottawa, December 2015), online: *Office of the Privacy Commissioner of Canada* <https://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_25/> [https://perma.cc/BZ35-BTQD] [OPC, "Municipalities"].

11) Emergency Services

Incident response apps can cover a variety of uses and situations, from university campus alerts to city-wide reporting capabilities. However, they tend to be both municipal and non-commercial, so are unlikely to fall under federal jurisdiction.

Policing apps can have a range of implementation styles. Some can be used to contact police without using the voice function of a phone, while some are more imaginative - a police app in the Netherlands has been likened to Pokémon Go, as users can earn points by searching for lost cars or missing persons.[116]

Policing is primarily under provincial jurisdiction. While telecommunications are federal, an app for an individual police service is unlikely to be a federal work, undertaking, or business, and is unlikely to be commercial activity. While there should be a level of security over information collected by such apps, it is likely to be dealt with outside of federal jurisdiction.

12) City Services

Many cities are providing access to city services through phone apps or online portals. These can include everything from parking, reporting potholes, and using city transit, to allow users to see historical photographs taken at their location.[117] As most apps and webpages are likely to be less commercial and more strictly municipal, they are more likely to engage local privacy laws rather than federal ones. Even if the service does charge a fee, PIPEDA will not be triggered if the service is part of the institution's 'core activities.'[118] Instead, only provincial or municipal privacy laws will be engaged.

13) Environmental Technologies

Air quality

While systems that combine location, time and activity to regional air quality data to esteem individual carbon footprint[119] can reveal personal information, air quality monitoring alone "reveal[s] nothing about individual people and hence will probably fall outside of the realm of privacy worries."[120]

Trash

Trash bins containing radio-frequency identification (RFID) chips and/or sensors can track the type of trash in a container, its fill level, how often it is moved, and even events such as fires or vandalism.[121] This information is communicated to a trash-collecting agency, who can use it to plan more efficient collecting routes and prevent trash overflow. Ideally, the amount of trash collections is reduced, saving money and reducing emissions. In Canada, Saint John and

---

116 Smith, "Policing in the future involves citizen detectives and a Pokémon Go-like app" (10 October 2017), online: *CSO* <https://www.csoonline.com/article/3232367/security/policing-in-the-future-involves-citizen-detectives-and-a-pokemon-go-like-app.html> [https://perma.cc/4QEN-93C2].

117 CBC News, "City app lets users travel through time", *CBC* (12 August 2018), online: <https://www.cbc.ca/news/canada/ottawa/ottawa-history-travel-time-1.4780132> [https://perma.cc/8DXX-B9LU].

118 OPC, "Municipalities", *supra* note 115.

119 Shilton et al, "Designing the Personal Data Stream: Enabling Participatory Privacy in Mobile Personal Sensing" (2009), online (pdf): *UCLA* <https://escholarship.org/uc/item/4sn741ns> [https://perma.cc/B5QN-UWXV].

120 Liesbet van Zoonen, "Privacy concerns in smart cities" (2016) 33 Government Information Quarterly 472 (ScienceDirect).

121 Enevo, "Technology", online: *Enevo* <https://www.enevo.com/waste-analytics-technology> [https://perma.cc/B9RJ-MD96]; Dru Bloomfield, "Smart Trash Cans-RFID based trash cans" (1 June 2012), online: greener ideal <https://greenerideal.com/news/technology/0601-smart-trash-cans/> [https://perma.cc/FF9F-NS2N].

Winnipeg have implemented smart trash bins and compactors in public places.[122]

Other jurisdictions use smart trash bins to enforce laws and promote recycling. Cleveland uses smart trash bins to detect people who may not be recycling and target them for investigation.[123] South Korea plans to monitor when edible food is thrown into smart trash bins for the purpose of issuing fines.[124] Pay-as-you-throw schemes have been implemented in many North American and European cities with smart trash bins to charge individuals for waste collection based on the amount of trash they generate.[125]

If, for example, the smart trash system is a municipal project in Ontario, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) will apply.[126] If it is run by a private business, PIPEDA will apply unless the information is collected and used within Alberta, British Columbia, or Quebec (where provincial legislation applies).

Smart trash bins may collect personal information not needed for implementing more efficient trash collection. In a European privacy impact assessment of smart trash systems, experts ranked "uncontrollable data gathering" as the most relevant privacy risk.[127] If products contain RFID tags, smart trash bins could collect information regarding the products a person uses and, by extension, information about that person's activities and preferences. Smart trash bins used in a residential setting will likely provide location data, identifying the owner by linking the bin to their address.[128]

Smart trash bins may even collect information unrelated to trash. Enevo, a smart trash company, claims that their sensors can detect when containers are vandalized.[129] Additionally, RFID chips in fixed, public locations may be able to track people passing by who are carrying products with RFID tags.[130] In London, internet-connected smart trash bins were removed following public outcry over how the bins were picking up signals of Wi-Fi devices, identifying and tracking passersby.[131]

This sort of unpredictable and broad information collection may not comply with privacy legislation, such as MFIPPA's requirement that only personal information necessary to administer a municipal organization's authorized activities be collected, or the limiting collection principle of PIPEDA. It also presents challenges related to obtaining consent. The Information and Privacy Commissioner of Ontario recommends that consumers be notified when, where, and why an RFID tag is being read, including an audio or visual indicator built into the RFID

---

122 Bryce Hoye, "City approves $135K solar-powered recycling bins, trash compactors", *CBC* (16 April 2018), online: <https://www.cbc.ca/news/canada/manitoba/winnipeg-solar-garbage-compactors-1.4622383> [https://perma.cc/J8ZZ-T9VV]; CBC News, "Uptown Saint John piloting 'smart' solar trash compactors", CBC (17 June 2014), online: <https://www.cbc.ca/news/canada/new-brunswick/uptown-saint-john-piloting-smart-solar-trash-compactors-1.2678492> [https://perma.cc/6AMX-UZCR].

123 Mark Gillispie, "High-tech carts will tell on Cleveland residents who don't recycle … and they face $100 fine" (20 August 2010), online: <http://blog.cleveland.com/metro/2010/08/city_of_cleveland_to_use_high-.html> [https://perma.cc/5Z55-KPGA].

124 Bloomfield, *supra* note 121.

125 RAND Europe, "SMART TRASH: Study on RFID tags and the recycling industry" (February 2012), online(pdf): <https://www.rand.org/content/dam/rand/pubs/working_papers/2012/RAND_WR922.pdf> [https://perma.cc/55WR-NTSV].

126 *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56 [*MFIPPA*].

127 RAND Europe, *supra* note 125 at 171.

128 Enevo, *supra* note 121.

129 *Ibid*.

130 Dong-Her Shih, Binshan Lin & Chin-Yi Lin, "RFID tags: Privacy and security aspects" (2005) 3 International J of Mobile Communications 332 at 336 (Research Gate).

131 Information and Privacy Commissioner of Ontario, *Smart Cities and Your Privacy Rights*, (Toronto: IPC, April 2018) at 3, online (pdf): *Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/2018/04/fs-tech-smart-cities.pdf> [https://perma.cc/B6FS-DQR4] [IPC, "Smart Cities"]; RT, "Watched from a waste bin: UK pulls plug on 'spy' trash cans" (12 August 2013), online: *RT* <https://www.rt.com/news/trash-bin-surveillance-wifi-402/> [https://perma.cc/YF5T-9N6A].

system.[132] Most smart trash bins, however, only use RFID chips and other sensors to track the bin's weight and location.[133]

Smart trash systems also raise security concerns. Given the large number of data collection points in smart trash systems, they are especially vulnerable to security breaches.[134] MFIPPA requires Ontario municipalities to have reasonable measures in place to protect personal information from unauthorized access.[135] PIPEDA stresses the implementation of safeguards relative to the sensitivity of the personal information held, which may be minimal or great depending on what information the bin is capable of collecting.[136]

With respect to s. 8 of the *Charter*, protection against unreasonable search and seizure, trash put out on the curb for collection is considered abandoned and can be taken by police without a warrant.[137] Trash in a smart trash bin, however, may be searched while it is still in the house and while there is still an active privacy interest in the trash.

