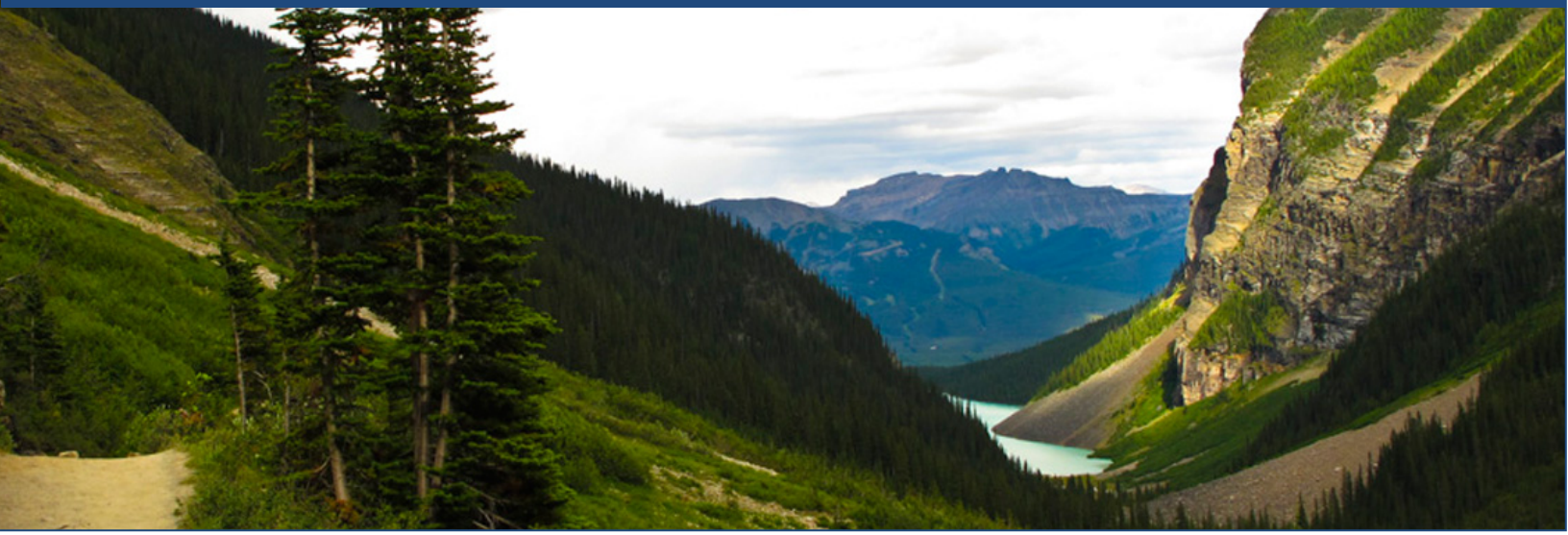
Energy Consumption Data and Rights to Privacy:

Climate change mitigation policy, privacy and the "internet of things" in Alberta



Prepared By
Astrid Kalkbrenner and Jason Unger
Environmental Law Centre (Alberta)

January 17, 2018

Environmental Law Centre

The Environmental Law Centre (Alberta) Society

The Environmental Law Centre (ELC) has been seeking strong and effective environmental laws since it was founded in 1982. The ELC is dedicated to providing credible, comprehensive and objective legal information regarding natural resources, energy and environmental law, policy and regulation in the Province of Alberta. The ELC's mission is to educate and champion for strong laws and rights so all Albertans can enjoy clean water, clean air and a healthy environment. Our vision is a society where laws secure an environment that sustains current and future generations.

Environmental Law Centre
#410, 10115 – 100A Street
Edmonton, AB T5J 2W2

Telephone: (780) 424-5099
Fax: (780) 424-5133
Toll-free: 1-800-661-4238
Email: elc@elc.ab.ca

Website: www.elc.ab.ca
Blog: www.elc.ab.ca/blog/
Facebook: http://www.facebook.com/environmentallawcentre
Twitter: https://twitter.com/ELC_Alberta
To sign up for email updates visit: http://elc.ab.ca/newsandmedia/news/

Charitable Registration #11890 0679 RR0001

Acknowledgements

The Environmental Law Centre would like to thank our supporters that have made this project possible. This report, along with other work in relation to climate mitigation and adaptation was funded by the Alberta Law Foundation.

The ELC would also like to thank Stephanie Joyce, a law student who joined us for the summer and provided essential research in support of this report.

Executive Summary

We live in a data rich environment. The current and future state of climate mitigation regulation, policy and programming undertaken by governments requires ongoing tracking and understanding of energy consumption and efficiency across society. Data is not only necessary for evaluation of policy and regulatory directions but can act as a significant motivator in changing behaviour. The behaviours of state actors, individuals, and the private sector in how they monitor, gather and disclose information is central to ensuring privacy rights are not infringed.

A review of privacy legislation, both federally and provincially, indicates that there is a need to increase effectiveness of gathering energy consumption information to efficiently evaluate the effectiveness of climate policy. Similarly, there is a need to clarify what type of private information should be publicly disclosable to foster goals related to education and awareness among citizens.