14) Traffic and Parking

There are a wide variety of traffic and parking applications. Traffic applications are typically used to either reduce traffic congestion or inform about the state of traffic, whereas parking generally alerts drivers to open spaces.

Traffic

Smart city traffic technologies can include video feeds of roads, highways, and intersections; cameras mounted on city vehicles to scan license plates and identify parking violations; noise sensors to measure traffic noise; apps to identify user travel habits; construction cones embedded in sensors; and sensors collecting information to optimize traffic flow.

As traffic technologies are generally employed or contracted directly by the city, and thus are public works rather than commercial activity, PIPEDA is not engaged. Instead, provincial, territorial, or municipal privacy laws apply.

Privacy concerns vary greatly with the kind of technology employed. The more limited the scope of the sensor, the less privacy concerns are engaged. For example, an inductive loop bicycle traffic sensor senses only that a metal sufficient to complete the loop has passed by. This will only engage personal information in very limited circumstances, such as in minimally populated areas, or those with very few cyclists. Conversely, an application that uses video will raise many more concerns, as information about individuals can easily be ascertained: license plates, faces, driving styles, and destinations.

Even if information such as license plates and faces are blurred, there is a risk that individuals or vehicles may still be identified. Multiples video spots allow the surveillance of an individual over a large distance, and give information on their schedule and habits, including "private life, habits, acts, and relations."[138] Even if such recordings are not made available to the public,

---

132 Information and Privacy Commissioner of Ontario, *Privacy Guidelines for RFID Information Systems* (Toronto: IPC, June 2006) at 8, online (pdf): *Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/wp-content/uploads/resources/rfid-guides&tips.pdf> [https://perma.cc/4NYJ-3K4V].

133 Bloomfield, *supra* note 121.

134 IPC, "Smart cities", *supra* note 131 at 4.

135 *Ibid*.

136 *PIPEDA*, *supra* note 16.

137 *R v Patrick*, 2009 SCC 17.

138 Delphine Christin et al, "A survey on privacy in mobile participatory sensing applications" (2011) 84 Journal of Systems and Software 1928 at 1931.

data that is insufficiently safeguarded can be accessed. Furthermore, data that is not by itself attributable to an individual can become so when combined with other information.

While traffic applications can be used in such a way as to reveal minimal personal information, such as inductive loops and limited sensors, combining traffic sensing with other technologies such as smartphones, can allow the apps to collect and reveal more personal data. This can include not only individual identity, but location and habits. There are also methods to obscure personal information even with broad collection, such as pseudonymity; data perturbation where the sensor "intentionally perturbs the sensor samples by adding artificial noise to the data; masking sensitive locations; aggregating data; data processing by privacy-aware methods; and data auditing.[139]

Parking

Parking applications are employed by private companies as well as municipal organizations. Where there is a private company, which is either paid to help find spots or paid to park in those spots, commercial activity is present. PIPEDA or substantially similar legislation is therefore engaged.

Smart city parking technologies can include automated parking, realtime parking space maps, and electric charging stations. As with traffic technologies, these vary considerably in what information they collect - the narrower the range of information collected, the less the concern. Identifying empty parking spaces can be achieved as simply as a light sensor, or as broadly as a video feed. The concerns are thus very similar to traffic technologies, and vary according to what information is collected. Automated parking technologies could, for example, not identify the car directly, and simply provide the driver with a ticket with which to claim the car later. If the car is identified by license plate, however, or the driver on camera, then much more personal information is being collected and is potentially at risk.

15) Internet Services

Connectivity is an essential aspect of any modern city and developing Wi-Fi networks is an efficient and cost-effective way of supplying connectivity to smart cities.[140] Wi-Fi networks can be provided by municipalities or by private businesses, and most smart cities offer a combination of both. Municipal Wi-Fi networks support many public services, such as water management, parking meters, security video management and smart lighting.[141] Such systems often operate on municipally-owned networks, which means there is no cost passed onto users, while other municipalities choose to pay for public networks to host Wi-Fi services.[142]

Many private companies also provide free public Wi-Fi services to entice customers to use their services and buy their products. For example, Bell Mobility provides Wi-Fi in many Tim Horton's, McDonald's and Chapters Indigo locations.[143] Such businesses often use splash screens, which users see when logging into their Wi-Fi networks, to help offset costs through advertising.[144]

Strategic placement of Wi-Fi networks in downtown and high-traffic areas can also help

---

139 *Ibid*.

140 Alex Puregger, "Are WiFi networks ready for Smart Cities?" (30 July 2018), online (blog): *TechRadar.pro* <www.techradar.com/news/are-wifi-networks-ready-for-smart-cities> [https://perma.cc/U2WG-FJ7T].

141 Maureen O'Higgins, "Municipal Public Wi-Fi: A Sound Investment?" (2016), online (pdf): *Eastern Ontario Regional Network* <www.eorn.ca/en/resources/Municipal-Wi-Fi/EORN_WP_WiFi_FINAL.pdf> [https://perma.cc/P3PF-KSS6].

142 *Ibid* at 6.

143 *Ibid* at 14.

144 *Ibid* at 17.

overcome inequality and access to information problems that burden those who do not have reliable internet access. This would allow disadvantaged residents to search for employment, use online banking, access correspondence and use countless other online services. As well, a wireless network can be used for communicating major updates, mass alerts, and disaster responses in a timely and efficient manner.[145]

Smart cities that successfully adapt wireless networks become attractive to businesses, investors and tourists.[146] Businesses are more willing to choose a location with a strong wireless network in order to improve efficiency and sales, while investors recognize the value of connectivity in urban areas.[147] Similarly, smart cities that offer good Wi-Fi networks allow tourists to take advantage of connectivity, enjoy increased tourist revenue and become competitive tourists destinations.[148]

There are several privacy concerns for users of such networks, especially pertaining to data collection and sharing. Different legislation restricts data collection depending on whether the collector is a public or private body. Information gathered by private companies through Wi-Fi networks is subject to PIPEDA, which applies in all provinces and territories except for Alberta, British Columbia and Quebec.[149] These three provinces have independent private-sector laws that resemble PIPEDA. Wi-Fi networks provided by municipalities, universities, schools and hospitals are subject to provincial laws and must adhere to PIPEDA only if these organizations are engaged in commercial activities outside of their core purposes.[150]

Information gathered through Wi-Fi provided by the public sector is subject to provincial laws, which differ for each province and territory. For example, in Alberta the Freedom of Information and Protection of Privacy Act governs public sector privacy while the Personal Information Protection Act, deemed substantially similar to PIPEDA, governs private-sector privacy.[151]

Additional privacy concerns arise from the Internet of Things (IoT) technology, which is the networking of physical objects that connect through the internet.[152] Mobile phones and tablets are built to facilitate communications with other devices using networks, and the rise of public Wi-Fi means that user information is now easier than ever to collect.[153] Businesses have adopted models that help them collect such information efficiently, and providing public Wi-Fi networks to users allows businesses to effectively market products and target consumer groups with ease.[154] Internationally, many government bodies, including the European Commission's Article 29 Data Protection Working Party, suggest that IoT technology raises serious privacy concerns because personal devices become powerful data trackers when connected to networks.[155]

Apart from collection and sharing of information gathered through Wi-Fi networks, another concern is that these networks are prime targets for hackers. Public Wi-Fi networks may not

---

145 Wipro Insights, "Public Wi-Fi: Enabling Smart Cities and Connected Communities" (6 November 2014), online (blog): *Wipro* <www.wipro.com/en-CA/blogs/wipro-insights/public-wi-fi--enabling-smart-cities-and-connected-communities/> [https://perma.cc/QE5F-Y2YX].