The Environmental Law Centre recommends undertaking a statutory reform to ensure public authorities[1] have the tools they need for climate mitigation policies to succeed while respecting the privacy of citizens. The amendments proposed are focused on efficient and effective data gathering and sharing among public authorities and utilities and providing additional clarity around when and how data may be gathered, used, shared and distributed by public authorities to facilitate individual behavioural changes.

The amendments are responsive to several barriers that have been identified in the existing regulatory scheme, including a lack of municipal powers to require data disclosure for climate based programs, a lack of ability or clarity around data sharing among public authorities and

[1] "Public Authorities" are inclusive of local government bodies, such as municipal governments, departments and branches of government, agencies, board or commissions, and offices of the executive branch of government.

utilities, and a lack of clarity around public disclosure of energy consumption that provide individual motivators to augment behavior.

Alberta laws should be amended to ensure:

1. Statutory powers to gather, use and disclose information on energy consumption exist for relevant public authorities (i.e., municipal, provincial, and federal).

2. Sufficient flexibility exists to allow sharing of energy consumption information among and within public authorities with clear limits on use and disclosure.

3. Clear disclosure rules exist for public authorities to access and use energy consumption data gathered by utilities. This data, once disclosed to public authorities, should be presumed to be confidential except where aggregated.

4. Limit the use of energy consumption data for the purpose for which it is gathered or for the administrative, enforcement, and evaluation of climate relevant regulations, policies and programs.

5. Privacy legislation should be amended to clarify the types and nature of energy consumption data that is sufficiently "de-identified" or anonymized to enable and allow for public disclosure.

Table of Contents

INTRODUCTION

> *[P]rivacy can never be absolute. It must be balanced against legitimate societal needs. This court has recognized that the essence of such a balancing process lies in assessing a reasonable expectation of privacy and balancing that expectation against the necessity of interference from the state . . . The greater the reasonable expectation of privacy and the more significant the deleterious effects flowing from its breach, the more compelling must be the state objective and the salutary effects of that objective in order to justify interference with this right.*
>
> Justice L'Heureux-Dubé -Supreme Court of Canada - *R. v. O'Connor* [1995] 4 S.C.R. 411

Your neighbour keeps their house at 16 °C when they are at work. The house burns through natural gas at a rate indicating your neighbour's house has below average insulation in the attic. We know when they went to work and how much gas they consumed on the way, thanks to the car's GPS and onboard computer measuring fuel consumption. This information is relayed to a search engine that then targets your neighbour with advertisements about attic insulation, green rebates, and riding a bike. Real scenario or not? Privacy and the *internet of things* has opened a new era of what is private, what may be commercialized and what is validly collected and considered by governments to administer effective climate mitigation policy.

Climate change legislation and policy for the most part attempts to address big sources of pollution – industrial sectors including oil and gas production, electricity generation, building construction and operation, and other industrial emissions. The approach is understandable since these sectors are responsible for the majority of emissions and pollution. Compared to these sectors, the quantities of emissions of an individual person seem to be little. However,

the sum of individual emissions is significant.[2] Attention to individual pollution and how it could and should be dealt with is increasing among environmental legal scholars, legislators and regulators.[3]

Attempts to alter emissions from individuals, corporations and institutions are essential to broader goals of altering emission trajectories as a society. Altering carbon footprints may take the form of regulation or focus on voluntary measures driven by increased knowledge of consumption and monetary incentives (either inherent in becoming more energy efficient or through government rebate programs). A combination of regulation and market pressure may also be applied, as is currently the case in Alberta with a carbon levy and increased policies and programs focused on efficiency.[4]

What is the "Internet of Things"?

Wikipedia describes "the Internet of things (IoT)" as "the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data." See also: Forbes and Business Insider for further descriptions.

[2] Katrina Fischer Kuh, "Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms" (2012) 65:6 *Vanderbilt Law Review* 1566 at 1575. "Individuals constitute a regulatory target that is notably distinct from the archetypal regulatory target in environmental law, the polluting factory. Individuals are more numerous and more widely dispersed. They contribute to pollution in amounts that are often invisible at the time of release, impose harms that are frequently chronic (as opposed to acute), and become significant only when aggregated over time or with the contributions of others."

[3] *See e.g.* John C Dernbach, "Harnessing Individual Behavior to Address Climate Change: Options for Congress" (2008) 26 Va Envtl L J 107 at 123-24, 132, 144; Michael P Vandenbergh & Anne C Steinemann, "The Carbon-Neutral Individual" (2007) 82 *NYU L Rev* 1673 at 1724. Vandenbergh comments: "We are polluters. Each of us. We pollute when we drive our cars, fertilize and mow our yards, pour household chemicals on the ground or down the drain, and engage in myriad other common activities. Although each activity contributes minute amounts of pollutants, when aggregated across millions of individuals, the total amounts are stunning." Michael P Vandenbergh," From Smokestack to SUV: The Individual as Regulated Entity in the New Era of Environmental Law" (2004) 57 *Vand L Rev* 515 at 518.

[4] Kuh, *supra* note 21 at 1566. States can indirectly regulate environmentally significant individual behaviors by directly regulating the market (examples: subsidies on purchase of hybrid or e-cars and taxes on SUVs); or directly regulate environmentally significant individual behaviors by imposing mandates on individuals (example: anti-idling law combined with fines).

> A failure to recognize the regulatory benefits of personal environmental information could result in privacy controls that too greatly and unnecessarily constrain access to information. A failure to recognize the privacy harms occasioned by the development of personal environmental information could not only impose unwarranted privacy harms but, once these harms are discovered, could also spur a backlash that even more greatly constrains access to personal environmental information.
>
> Katrina Fischer Kuh[5]

Increased access to individual environmental data offers great benefits for environmental law, policy and regulation. However, new technologies that disclose individual environmental information not only offer regulatory benefits but also potentially infringe on individual privacy.[6]

Katrina Kuh points out that "[t]echnology continues to increase the ability to detect and record individual behaviors; modern computing further allows for the volumes of amassed data to be readily compiled and searched."[7] Every person leaves behind an electronic trail that comprises location information from cell phones and GPS in cars, personal consumption choices during online shopping or using store saving cards. As the amount of individual environmental information that is feasible to collect increases the social expectation of privacy will become increasingly relevant to how we support and evaluate environmental regulation.[8]

---

[5] Kuh at 1574.
[6] Kuh, *ibid* at 1569.
[7] Kuh, *ibid* at 1571; Daniel J Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 *S Cal L Rev* 1083 at 2.
[8] Kuh, *ibid* at 1570.

Pursuing effective climate mitigation policy and programming requires effective and comprehensive data acquisition, use and dissemination. Whether the data is used to track regulatory effectiveness or used to shine a light on costly and inefficient behaviors, there is a balance between the information systems and the potential infringement of a reasonable expectation of privacy. The nature of these data needs are such that data sharing among public authorities is likely to be essential, as the financial and human capacity to manage this information is likely to be tested.

Pursuing effective climate mitigation policy and programming requires effective and comprehensive data acquisition, use and dissemination.

This paper explores privacy issues of energy consumption data. The focus is on federal and provincial privacy frameworks in operation in Alberta and how government monitoring, use and disclosure of energy consumption information is currently regulated. A brief case summary of the Ontario approach is also considered.

An expectation of privacy

Expectations of privacy are not static. Information some people guard as highly private others treat cavalierly. In this regard, the concept of privacy is difficult to pin down. Individual versus industry privacy is often viewed differently and privacy concerns fluctuate with the nature of the information. Yet privacy is typically seen a foundation of our concept of a free and

democratic society. Privacy has been described as "an ill-defined but apparently well-understood concept".[9] Further, it has been observed:[10]

> privacy in any given situation may be in tension with other values and desires of the individual, subgroups, and society at large. Privacy, like most other values in modern democratic societies, is not an absolute but rather must be interpreted and weighed alongside other socially important values and goals. How this balancing (which need not mean equivalent weighing) is to be achieved is often the center of the controversy around privacy, because different people and groups balance in different ways these values that are in tension.

It is in this complex framing that we look at the current legislative and regulatory treatment of privacy in Canada and in Alberta. The notion of privacy is further complicated when one considers societal goals around pollution and carbon footprints related to energy consumption. There may be broad acceptance of disclosure of pollution among the corporate sector but it has not translated to individual pollution disclosure. Should individuals be subjected to the same pollution disclosure requirements of corporations, and if not, why not? We do not endeavour to answer this question in this report rather we consider the current state of how privacy of energy consumption data is treated in Alberta and in Canada.

There are various parties that have an interest in accessing energy consumption data: utility companies, government, commercial enterprises, third party researchers, law enforcement entities and of course individuals themselves.[11] A variety of privacy frameworks apply to

---

[9] See James Waldo, Herbert S Lin, and Lynette I Millett, *Engaging Privacy and Information Technology in a Digital Age,* eds, Committee on Privacy in the Information Age, National Research Council (Washington D.C.; National Academy of Sciences, 2007), online at: <https://pdfs.semanticscholar.org/5030/45f1f73746fd2f31f34d9ef466096 1ec53a2.pdf>.

[10] Waldo, Lin & Millet, *ibid.* at 22.

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

different enterprises. The focus of this report is on the gathering and use of information by *public authorities*, including all levels of government (provincial, federal and municipal), and to a lesser degree on the powers of utilities to disclose information to the public and/or other parties. The report concludes by making recommendations to ensure the benefits of energy consumption disclosure and privacy are effectively balanced in tackling society's climate mitigation challenges.

How the "internet-of-things" will change the privacy discussion

The world has quickly evolved into an integrated system of information "sharing" and gathering. As this "internet of things" evolves and broader adoption of *smart metering* and *smart grid* technologies occurs, there will be heightened ability to scrutinize individual data generators such as the personal habits and activities of individual energy consumers. Thus, private data might be subject to a variety of abuse, such as profiling and data mining of information on consumer behaviour; exploitation for direct marketing purposes; and event-driven marketing.[12] Another concern is price discrimination resulting from information imbalance between consumers and energy suppliers/third parties.[13]

Smart grids and smart meters generate energy consumption data of individual households and commercial buildings. Generally, a smart grid enables a "two-way flow of electricity and

[12] Eva Fialová, "Smart Grid and Surveillance" (2015) 1 *JURA* 197; Harvey, *ibid*. Event-driven marketing refers to scenarios where mined data reveal a technical issue of for example household appliances or devices (higher energy consumption) and thus trigger unsolicited offers for replacement devices etc.
[13] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Commission Recommendation on Preparations for the Roll-out of Smart Metering Systems*, (2012) at 6, online: <http://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf>.

information to create an automated, widely distributed energy delivery network."[14] Energy consumers receive more information about their consumption and thus influence their behaviour into a better direction i.e. energy saving.