146 Rebecca Moy, "Smart Cities and WiFi: A step in the right direction for our #travelgoals and woes?" (14 November 2018), online (blog): *fontech* <fontech.com/blog-smart-cities-and-wifi-tourism/> [https://perma.cc/8KJL-DFM3].

147 O'Higgins, *supra* note 141 at 15-16.

148 *Ibid* at 17.

149 OPC, "Summary", *supra* note 9.

150 *Ibid*.

151 *Ibid*.

152 OPC, "Internet of Things", *supra* note 48 at 1.

153 *Ibid*.

154 *Ibid* at 2.

155 *Ibid*.

be as strongly protected as other networks, such that users do not have the safety of a firewall or other protection offered by personal networks. As public Wi-Fi networks become more common, the Privacy Commissioner of Canada suggests taking steps to secure privacy, such as carefully reading privacy agreements on splash screens.[156]

16) Airport Technologies

Although a wide range of smart city initiatives can be considered airport technologies, this section reviews the privacy implications of self-service security kiosks and mobile airport apps as examples thereof. Airport technologies are under federal jurisdiction, and so attract federal legislation: the *Privacy Act* and PIPEDA.

BorderXpress, developed by Innovative Travel Solutions (ITS) of the Vancouver Airport Authority, provides self-service border control kiosks that accept all passports and do not require pre-registration or fees.[157] The Canada Border Service Agency (CBSA) has made these self-service kiosks, deemed primary inspection kiosks, available to most incoming travelers at Canadian airports. Using the kiosks, passengers scan their travel documents, complete their declaration and verify their identity with facial recognition.[158] Travellers then proceed to a border control officer for final approval.[159] This eliminates the need for a paper form and ITS claims that their kiosks reduce wait times by more than 50 percent.[160]

Self-service kiosks collect all kinds of sensitive personal information: passport; residency cards; driver's licenses; travel information from QR codes, 2D barcodes and mobile devices; credit and debit card information; facial, fingerprint and iris biometric data; and answers to various questions, including information related to the duration and purpose of a trip.[161] A companion app allows travelers to fill out information on their mobile device and prepopulate the kiosk forms by scanning a QR code. This app is not connected to CBSA systems and retains only "basic, non-protected, traveler information."[162]

The *Privacy Act* applies to the collection, use and disclosure of personal information by agencies of the federal government, such as CBSA.[163] Under the *Privacy Act*, only personal information which relates to an agency's programs or activities may be collected. Without consent, and subject to some exceptions, personal information can only be used or disclosed for a use consistent with the purpose for which it was collected.[164]

In a privacy impact assessment of these new kiosks, CBSA stated that the information they

---

156 Office of the Privacy Commissioner of Canada, *Privacy and the Internet of Things* (Ottawa: OPC, 12 December 2017), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/02_05_d_72_iot/> [https://perma.cc/Q2TD-4R5E].

157 YVR, "Innovative Travel Solutions celebrates 2017 as leading global provider of border kiosks" (21 December 2017), online: *YVR* <http://www.yvr.ca/en/media/news-releases/2017/innovative-travel-solutions-celebrates-2017-as-leading-global-provider-of-border-kiosks> [https://perma.cc/YS8Z-DLPZ] [YVR, "Innovative Travel"]

158 YVR, "BORDERXPRESS™ Primary Inspection Kiosks", online: *YVR* <http://www.yvr.ca/en/business/self-service-border-products/primary-inspection-kiosks> [https://perma.cc/89DW-QSVE].

159 YVR, "BORDERXPRESS Vancouver Airport Authority English Brochure" (March 2018) at 10, online (pdf): *YVR* <http://www.yvr.ca/-/media/yvr/documents/border-products-documents/borderxpress--vancouver-airport-authority--english--brochure--march-2018-web.pdf?la=en> [https://perma.cc/D9YX-BSKV] [YVR, "Brochure"]; Canada Border Services Agency, *Primary Inspection Kiosk Privacy Impact Assessment* (Ottawa: CBSA, 14 March 2017, online: *CBSA* <https://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pik-bip-eng.html> [https://perma.cc/2XKQ-6BV4].

160 YVR, "Innovative Travel", *supra* note 157.

161 YVR, "Brochure", *supra* note 159; CBSA, *supra* note 159.

162 CBSA, *supra* note 159.

163 *Privacy Act*, RSC 1985, c P-21.

164 *Ibid*, s. 7.

collect remains mostly unchanged except for the facial recognition feature.[165] That facial recognition capability has caused concern among privacy experts, however, because the biometric data which it collects is particularly susceptible to being used for other purposes.[166] For example, the Insurance Corporation of BC offered Vancouver Police access to its database of driver's license photos to identify people who participated in a riot.[167] CBSA also mentions that information collected at primary inspection kiosks will be disclosed to Statistics Canada for the purpose of statistical analysis.[168]

CBSA's privacy impact assessment claims that primary inspection kiosks improve data transmission security.[169] Smart initiatives, however, may be especially vulnerable to hacking because there is usually a large amount of data collection points.[170]

YULi is a mobile app for the Montréal-Trudeau Airport. Users can get personalized routes around the airport, receive real-time updates about their flight information, and make online parking spot reservations. The app also advertises the airport's retailers and partners with "offers tailored specifically for you."[171]

Since the app is published by Aéroports de Montréal, the Quebec *Act respecting the protection of personal information in the private sector* (ARPPIPS) would apply.[172] Given that this is an airport app, information may at times be collected from another province or country, in which case PIPEDA would apply.[173]

A privacy issue typically associated with mobile apps is obtaining meaningful consent despite the device's small screen. The Office of the Privacy Commissioner of Canada recommends that app developers implement a privacy dashboard where users can easily change their privacy settings, layer privacy information by listing important points first, and use symbols to convey privacy-related information to users.[174]

17) Economic Development

Economic development is a broad category, encompassing many of the smart city technologies previously discussed. This section covers the privacy implications of a contained smart city project and smart technologies that monitor buildings and public spaces as demonstrative examples, but should not be considered to represent the full range of economic development smart city applications possible.

Sidewalk Toronto is a project headed by Sidewalk Labs, a Google-affiliated company, and Waterfront Toronto, a municipal organization, to build a contained smart city in Toronto's

165 CBSA, *supra* note 159.

166 Matthew Braga, "Facial recognition technology is coming to Canadian airports this spring", *CBC* (2 March 2017), online: <https://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344> [https://perma.cc/NDP4-TBNW].

167 *Ibid*.

168 CBSA, *supra* note 159.

169 *Ibid*.

170 IPC, "Smart Cities", *supra* note 131.

171 Aéroports de Montréal, "YULi Mobile app", online: *Aéroports de Montréal* <https://www.admtl.com/en/mobile-apps> [https://perma.cc/8J74-S9WP].