Real-time measurement means far more information and especially very detailed information about the consumers is generated, collected and potentially used for a variety of purposes.

An important difference between a traditional electricity meter and smart meter is that the former measures total electricity usage whereas the latter measures a home's energy usage in near real-time (e.g. a 15-minutes interval).[15] Real-time measurement means far more information and especially very detailed information about the consumers is generated, collected and potentially used for a variety of purposes.

The data discloses consumers' daily routines and give a detailed picture about someone's private life, such as when the kettle runs, the garage door opens, the TV is on, whether the home security system has been activated or certain medical equipment is used.[16] Through the near real-time energy consumption measurement, consumers can better assess, with more detail, their own consumption and choose to alter their behaviour to reduce their energy consumption and save money.[17] The awareness of current energy usage might shift behaviour

[14] H Russell Frisby & Jonathan P Trotta, "The Smart Grid: The Complexities and Importance of Data Privacy and Security" (2010-2011) 19 *CommLaw Conspectus* 297 at 300. See also Fialová *supra* note 10 at 2070.
[15] Harvey, *supra* note 9 at 2072.
[16] Elias Leake Quinn, "Smart Metering & Privacy: Existing Law and Competing Policies", report for the Colorado Public Utilities Commission (2009) at 3; US Department of Energy, "Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy", DOE Request for Information, 75 Fed. Reg. 26203 at 26205 (July 12, 2010) [US Dep. of Energy 2010].
[17] Harvey, *supra* note 9 at 2072.

from using energy during expensive peak hours to cheaper periods.[18] Also, consumers will be able to identify inefficient home appliances and make upgrades accordingly.[19]

Consumer behaviour is expected to change because smart meter technology enables utility companies to track household energy consumption in greater detail which in turn also results in higher energy prices during peak periods. [20] Smart technology like smart appliances connected to smart meters receive energy price signals and shift to different modes with reduced electricity usage in order to benefit from discounted energy prices or to avoid high energy costs during peak hours.[21]

However, a future widely deployed smart grid entails a potential conflict between the generation and collection of massive data (Big Data[22]) and data privacy over the use and privacy of energy consumption data. Smart data offer a very detailed picture of an individual's life and behavior. These data are of interest to a variety of stakeholders such as the

> *Smart grid technology's success depends on its "ability to encourage and accommodate innovation while making usage data available to consumers and certain third party service providers in a responsible manner, and respecting individual consumer choices in how to balance the benefits of access to usage data against the protection of personal privacy and security"*

[18] Harvey, *ibid* at 2073.
[19] Harvey, *ibid* at 2073. Other promises and benefits with the advancement from ordinary electrical grids to smart grids are cited to include: improved reliability, prevention of power outages or quicker outage responses; reduction in peak demand; reduction of line loss; increased energy efficiency; lower costs with behavior changes; and reduced energy consumption (with coinciding reduced need for expenditures on expanding supply). See US Department of Energy 2010, *supra* note 14; Federal Communications Commission, *Connecting America: The National Broadband Plan* (2010) at 249, online at <https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf>.
[20] Kuh, *supra* note 21 at 1589.
[21] Stephanie M Stern, "Smart-Grid: Technology and the Psychology of Environmental Behavior Change" (2011) 86 *Chicago-Kent Law Review* 139 at 146.
[22] The term "Big Data" refers to the "management of large amounts of data and the use of tools and processes that enable the discovery of patterns that allow predictive models to emerge." James D Ford, *et al.* "Big Data has Big Potential for Applications to Climate Change Adaptation" (2016) 113:39 *NNAS* 10729.

government, utilities, third party service providers, researchers, law enforcement and the consumer. The value to mine these data is different for each of the stakeholders: reaching from the development of new electric devices for energy saving, marketing and business purposes, to collecting evidence for suspected illegal activities.

Russel Frisby Jr and Jonathan Trotta point out that "insufficient thought has been given to questions of controlling access to this information-and if so, how to do so-because much of this information was either never accessible or simply did not exist."[23] They also emphasise that the long-term success of smart grids require on the one hand that policymakers and regulators understand and recognise consumers' expectations of privacy, security and control over their energy consumption data. On the other hand, smart grid technology's success depends on its "ability to encourage and accommodate innovation while making usage data available to consumers and certain third party service providers in a responsible manner, and respecting individual consumer choices in how to balance the benefits of access to usage data against the protection of personal privacy and security."[24]

The mining and assessment of energy consumption data is needed to improve programs offering energy efficiency incentives and educating residential, commercial, and industrial customers about cost-effective energy saving opportunities.[25] Granular data from smart meters can assist in effective consumer empowerment and develop informed consumer decisions when to reduce energy use.[26] Government, regulators and cities are able to quantify

---

[23] H Russell Frisby & Jonathan P Trotta, "The Smart Grid: The Complexities and Importance of Data Privacy and Security" (2010-2011) 19 *CommLaw Conspectus* 297 at 299.
[24] US Department of Energy, Data Access and Privacy Issues related to Smart Grid Technologies (2010) at 2, online at <http://www.gc.energy.gov/documents/BroadbandReportDataPrivacy_ 0_5.pdf> [Data Access & Privacy Issues].
Frisby & Trotta, *supra* note 21 at 319, 329; Kuh, *supra* note 21 at 1597.
[25] Alexandra B Klass & Elizabeth J Wilson, "Energy Consumption Data: The Key to Improved Energy Efficiency" (2014-2015) 6 San Diego J Climate & Energy L 69 at 71.
[26] Elias L Quinn & Adam L Reed, "Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act (2010) 81 U Colo R Rev 833 at 870-871.

greenhouse gas emissions, assess their own policies and programs, and check whether they meet specific and self-imposed energy efficiency targets.[27]

As the internet of things, smart metering and smart grids evolve it is likely to be accompanied by increased scrutiny in terms of our privacy rights, as set out in the *Charter* or contemplated in other codification of these rights, both federally and provincially.

Canadian Privacy Legislation

The treatment of privacy at the federal level is grounded both in statute and the Canadian *Constitution*.[28] As such, where the state (be it federal, provincial or territorial, or municipal) gathers and monitors information, there must be consideration given to the privacy of citizens.

The Canadian *Charter* guarantees a reasonable expectation to privacy for its citizens. There is also a substantive base for privacy protection of data in other federal legislation such as the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), the latter of which focuses on private entities (and is summarized in Appendix A). Several themes arise as part of the federal privacy regulatory structure, that, as we will see, are also integrated into provincial law.

First, a basic starting point for protecting privacy is to require consent for the gathering, use and disclosure of information. Exceptions to this general premise are numerous and clearly enable government action in managing private information. Each exception to the general rule

[27] Klass & Wilson, *supra* note 23 at 73. Quinn & Reed, *ibid* at 870-71; Stern, *supra* note 19 at 146-47. Individuals can use smart technology to track the energy use of particular appliances and preprogram appliances to run (or not run) at certain times depending upon electricity prices.
[28] *Constitution Act, 1867 (UK), 30 & 31 Vict., c. 3 (U.K.),* reprinted in RSC 1985, App. II, No. 5.

of consent requires circumstance specific evaluations of the facts to determine their application.

While government is often authorized by statute to gather, use and disclose information, the use of the information is typically limited to purposes for which it was gathered. In this way there is an attempt to balance the use of personal information by ensuring government discretion to use the information is restricted to its intended use.

1) Canadian *Charter of Rights and Freedoms*

The "right" to privacy is protected by sections 7 and 8 of the Canadian *Charter of Rights and Freedoms*. More accurately, the *Charter* provides legal persons with a "reasonable expectation of privacy". Section 7 concerns the right to life, liberty and security of the person and deals with aspects of privacy in the context of self-incrimination. Section 8 concerns the right from unreasonable search and seizure.[29]

Privacy and search and seizure

The legal test applied for privacy analysis by the courts under section 8 of the *Charter* is conducted in two primary parts, one subjective and one objective. First the court will look to determine whether the party had a "subjective expectation of privacy" and this is followed by a review of whether that expectation was "objectively reasonable".[30] If a violation of a charter right is found, it may be upheld through a section 1 *Charter* analysis to determine if the infringement of the right is justified. For privacy cases related to criminal infractions a section

[29] *Hunter v Southam* [1984] 2 SCR 145; *R v Dymet*, [1988] 2 SCR 417; Ritu Khullar & Vanessa Cosco, "Conceptualizing the Right to Privacy", paper prepared for the Canadian Bar Association, National Administrative Law, Labour and Employment Law, and Privacy and Access Law PD Conference, Ottawa Ontario, November 26-27, 2010.
[30] See *R v Patrick*, [2009] 1 SCR 579, 2009 SCC 17 (CanLII), <http://canlii.ca/t/231wj>.

1 analysis is typically curtailed, as activities that infringe on the section 8 rights are not justified (such as warrantless searches which cannot be justified in light of the ability to obtain a warrant). [31] A fulsome review and analysis of whether a privacy infringement may be saved under section 1 of the Charter in the climate change regulation context is beyond the scope of this paper but is certainly worthy of further consideration.[32]

The Supreme Court of Canada has applied a broad definition to grant a general right against unreasonable search and seizure beyond the protection of property under section 8 of the *Charter*. The Court has consistently found that the purpose of section 8 is to "protect against intrusion of the state on an individual's privacy".[33] The Court has also found that "surreptitious electronic surveillance of an individual by an agency of the state constitutes unreasonable search and seizure" under this section.[34]

It is important to note that all the cases cited below relate to electronic surveillance or information that was gathered or disclosed for the purpose of a criminal prosecution. Section 8 analysis is not solely concerned with whether or not information was gathered but also the "*purpose for which it is made available*".[35] Insofar as the information collected to track energy consumption may be used for criminal or quasi-criminal (i.e. regulatory) prosecutions these cases remain relevant.[36]

However, it is apparent upon review of existing case law that section 8 rights and energy consumption data in a regulatory context is substantively distinguishable from the use of