172 *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 [*ARPPIPS*].

173 *PIPEDA*, *supra* note 16.

174 Office of the Privacy Commissioner of Canada, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps* (Ottawa: OPC, October 2012), online: *OPC* <https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/> [https://perma.cc/3BDU-WC6Z].

Quayside district.[175] The project seeks to employ numerous smart and futuristic technologies, including data-collecting sensors, an advanced microgrid to power electric cars, sensor-enabled waste separation, and driverless vehicles.[176] Still in its early stages, Sidewalk Toronto aims to address some of the challenges facing the city, such as energy use, housing affordability, and transportation.[177] These plans have been met with opposition from privacy activists, who see the project as an attempt by tech companies, operating under the guise of environmentalism and quality of life improvement, to commodify urban data.[178]

Representatives of the Office of the Privacy Commissioner of Canada met with those behind the project and emphasized PIPEDA principles such as specifying the purpose for which data is collected and ensuring individuals can access their own personal information.[179] They also communicated to Sidewalk Toronto the importance of high standards for de-identifying data, such that individuals cannot later be re-identified.[180]

Soofa benches are solar-powered public benches that gather data from the surrounding environment.[181] They use sensors to passively listen for Wi-Fi-enabled devices, allowing cities to monitor how public spaces are being used. Newmarket, for example, says that Soofa benches allow the city to understand how many people are visiting certain areas, how long they are staying, how often they return and how people are moving around in the downtown area.[182] This will help the city make decisions related to waste collection, capital investments, maintenance, parking, and event logistics.[183]

If the smart benches are operated by a municipality in Ontario, the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) will apply.[184] If the data is handled by Soofa or another private company, PIPEDA will apply unless the information is collected and used within Alberta, British Columbia, or Quebec (where provincial legislation applies).[185]

Newmarket and Soofa maintain that all data collected by the benches is anonymous.[186] According to Soofa's privacy policy, "[a]fter receiving the non-identifiable data sent by mobile devices, Soofa applies a cryptographic function to the MAC addresses to further anonymize them."[187] But Timothy Yim, director of data and privacy at the Startup Policy Lab, says, "It is very hard to guarantee that any de-identification process is 100 percent fool proof."[188] Yim notes

---

175 Sidewalk Toronto, "Welcome to Sidewalk Toronto", online: *Sidewalk Toronto* <https://sidewalktoronto.ca/> [https://perma.cc/KBB8-5LEQ].

176 Brian Barth, "The fight against Google's smart city", *The Washington Post* (8 August 2018), online: <https://www.washingtonpost.com/news/theworldpost/wp/2018/08/08/sidewalk-labs/?utm_term=.a894bdb98978> [https://perma.cc/8F4S-W5EW]; Office of the Privacy Commissioner of Canada, Remarks at the IAPP Canada Privacy Symposium 2018 (speech) (Ottawa: OPC, 24 May 2018), online: <https://www.priv.gc.ca/en/opc-news/speeches/2018/sp-d_20180524/> [https://perma.cc/9U87-DA2Y] [OPC, "Remarks"] .

177 Sidewalk Toronto, *supra* note 175.

178 Barth, *supra* note 176.

179 OPC, "Remarks", *supra* note 176.

180 *Ibid*.

181 Edmonton, "Environment Week ISpy Soofa Launch", online: *Edmonton* <https://www.edmonton.ca/attractions_events/schedule_festivals_events/ispy-contest.aspx> [https://perma.cc/JQZ8-JVXK].

182 Newmarket, "Soofa solar-powered benches", online: *Newmarket* <https://www.newmarket.ca/LivingHere/Pages/Parks,%20Trails%20and%20Sport%20Fields/Solar-Power-Bench.aspx> [https://perma.cc/92ZD-4GT6].

183 *Ibid*.

184 *MFIPPA*, *supra* note 126.

185 *PIPEDA* , *supra* note 16.

186 *Ibid*; Soofa, "Privacy Policy", online: *Soofa* <http://www.soofa.co/privacypolicy/> [https://perma.cc/9SES-7G63].

187 Soofa, *supra* note 186.

188 Jill Odom, ""Smart" bench gathers data to help urban planners meet public's needs" (21 July 2017), online (blog): *Total Landscape Care* <https://www.totallandscapecare.com/landscaping-blog/smart-bench/> [https://perma.cc/66JX-NEMV].

that as more data accumulates in data repositories, re-identification becomes increasingly possible.[189] This is especially relevant insight because Soofa states in their privacy policy that they share data with various research organizations.

Soofa's method of passively collecting data makes it difficult to obtain meaningful consent and inform individuals of the collection's purpose, important aspects of MFIPPA and PIPEDA.[190] Soofa benches do not have notices telling passersby that they are being tracked, and Newmarket says that if people do not want the benches to access their device, they must turn off their Wi-Fi signal.[191]

Soofa benches also raise data security concerns. MFIPPA requires Ontario municipalities to have reasonable measures in place to protect personal information from unauthorized access.[192] PIPEDA stresses the implementation of safeguards relative to the sensitivity of the personal information held.[193] Much of Soofa's data protection emphasis seems to be on anonymity, which may not be guaranteed, rather than technological or physical safeguards.[194]

Similar privacy concerns may arise as smart space-monitoring technologies are integrated into existing buildings. As part of the Toronto Urban Pilot Program, a number of smart city technologies were selected to be tested in properties owned by QuadReal Property Group and the City of Toronto.[195] ArgosAI, for example, is a digitized data stream integrated with existing video cameras that can be used to count people, manage the use of space, automate security and room temperature, and measure the effectiveness of advertising tools.[196]

Because such a wide range of technologies can be categorized as promoting economic development, which privacy legislation applies will vary depending on the circumstances.

Conclusion

This report has examined the impacts smart cities may have on privacy and explored the potential for PIPEDA, Canada's private sector commercial privacy law, to regulate those impacts. Smart cities run on data, and this presents a balancing act between protecting privacy and obtaining useful data: the more detailed the data collected, the more useful it is. However, the more detailed the data, the likelier it is to include information about identifiable individuals, raising privacy concerns.

Canada's spectrum of privacy laws mediate the need for useful data and privacy. The first issue, however, is determining which legislation applies to the personal information dealing in question. Jurisdiction is particularly important when it comes to data collection, as there are different rules and standards depending on which legislation applies. Federal government institutions are governed by the *Privacy Act*. PIPEDA applies to federal works, undertakings, and businesses. Collection related to commercial activity is also governed by PIPEDA, unless the collection is solely within British Columbia, Quebec, or Alberta. Collection by a provincial

189 *Ibid*.

190 *Ibid*.

191 *Ibid*; Newmarket, *supra* note 182.

192 IPC, "Smart Cities, *supra* note 131.

193 *PIPEDA*, *supra* note 16.

194 Newmarket, *supra* note 182.

195 Max Greenwood, "UPPlift, QuadReal and Toronto Announce Seven Smart City Pilot Projects" (24 May 2018), online: *Techvibes* <https://techvibes.com/2018/05/24/upplift-quadreal-toronto-seven-smart-city-pilot-projects> [https://perma.cc/8BX4-KMC7].

196 *Ibid*; Argos AI, "Generate Actionable Insights Using Existing Architecture", online: *Argos AI* <https://argosai.co> [https://perma.cc/Z2KT-KBJS].

public sector organization is governed by provincial privacy laws, such as, in Ontario, FIPPA and MFIPPA. Legislative exceptions and holes in this patchwork mean that some dealings with personal information remain completely unregulated (e.g., federal political parties remain beyond the reach of these laws).

This report has examined smart city technologies to explore PIPEDA's jurisdiction, privacy concerns with smart city technologies, and the potential application of PIPEDA to those technologies. Smart city technologies are not monolithic; their functions, types, and producers vary. Which legislation applies will depend on the specific facts of the technology: the type of technology, the province in which it is located, whether the entity that controls it is public or private, and whether the activity is commercial.

Concerns

The review of smart city technologies and applications disclosed significant and serious privacy challenges. Personal information collected by smart city technologies can include everything from credit card information and purchasing preferences to sensitive medical information and individuals' minute-to-minute location. As a result, there is the overarching potential for detailed surveillance. It is not that every smart city technology presents a serious concern, or significant surveillance, but the potential to create an environment of surveillance exists, particularly as different technologies may be employed in the same physical area. Smart cities promise to improve the spaces in which we live, work, and play. These promises should not be accepted without acknowledging the potential dangers to individuals' privacy.

Smart cities are often characterized by public/private partnerships - arrangements between a public sector entity and a private sector entity to build out public services and/or infrastructure. Ordinarily, public sector privacy laws regulate public sector activities, and private sector privacy laws regulate private sector activities. Where a public entity contracts a private entity to perform public sector service activity, public sector privacy laws have historically applied. However, smart cities introduce additional factors that complicate this simple calculus. The addition to traditional public services of commercial elements, such as charging for those services or for new ancillary services, muddies the question of jurisdiction. Even public entities acting alone may engage in commercial activity that triggers the application of PIPEDA, such as where a university undertakes commercial activities (e.g., selling alumni lists) that fall outside of its core educational mandate in a commercial manner.

Dual jurisdiction occurs where an entity is subject to both a provincial privacy law and PIPEDA. In such cases, the entity is to look at the differences between the laws, and follow the most stringent requirements. One approach to the grey areas of jurisdiction for public/private partnerships is to treat personal information as though under dual jurisdiction. If a commercial service involves personal information collection, even for a public purpose, that data should be treated as if subject to dual jurisdiction: where it is unclear whether provincial laws or PIPEDA apply, whichever law provides the strictest requirements should be followed. This includes cases where a private sector actor is performing public services, or where new or ancillary services are added.

Solutions

PIPEDA and other Canadian privacy legislation are not obsolete, nor useless. But in the case of smart cities, their effects must be bolstered to fit new challenges. Reform to privacy laws must include enforcement powers, and modernizing privacy legislation to a higher standard, such as that of the European *General Data Protection Regulation*. These reforms should include:

- **A smart city policy at all levels of government:** this would benefit actors in every sector by removing uncertainty and providing a clear set of guidelines.

- **Technological recommendations to smart city actors:** would serve to set a minimum standard of what actors must achieve, such as privacy by design, and data minimization.
- **Designating certain types of data as 'No Go Zones,' or 'Proceed with Caution,' zones:** where data should never be collected, or collected only under certain controls, respectively.
- **Smart city data rights:** Canadian should explicitly be given smart city data rights such as the ability to view, delete, and download the personal information held about them. This right is available under existing privacy legislation, but should be made explicit in the case of smart cities.
- **Educating the public:** public education is important not only regarding data rights, but also the privacy concerns at play, and allowing individuals to take better ownership of their data and manage their personal information.

Smart city technologies are already here: collecting , using, and disclosing data. The sooner reforms and adaptations can be made to privacy legislation, the better their impact will be on smart cities: rather than clawing back information that shouldn't have been collected, or curbing undesirable practices after they've already been started, they can be blocked from occuring in the first place. The smart city presents a very clear challenge to the balance between individual privacy and technological promise, and protecting that balance should be of key concern to regulators.

ANNEX 1: Research Exceptions

The availability of data in the smart city space is very attractive to companies, as data can be used not only for marketing and business-structuring purposes, but also for larger goals such as analyzing, modelling, and training artificial intelligence applications, or selling the data to other companies to do so. Privacy laws differ in their exceptions to the overarching need for consent where data is being dealt with for research purposes, and how exactly these exceptions are structured is likely to affect how different entities structure their collection, use, and disclosure of personal information.

Under the Privacy Act, which applies to Federal government institutions, personal information may be used or disclosed

to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information would be made in a form that could reasonably be expected to identify the individual to whom it relates.[197]

Furthermore, information may be disclosed "[s]ubject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes."[198]

PIPEDA applies to the collection, use, and disclosure of personal information by federal works, undertakings, and businesses, or where there is commercial activity. In provinces with 'substantially similar' legislation, the provincial legislation applies instead. Generally speaking, PIPEDA and substantially similar provincial legislation require that consent be obtained to the collection, use, and disclosure of personal information. Under PIPEDA, the initial collection of personal information requires consent, even if the information is collected for research purposes. However, PIPEDA section 7(2) allows for the use of personal information for statistical, scholarly, or research purposes. Four conditions must be met for personal information to be used: the research purpose cannot be met without using personal information; the information must be used in a way that maintains confidentiality; consent must be impracticable to obtain; and the organization must inform the Privacy Commission before the information is used for the research purpose. Information may also be disclosed for statistical or research purposes, provided that the research purpose cannot be met without disclosing the personal information; consent is impracticable to obtain; and the organization informs the Privacy Commission prior to disclosure.

In summary, to fit under PIPEDA's research exemption of consent for use, consent must be obtained for the initial collection. Whether or not the primary purpose of collecting the information was research purposes, no consent is needed to use that information for research purposes, as long as the four conditions listed above are met. Information can also be disclosed for research purposes, as long as all three listed requirements are met.

197 *Privacy Act*, RSC 1985, c P-21 [Privacy Act] 7b

198 *Ibid.*

For example: A company that uses smart energy meters obtains consent from consumers to record information from their meters regarding energy use with the stated purpose of timing their use to lower costs. The company then decides they would like to research the ways in which individuals versus family homes use energy in order to customize their products towards different users. The company must use personal information regarding their users in order to meet this purpose. Information will be used in a way that maintains confidentiality, as all data will be aggregated to customer types rather than individuals. The company serves a large number of customers, many of whom do not respond to updates on their services. The company has informed the Privacy Commission before undergoing this research. The company does not need consent to use the data for research, or to disclose it, as the research purpose cannot be met without disclosing personal information, and consent is impractical to obtain.

Provinces with legislation substantially similar to PIPEDA:

Rather than focusing on use, the provinces focus on disclosure. This means that there does not need to be a focus on secondary or additional purposes, as that distinction is already assumed.

Quebec:

Quebec's ARPIPS legislation is structured differently than PIPEDA, but achieves a similar effect. Rather than focusing on personal information through the lens of collection, use, and disclosure, ARPIPS focuses on the parties: which entity is disclosing information, and which entity is receiving. If a party can be identified, the entity receiving the information must be authorized to do so.

An enterprise may communicate personal communication without consent to a person who is authorized to use that information for study, research, or statistical purposes, if the Commission d'Accès à l'Information (CAI) authorizes that person to receive it. Authorization depends on the CAI determining that the intended use is not frivolous, and cannot be achieved unless the information is communicated in such a way that the individual is identified; and that the information will be used in a way that ensures confidentiality. Such permission by the CAI must be obtained by completing and submitting a form. The permission is granted for a particular period, on particular conditions, and it may be revoked if such conditions are not respected. The CAI's discretion is complete on such matters, and there is no administrative appeal process.