---

[31] See *R. v. Duarte*, [1990] 1 SCR 30, 1990 CanLII 150 (SCC), http://canlii.ca/t/1fszz.
[32] A section 1 charter analysis requires several hurdles being overcome, including 1: a pressing and a substantial objective, 2 a rational connection between the impugned legislation and the objective, and 3 minimal impairment of a *Charter* right. See *Re B.C. Motor Vehicle Act*, [1985] 2 SCR 486, 1985 CanLII 81 (SCC), http://canlii.ca/t/dln
[33] *R v Plant* [1993] 3 SCR 281; *R v Duarte* [1990] 1 SCR 30.
[34] *R v Duarte, ibid.*
[35] *R v Gomboc,* [2010] 3 SCR 211 at para 27.
[36] This has been considered by the courts in a variety of taxation cases but otherwise jurisprudence of the "right to privacy" in the regulatory framing remains sparse. See *Kligman v M.N.R.*, [2003] 3 FCR 569, 2003 FCT 52 (CanLII), <http://canlii.ca/t/hxq>, retrieved on 2017-12-14 adopting *R v Jarvis,* [2002] 3 SCR 757, 2002 SCC 73 (CanLII), http://canlii.ca/t/50d7 , retrieved on 2017-12-14.

information by the state with the potential for penal consequences. Further, the remedy that a court would grant in a regulatory context would substantively differ from an exclusion of evidence in a criminal or quasi-criminal prosecution. Section 24 of the *Charter* indicates a court may grant a remedy "as the court considers appropriate and just in the circumstances" in instances of a rights infringement. Monitoring and disclosure of personal information for regulatory purposes may be deemed unconstitutional but it would likely need to be at the extreme end of information gathering. The remedies would likely be limited to declaratory relief or possibly a monetary award (although the quantification of compensable harm would be a challenge). A detailed review and analysis of what remedies might appropriately be granted in instances where there is a privacy infringement with non-penal consequences is beyond the scope of this report.

The "right to privacy" and the use of energy related information for criminal prosecutions

Energy use tells a story. That story may include criminal activities and energy stories may often be private in nature.

The case of *R v Tessling*[37] involved the use of an overhead Forward Looking Infra-Red (FLIR) technology by police to take pictures of a suspected marijuana grow-operation to pick up heat signatures from the house. It was found that this was a 'passive' technology because it did not show what was inside the home - just gleaned information about what was transpiring inside. The Court found that there was no violation of section 8 because the information that was gathered did not touch the "biographical core" of the respondent's personal information. This biographical core is found to be information which individuals in a free and democratic society

[37] *R v Tessling*, [2004] 3 SCR 432.

would wish to maintain and control from dissemination to the state, i.e. information which could reveal intimate details of the lifestyle and personal choices of the individual.

In *R v Plant* the court dealt with police using a terminal from electrical utility's computer to check the electrical consumption of a specific address.[38] This was done under the suspicion that said address was a marijuana grow-operation. The Supreme Court found that the police check of computerized records was not unreasonable but "in view of the nature of the information, the relationship between the accused and the electrical utility, the place and manner of the search and the seriousness of the offence under investigation, it cannot be concluded that the accused held a reasonable expectation of privacy…outweighed the state interest in enforcing the laws".[39]

The Court also found that the electricity records did not reveal intimate details of the accused's life, stating: "The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence."[40] The opinion of McLachlin, although concurring, found that the records are indeed capable of telling much about an individual's personal lifestyle and what is happening within a private dwelling.[41]

Finally the Supreme Court of Canada in the 2010 case of *R v Gomboc* considered surveillance of usage of electricity and section 8 privacy concerns. [42] In this case the police in Alberta approached the utility provider and requested the installation of a digital recording ammeter (DRA) in order to record the electricity usage. The case concerned whether Mr. Gomboc had a reasonable expectation of privacy in information about the pattern of use of electricity disclosed by the DRA. Justice Deschamps, writing for Charron, Rothstein, and Cromwell JJ,

---

[38] *R v Plant*, *supra* note 29.
[39] *R v Plant*, *ibid.*
[40] *Ibid.*
[41] *Ibid.*
[42] *R v Gomboc, supra* note 31.

found that there was no reasonable expectation of privacy regarding this information and therefore section 8 was not engaged. Justice Deschamps reasoning was based on the totality of the circumstances – the nature and quality of the information, the remoteness from the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state", and the legislative scheme permitting disclosure of customer information to authorities investigating an offence.[43]

The Court questioned the invasiveness of the information that was being received, specifically whether that information could provide answers to the following questions: how many occupants live in the residence; whether any occupants are home at a particular time; whether anyone is watching television; whether anyone is using a computer; whether anyone is listening to a stereo; whether anyone is taking a bath, sitting in a hot tub, or showering; whether anyone is cooking or washing dishes; the gender of the occupants; the political affiliation of the occupants; the sexual orientation of the occupants; where electricity is being used in the house; whether any electrical devices are on a timer. In finding the answer to each of these questions as "no" Deschamps J was satisfied that there was "no room for speculation" as to the possibility of data disclosing personal information.[44]

The fact that the Alberta *Code of Conduct Regulation*[45] pursuant to the *Electric Utilities Act*[46] allowed "disclosure to a peace officer for the purpose of investigating an offence if the disclosure is not contrary to the express request of the customer" was central to the finding that there was no objective expectation of privacy considering the totality of the circumstances.