An enterprise may communicate personal information for research purposes to any person without consent "if the documents containing the information are not structured so as to allow retrieval by reference to a person's name or identifying code or symbol and the information cannot be retrieved by means of such reference."[199] However, the person receiving the information must preserve the confidentiality "until 100 years have elapsed since the date of the document, or until more than 30 years have elapsed since the death of the person concerned."[200] The CAI has not yet rendered a decision on the interpretation of this provision.

For example: an independent research body would like to publish a study on energy consumers using smart meters, and would like this information from a smart meter energy company. In order to follow ARPIPS in the data transfer from the smarty energy meter company, they must submit the appropriate form to the CAI in order to be allowed to receive the information. To grant this permission, the CAI must be convinced that the study is not frivolous, that there must be personal information in order to complete the study, and that the confidentiality of the individuals involved will be protected. However, if the smart energy meter company is able to completely de-identify the information requested in such a way that it cannot be re-identified,

199 *Gratton*, *supra* note 24.

200 *Ibid.*

they may be able to transfer the information without consent. This approach, however, has not been tested.[201]

British Columbia:

British Columbia's PIPA legislation shares PIPEDA's structure of collection, use, and disclosure, but for the research exemption focuses on disclosure rather than collection and use. An entity may disclose personal information without consent, for a research purpose, if certain conditions are met: the research purpose cannot be accomplished without the personal information in identifiable form; the information disclosed will not be used to contact the individual to ask them to participate in the research; that the information is clearly in the public interest, and not harmful to individuals identified even if by linked information; the organization to which information is disclosed agrees to certain terms; and that it is impractical for the organization to seek the consent of the individual for disclosure.[202] The terms that must be complied with include the BC PIPA Act as a whole, policies and procedures relating to confidentiality; security and confidentiality measures, removal of individual identifiers at the earliest reasonable opportunity, and a prohibition of subsequent use without express authorization of the individually identifiable form without the express authorization of the organization disclosing the personal information.[203]

In practice, this would function very similarly to Quebec's ARPIPS, but rather than requiring consent from a state regulator, the organization to which the personal information is to be disclosed must sign an agreement with the disclosing organization to comply with the terms listed above.

Alberta:

Alberta's PIPA also keeps the PIPEDA format of 'collection, use, and disclosure,' but functions in a way that is a hybrid of Quebec's ARPIPS and BC's PIPA: it allows disclosure without consent, and requires approval by an external body. Alberta's PIPA functions differently when the organization in question is an archival one, but for the purposes of this report this section will focus on non-archival institutions. Alberta's PIPA permits an organization to disclose personal information without consent for research purposes where it would be unreasonable to obtain consent as long as the disclosure meets the following conditions: the person to whom the information is to be disclosed enters into a research agreement (which has its own requirements); the research has been approved by a recognized research ethics review committee (such as an ethics committee of a national research council or a professional regulatory organization); and the researcher has agree to any additional conditions imposed by the ethics review committee.[204] The requirements for the research agreement must at a minimum include the person to whom the information is to be disclosed agreeing:

- to use the information only for the research purpose,
- to make reasonable security arrangements to protect the information,
- to maintain the confidentiality of the information,
- to not contact any individual to whom the information relates,
- to remove or destroy, at the earliest reasonable time, individual identifiers,
- to not disclose the information in individually identifiable form, and

201 *Ibid.*

202 *Personal Information Protection Act*, SBC 2003, c 63 [*BCPIPA*] 21

203 *Ibid.*

204 *Service Alberta, Collection, Use and Disclosure of Personal Information for Archival and Research Purposes (PIPA Information Sheet 8)* online: <http://provincialarchives.alberta.ca/docs/who-we-are/about-us/opman/PIPAInformationSheet8.pdf> 8-9.

- to notify the archival institution immediately of a breach of the agreement.[205]

In summary, the individual who seeks information for a research purpose must enter into a research agreement with the above requirements, and to which more requirements may be added by the disclosing institution; have their research approved by an ethics review committee, and agree to any further conditions imposed by the research ethics committee. It must also be unreasonable to gain the consent of the individual that the information is about.

This chart further lays out the research exception to consent characteristics by province:

Legal instrument	Specified allowed uses	Section(s)	Conditions
PIPEDA (Federal)[206]	Research Scholarly study Statistical	s7(2)(c)	**Information may be USED if:** • Purpose cannot be achieved without using the information • Information is obtained in a manner that ensures confidentiality • Impracticable to obtain consent • Organization using information informs the Privacy Commissioner before information is used
		s7(3)(f)	**Information may be DISCLOSED if:** • Purpose cannot be achieved without disclosing the information • Impracticable to obtain consent • Organization using information informs the Privacy Commissioner before information is disclosed

	Historical or Archival importance	s7(3)(g)	**Information may be DISCLOSED to an institution whose functions include conservation of historic or archival records if:**
			• It is made for the purposes for conservation
			• And is made the earlier of:
			  • 100 years since record was created;
			  • 20 years of the individual whom information is about.

ARPPIPS (QC)[207]	Research (without Commission d'accès à l'information (CAI) approval)	s18.2	**Information may be COMMUNICATED if:** • Information is structured in a way as to not allow retrieval by reference to a person's name, identifying code, or symbol. • Person to whom information is communicated must preserve confidentiality during the period it may not be communicated.
	Research Scholarly study Statistical (with CAI approval)	s18(8) s21	**The Commission d'accès à l'information (CAI) may grant a person authorization to RECEIVE communication of personal information if:** • Intended use is not frivolous • The ends contemplated cannot be achieved unless the information is communicated unless the identifying information is communicated. • The information will be used in a manner that ensures confidentiality Such an authorization by the CAI will be granted for a period and on conditions fixed by the Commission, and may be revoked if the CAI believes that the authorized person does not respect confidentiality or the other conditions imposed.

205 *Ibid.*

206 *PIPEDA*, *supra* note 16.

207 *ARPPIPS*, *supra* note 172.

PIPA (BC)[208]	Research Statistical	s21(1)	**Information may be DISCLOSED if:** • Purpose cannot be achieved unless identifiable information is provided • Information will not be used to contact persons to ask them to participate in research • Linkage of the information to other information is not harmful to the individuals identified and linkages formed are clearly in the public interest • Organization to be disclosed to has signed an agreement agreeing to: ○ This act; ○ The policies and procedures relating to confidentiality of identified persons adopted by the collecting organization; ○ Security and confidentiality conditions; ○ A requirement to remove or destroy identifying information at the earliest possible opportunity; ○ A prohibition of any subsequent use or disclosure without the express authorization of the disclosing party. • It is impracticable for the organization to seek consent of the individual for disclosure.
	Prohibition on Market Research	s21(2)	Section 21(1) does not authorize disclosure for the purposes of market research.
	Archival or Historical Purposes	s22	**An organization may DISCLOSE personal information for archival or historical purposes if:** ○ A reasonable person would not consider the information too sensitive to the individual disclosed at the proposed time; ○ The disclosure is in accordance with s21; ○ The information is about someone who has been dead for 20+ years; ○ The information is in a record that has existed for 100+ years.

208 *BCPIPA*, *supra* note 203.