---

[43] *Ibid*. at para 2.
[44] I*bid* at para 7.
[45] *Code of Conduct Regulation,* Alberta Regulation 58/2015.
[46] *Electric Utilities Act,* RSA 2003, c E-5.1.

The Court specifically addressed the looming issue of smart meters stating that as technology improves and the nature and quality of information changes the case will be different and those cases should be dealt with at that time.[47]

Abella J, writing for Binnie, and LeBel, provided the concurring opinion finding that the legislative scheme eroded the expectation of privacy in this instance. Furthermore, Abella J noted that the regulation in this instance was not brought up on a Charter challenge to its constitutionality. Abella J found that since the DRA provides a strong inference of the presence of a marijuana grow operation, this information is covered by a reasonable expectation of privacy due to it being information about an activity *inside the home*.[48] Thus, classifying the information as personal information. But for the *Regulation*, Abella J would have found that section 8 was sufficiently engaged and violated. The court noted:[49]

> The contractual terms the statutory scheme creates are not only clear and unambiguous; they are also clearly relevant to an objective assessment of the reasonableness of any expectations of privacy Mr. Gomboc may have had in the DRA information, regardless of whether he decided to inform himself of the legal parameters of his relationship with his utility provider.

McLachlin CJ and Fish J, in the dissenting opinion, found that a reasonable person would not have concluded that their expectation of privacy in activities inside the home was negated because of the *Regulation*. In relation to how the regulation may determine an assessment of whether the invasion of privacy was "objectively reasonable", the justices noted:

> The average consumer signing up for electricity cannot be expected to be aware of the details of a complex regulatory scheme — the vast majority of which applies to the companies providing services, and not to the

[47] *R v Gomboc*, *supra* note 33 at para 40.
[48] *R v Gomboc*, *ibid* at para 80.
[49] *R v Gomboc*, *ibid* at para 94.

> consumers themselves — which permits the utility company to pass information on electricity usage to the police, especially when a presumption of awareness operates to, in effect, narrow the consumer's constitutional rights. (at 139)

More recently, the Ontario Court of Appeal in *R. v. Orlandis-Habsburgo*, reviewed *Gomboc* in a case where energy consumption data was provided by a utility to the police.[50] In applying *Gomboc*, the court found that energy consumption data did reveal private information sufficiently to engage a s.8 analysis and distinguished the case based on the lack of regulation that dealt with disclosure of information in Ontario. An expectation of privacy may be undermined where a utility pursues discretionary data disclosure to police. However, the Court concluded that the information was nevertheless admissible as the police were reasonable in using the information as it did not relate to "core biographical information or information that reveals intimate and personal details of a person's lifestyle" and that "society's interest in an adjudication of the case on the merits – does not favour exclusion".[51] The Court also noted, in *obiter*, that:[52]

> the value-laden nature of the expectation of privacy inquiry explains why the purpose of the state intrusion is important in assessing whether that intrusion violates a reasonable expectation of privacy. The community may accept certain state intrusions for certain purposes. For example, unfettered state access to business-related documents in a regulatory context may be seen as entirely consistent with community notions of personal privacy. However, the same state access to the same documents, but for a criminal law purpose may be regarded as an unacceptable state intrusion into personal privacy.

---

[50] *R. v. Orlandis-Habsburgo*, 2017 ONCA 649
[51] *Ibid* at para 134.
[52] *Ibid* at para 46.

The approach taken by the Court of Appeal illustrates the need for clear language in regulations where the privacy of information is at issue.

Privacy and liberty

A reasonable expectation of privacy also arises in the context of section 7 of the Charter which states that everyone "has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice". Privacy rights are found in both s.7 guarantees: security of person and liberty.[53] Courts have framed the infringement of one's liberty under s.7 in instances where the "dignity and self-worth" of an individual may be impacted.[54] The right to the security of the person protects "the physical and psychological integrity of the individual".[55]

A reasonable expectation of privacy under s.7 has arisen in the context of disclosure of private personal records of witnesses and in relation to legislative disclosure of private adoption information.[56] Central to these decisions (and suggested "principle of justice" under s.7) is that "where an individual has a reasonable expectation of privacy in personal and confidential information" it should only be disclosed with the consent of the individual.[57] What is "reasonable" in a given instance mimics the section 8 analysis.[58]

---

[53] See *R.v. O'Connor* [1995] 4 S.C.R. 411, at para 82&83
[54] See *Cheskes v. Ontario (Attorney General),* 2007 CanLII 38387 (ON SC), http://canlii.ca/t/1sxx8 at para 82 citing O'Connor.
[55] *Ibid* at para 93.
[56] See O'Connor, supra note 53 and *Cheskes v. Ontario (Attorney General),* 2007 CanLII 38387 (ON SC), http://canlii.ca/t/1sxx8 and *Infant Number 10968 v. Her Majesty the Queen in right of Ontario*, 2007 ONCA 787 (CanLII), http://canlii.ca/t/1tpqf respectively.
[57] *Ibid*.
[58] *Ibid*.