PIPA (AB)[209]	Archival	s14(j) s17(k) s20(p) Regulations s11 s12 s13	**An organization may COLLECT/USE/DISCLOSE information if:** • It is an archival institution and the collection/use/disclosure of the information is reasonable for archival or research; **An archival institution is:** • An institution to which archival records are transferred for permanent preservation; • And provides public access to its archival collections. **Archival institutions may COLLECT/USE information:** • as part of carrying out the archival purposes, may engage in the appraisal, acquisition, conservation, arrangement and description of records. **Archival institutions may DISCLOSE information if:** • It is necessary for the research purpose; • The information is not harmful to the individual concerned; • The research purpose is not contrary to the purposes and intent of the Act; • Either; ○ A reasonable person would find the disclosure appropriate at the time; ○ The research is disclosed under a research agreement; • If under a research agreement, the receiving party must agree: ○ To use information only for research purposes; ○ To make reasonable security arrangements to protect the information; ○ To maintain confidentiality of the information; ○ To not contact any individual related to the information; ○ To remove or destroy at the earliest reasonable time individual identifiers; ○ To not disclose the information in individual identifiable form; ○ To notify the archival institution immediately of a breach of the agreement. **Archival institutions may not USE/DISCLOSE information for any purpose other than archival or research.**

209 *ABPIPA*, *supra* note 204.

	Non-Archival Organization Research	s14(k) s17(l) s20(q) Regulations s14	**An organization that is not an archival institution may COLLECT/USE/ DISCLOSE information if:** • It meets the requirements set out in the regulations for archival or research; • It is not reasonable to obtain consent. **An organization that is not an archival institution may COLLECT/USE information for archival purposes if:** • To transfer historical records to an archival institution; • The preparation of organizational records for archival appraisal and transfer to an archival institution **An organization that is not an archival institution may DISCLOSE information for archival purposes to:** • Obtain an archival appraisal of the organization's records. • Transfer custody and control to an archival organization **An organization that is not an archival institution may DISCLOSE information under a research agreement only if:** • The receiving party must agree: ○ To use information only for research purposes; ○ To make reasonable security arrangements to protect the information; ○ To maintain confidentiality of the information; ○ To not contact any individual related to the information; ○ To remove or destroy at the earliest reasonable time individual identifiers; ○ To not disclose the information in individual identifiable form; ○ To notify the sending institution immediately of a breach of the agreement. • The research has been approved by a recognized research ethics review committee (at a university or educational institution in Alberta) • The receiving party agrees to any additional conditions imposed by the ethics review committee.

ANNEX 2: Commercial Activity

Commercial activity is one of the two triggering parts for PIPEDA, the other being federal works, undertakings, or businesses. Commercial activity is, however, a difficult to define concept. While many different pieces of legislation refer to commercial activity, they have different definitions. Below are some examples of the different definitions and uses of the concept of commercial activity.

Source	Definition of "commercial activity"	Key
Personal Information Protection and Electronic Documents Act[210]	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	Of commercial character
Ontario (Regional Assessment Commissioner) v. Caisse populaire de Hearst Ltée; *Re Windsor-Essex County Real Estate Board and City of Windsor*[211]	"**Commercial activity**" has been judicially considered in a business context and found to require a preponderant purpose of making a profit. All relevant factors must be considered and weighed.	Purpose of making a profit
State Immunity Act[212]	It is not, however, always easy to discern whether an activity is a **commercial activity**, with the Act defining "**commercial activity**" in a somewhat circular fashion to mean "any particular transaction, act or conduct or any regular course of conduct that by reason of its nature is of a commercial character".	Of commercial character

210 *PIPEDA*, *supra* note 16.

211 *Ontario (Regional Assessment Commissioner) v Caisse populaire de Hearst Ltée*, [1983] SCJ No 8, [1983] 1 SCR 57 (SCC); *Re Windsor-Essex County Real Estate Board and City of Windsor*, [1974] OJ No 2135, 6 OR (2d) 21 (Ont CA).

212 *State Immunity Act*, RSC 1985, c S-18, s 2 [*SIA*].

The Comprehensive Economic and Trade Agreement 121, 123, Schedules V to X[213]	"**commercial activity**" *of a person means* (a) a business carried on by the person (other than a business carried on without a reasonable expectation of profit by an individual, a personal trust or a partnership, all of the members of which are individuals), except to the extent to which the business involves the making of exempt supplies by the person, (b) an adventure or concern of the person in the nature of trade (other than an adventure or concern engaged in without a reasonable expectation of profit by an individual, a personal trust or a partnership, all of the members of which are individuals), except to the extent to which the adventure or concern involves the making of exempt supplies by the person, and (c) the making of a supply (other than an exempt supply) by the person of real property of the person, including anything done by the person in the course of or in connection with the making of the supply.	Business for reasonable expectation of profit; in the nature of trade
Harmonized Sales Tax Act[214]	"**commercial activity**" means a commercial activity as defined in subsection 123(1) of the Excise Tax Act (Canada). [see below]	---
Act respecting the Québec sales tax[215]	"**commercial activity**" *of a person means* (1) a business carried on by the person, other than a business carried on without a reasonable expectation of profit by an individual, a personal trust or a partnership, all of the members of which are individuals, except to the extent to which the business involves the making of exempt supplies by the person, (2) an adventure or concern of the person in the nature of trade, other than an adventure or concern engaged in without a reasonable expectation of profit by an individual, a personal trust or a partnership, all of the members of which are individuals, except to the extent to which the adventure or concern involves the making of exempt supplies by the person, and (3) the making of a supply, other than an exempt supply, by the person of an immovable of the person, including anything done by the person in the course of or in connection with the making of the supply.	---
State Immunity Act[216]	**Commercial activity** includes any particular transaction, act or conduct or any regular course of conduct that by reason of its nature is of a commercial character	Of a commercial character

213 *Canada-European Union Comprehensive Economic and Trade Agreement*, 30 October 2016, (entered into force 21 September 2017).

214 *Harmonized Sales Tax Act*, SNB 1997, c H-1.01.

215 *Act respecting the Québec sales tax*, CQLR c T-0.1, s 1.

216 *SIA*, *supra* note 212.

Re Canada Labour Code; *University of Calgary v. Colorado School of Mines; Ferguson v. Arctic Transportation Ltd.*; *Butcher v. Saint Lucia*; *Sarafi v. Iran Afzal (The)*; *El Ansari v. Maroc*; *Accurso v. Royaume du Maroc*; *Collavino Inc. v. Yemen (Tihama Development Authority)*; *Smith v. Chin*; *Kuwait Airways Corp. v. Iraq*; *Bedessee Imports Ltd. v. Guyana Sugar Corp.*; *Bouzari v. Islamic Republic of Iran*; *Steen v. Islamic Republic of Iran*.[217]	In determining whether an activity is commercial, the courts may consider the purpose of the activity as well as its nature	Consider the purpose and nature of the activity
Alberta Personal Information Protection Act[218]	In this section, "**commercial activity**" means (i) Any transaction, act or conduct, or (ii) Any regular course of conduct That is of a commercial character and, without restricting the generality of the foregoing, includes the following: (iii) The selling, bartering or leasing of membership lists or of donor or other fund raising lists; (iv) The operation of a private school or early childhood services program as defined in the School Act; (v) The operation of a private college as defined in the Post-secondary Learning Act	Of commercial character

217 *Re Canada Labour Code*, [1992] SCJ No 49, 91 DLR (4th) 449 (SCC); *University of Calgary v Colorado School of Mines*, [1995] AJ No 1026, [1996] 2 WWR 596 at 608 (Alta QB); *Ferguson v Arctic Transportation Ltd* (1995), 101 F.T.R. 16 (FCTD); *Butcher v Saint Lucia*, [1998] OJ No 2026 (Ont Div Ct); *Sarafi v Iran Afzal (The)*, [1996] FCJ No 519, 111 FTR 256 (FCTD); *El Ansari v Maroc*, [2003] JQ no 13913, JE 2003-1973 (Qc CA); *Accurso v Royaume du Maroc*, [2003] JQ no 18660, JE 2004-289 (CQ) (no commercial activities); *Collavino Inc v Yemen (Tihama Development Authority)*, [2007] AJ No 531, 42 CPC (6th) 83 (Alta QB) (contract for construction of water canals and works was a commercial activity); *Smith v Chin*, [2006] OJ No 4091, 31 CPC (6th) 114 (Ont Sup Ct) (economic development program providing citizenship and passport privileges was commercial); *Kuwait Airways Corp v Iraq*, [2010] SCJ No 40, [2010] 2 SCR 571 (SCC) (active participation in litigation defending a state-owned corporation removed immunity from costs award); *Bedessee Imports Ltd v Guyana Sugar Corp*, [2010] OJ No 4575, 329 DLR (4th) 382 (Ont CA), leave to appeal refused [2010] SCCA No 476 (SCC) (defamatory statements made in a trade-mark dispute considered commercial); *Bouzari v Islamic Republic of Iran*, [2004] OJ No 2800 at paras 51-55, 71 OR (3d) 675 (Ont CA), leave to appeal refused [2004] SCCA No 410 (SCC); *Steen v Islamic Republic of Iran*, [2013] OJ No 228 at paras 17-22, 114 OR (3d) 206 (Ont CA) (demands for ransom not rendering state-sponsored kidnapping commercial).

218 *ABPIPA*, *supra* note 204.

Halsbury's Laws of Canada - Income Tax (General) (2017 Reissue)[219]	**Taxpayer's intention**. A **commercial activity** is one that the taxpayer undertakes for profit. The taxpayer's intention is determined by looking at objective evidence to support his or her intentions. The taxpayer must establish that his or her predominant intention is to make a profit from the activity and that he or she carries on the activity in accordance with objective standards of business behaviour. Thus, one looks at: • 1.The taxpayer's profit and loss experience in past years; • 2.The taxpayer's training and expertise in the field of his or her activities; • 3.The taxpayer's intended course of action; and • 4.The financial viability of the venture to show a profit. This is not an exhaustive list and the factors to be taken into account in determining intention will differ according to the facts and circumstances of each case. Thus, having a reasonable expectation in the financial viability of the venture to show a profit is only one of the factors in evaluating the taxpayer's intention and, by itself, it is not conclusive.	Commercial activity is one that the taxpayer (objectively) undertakes for profit
Halsbury's Laws of Canada - Taxation (Goods and Services) (2015 Reissue)[220]	"**Commercial activity**" of a person is defined to mean a business or an adventure in the nature of trade, except where it is engaged in by an individual, a personal trust or a partnership without a reasonable expectation of profit, or the making of a supply of real property including anything done by the person in the course of or in connection with that supply of real property. Excluded from this definition are exempt supplies (citing (CAN) *Excise Tax Act*, R.S.C. 1985, c. E-15, s. 123(1) "**commercial activity**".)	Business or venture in the nature of trade with a reasonable expectation of profit
Governor in Council Education Act Regulations[221]	For the purposes of Section 64A of the Act, "**commercial activity**" of a school includes entering into an agreement with a person to permit the person, for a fee, to place advertising posters in a school administered by the school board"	Can include agreements of schools to advertise

219 Vern Krishna, *Halsbury's Laws of Canada - Income Tax (General)* (Toronto: LexisNexis Canada, 2017).

220 Ronald J Maddock & Brian C Pel, *Halsbury's Laws of Canada - Taxation (Goods and Services)* (Toronto: LexisNexis Canada, 2015).

221 *Governor in Council Education Act Regulations*, NS Reg 74/1997, s 86.

An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act[222]	A "**commercial activity**" is broadly defined under CASL and covers "any particular transaction, act or conduct or any regular course of conduct that is of commercial character, whether or not the person who carries it out does so in the expectation of profit …"	Of commercial character
Excise Tax Act[223]	"**Commercial activity**" of a person is defined to mean a business or an adventure in the nature of trade, except where it is engaged in by an individual, a personal trust or a partnership without a reasonable expectation of profit, or the making of a supply of real property including anything done by the person in the course of or in connection with that supply of real property. Excluded from this definition are exempt supplies	Business or venture in the nature of trade with a reasonable expectation of profit
Halsbury's Laws of Canada - *Public International Law* (2014 Reissue) - HPI-81 Commercial activity exception[224]	any particular transaction, act or conduct or any regular course of conduct that by reason of its nature is of a commercial character.	Of a commercial character
Rodgers v. Calvert[225]	consideration in contract does not in itself lead to the finding of commercial activity in the PIPEDA context. In my view, there must be something more than a mere "exchange of consideration", as described by counsel, to be within the definition of "commercial activity". (PIPEDA specific case)	More than mere exchange of consideration

222 *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, s 1(1).

223 *Excise Tax Act*, RSC 1985, c E-15, s 123(1).

224 Halsbury's Laws of Canada (online), *Public International Law*, "Jurisdictional Immunities: State Immunity: Exceptions From Immunity" (VII.1.(2)) at HPI-81 "Commercial activity exception." (2014 Reissue).

225 *Rodgers v Calvert* (2004), 244 DLR (4th) 479, 49 BLR (3d) 53 (Ont Sup Ct).

ANNEX 3: Carve-outs for legislation 'substantially similar' to PIPEDA

For legislation to be 'substantially similar' to PIPEDA, and thus supercede PIPEDA in provincial application, it must be officially deemed so. Below are the pieces of legislation that officially confer the status of 'substantially similar' on legislation in Canada, current to the December 31st 2018.

http://laws-lois.justice.gc.ca/eng/regulations/SI-2012-72/page-1.html

> "Any personal health information custodian to which the *Personal Health Information Act*, SNL 2008, c P-7.01, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of the collection, use and disclosure of personal health information that occurs in Newfoundland and Labrador."[226]

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-265/page-1.html

> "Any personal health information custodian to which the *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of the collection, use and disclosure of personal health information that occurs in New Brunswick."[227]

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-399/page-1.html

> "Any health information custodian to which the *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Schedule A, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of the collection, use and disclosure of personal information that occurs within the Province of Ontario."[228]

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-219/page-1.html

> "An organization, other than a federal work, undertaking or business, to which the *Personal Information Protection Act*, S.A. 2003, c. P-6.5, of the Province of Alberta, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act*, in respect of the collection, use and disclosure of personal information that occurs within the Province of Alberta."[229]

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-220/page-1.html

> "An organization, other than a federal work, undertaking or business, to which the *Personal Information Protection Act*, S.B.C. 2003, c. 63, of the Province of British Columbia, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act*, in respect of the collection, use and disclosure of personal information that occurs within the Province of British Columbia."[230]

http://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-374/page-1.html

> "Any organization, other than a federal work, undertaking or business, that carries on an enterprise within the meaning of section 1525 of the Civil Code of Québec and to which *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1, applies is exempt from the application of Part 1 of the *Personal Information Protection and Electronic Documents Act* in respect of the collection, use and disclosure of personal information that occurs within the Province of Quebec."[231]

226 *Personal Health Information Custodians in Newfoundland and Labrador Exemption Order*, SI/2012-72.

227 *Personal Health Information Custodians in New Brunswick Exemption Order*, SOR/2011-265.

228 *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399.

229 *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219.

230 *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.

231 *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.