Charter and energy consumption data in the regulatory context

The *Charter* restriction on state power to gather and use electronic and energy information is primarily applied in the criminal law context. In a quasi-criminal or regulatory enforcement context section 8 may still arise, as illustrated by several tax related cases.[59] Similarly, regulatory orders to compel testimony under oath and production of documents in the context of securities and competition regulation may come under section 8 scrutiny.[60] The judicial consideration of a "right to privacy" in the broader regulatory framing remains sparse. In the environmental and climate change context judicial consideration of a reasonable expectation of privacy has not yet been dealt with.

Where one steps away from the use of information for a state imposed sanction (either criminally or quasi-criminally) the likelihood of a section 8 Charter violation appears to be greatly diminished. The case law would suggest that monitoring and use of energy consumption data, if it is gathered and authorized in compliance with our laws, would need to be highly detailed to justify court intervention for violating a *Charter* right.

In *British Columbia Securities Commission v. Branch* it was observed:[61]

---

[59] These cases often involve the requirement to disclosure documents for audit purposes that are subsequently used for prosecution purposes. Section 7 and 8 arguments are used to challenge their admissibility on the grounds of rights against self-incrimination and a reasonable expectation of privacy. *R. v. McKinlay Transport Ltd., [1990] 1 SCR 627, 1990 CanLII 137 (SCC),* http://canlii.ca/t/1fszd and *R. v. Derose*, 2000 ABPC 192 (CanLII), http://canlii.ca/t/5qwm. It should be noted that this was found not to extend to disclosure of lawyer's accounting record (see Canada (National Revenue) v. Thompson, [2016] 1 SCR 381, 2016 SCC 21 (CanLII), http://canlii.ca/t/grxb3 and Canada (Attorney General) v. Chambre des notaires du Québec, [2016] 1 SCR 336, 2016 SCC 20 (CanLII), http://canlii.ca/t/grxb1 *Thompson v. Canada (National Revenue)*, 2013 FCA 197 (CanLII), http://canlii.ca/t/gobjz.

[60] See *Thomson Newspapers Ltd. v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission),* 1990 CanLII 135 (SCC), [1990] 1 SCR 425; *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3, 1995 CanLII 142 (SCC) respectively. Section 8 has also arisen in relation to the financial review involved for security clearances conducted for correctional officers (*Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) v. Canada (Attorney General)*, 2016 FC 1289 (CanLII), http://canlii.ca/t/h4rfx).

[61] *British Columbia Securities Commission v. Branch*, 1995 CanLII 142 (SCC), [1995] 2 S.C.R. 3 para. 52

> [t]he greater the departure from the realm of criminal law, the more flexible will be the approach to the standard of reasonableness. The application of a less strenuous approach to regulatory or administrative searches and seizures is consistent with a purposive approach to the elaboration of s. 8.

The Alberta Court of Appeal has also noted that "regulated individuals are on notice of the regulator's potential investigatory (and intrusive) power…and cannot reasonably expect the same level of privacy towards the state as they might outside the regulatory context".[62]

As technology and the "internet of things" expands, the nature and detail of personal information is more likely to reveal details about activities "inside the home" and send out a detailed story of a person's energy consumption day.

Considering the context of individual energy consumption, while having touch points in regulation, the awareness of the regulatory system may not be so clear cut (as cited in the dissent in *Gomboc*, *supra*). The evaluation of whether energy consumption information reveal the "biographical core of personal information" may be reframed as whether the energy consumption data generates a personal narrative of your energy consumption day. As technology and the "internet of things" expands, the nature and detail of personal information is more likely to reveal details about activities "inside the home" and send out a detailed story of a person's energy consumption day.

The question that then arises is whether that information, if publicly disclosed, results in a deleterious effect that outweighs the social benefit. Certainly, some disclosure of fine details

[62] These observations were in the context of a request for records of a lawyer's electronic devices in the context of a disciplinary investigation in *Law Society of Alberta v Sidhu*, 2017 ABCA 224 (CanLII), <http://canlii.ca/t/h4mcw>.

of an energy story may be viewed as deleterious if they result in psychological stress. Underlying this discussion is whether naming and shaming is a valid policy approach to pollution and carbon emission abatement.

As such, the gathering and use of the information will likely face increased scrutiny. In the sphere of public authorities exercising regulatory roles it appears that the statutory requirements for gathering, use and disclosure of this information will provide, at least in part, a normative base line for what will or will not infringe the "reasonable" expectation of privacy.

2) Federal *Privacy Act*

The *Privacy Act* focuses on protecting personal information of individuals held by government institutions and providing individuals with a right of access to that information.[63] The Act applies to the federal government, its bodies or offices, any agents of a Crown corporation and any wholly-owned subsidiary of such as a corporation.[64] Personal information is broadly defined as information about an identifiable individual that is recorded in any form. The definition also lists specific types of information that will be considered personal but this listing doesn't detract from the general starting premise of "information about an identifiable individual". The definition includes some aspects where the use and disclosure of energy consumption data may arise:[65]

> (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

[63] *Privacy Act*, RSC 1985, c P-21 at s 2.
[64] *Privacy Act*, s 3.
[65] *Privacy Act*, at s 3.

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

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

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

...

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

Further, personal information shall not be collected by a government institution unless it relates directly to an operating program or activity of the institution.[66] The individual is to be informed of the purpose of the collection of this information.[67] Personal information shall not be used by the institution without the consent of the individual except for the purpose for which it was obtained, or for a purpose that the information may be disclosed to the institution under subsection 8(2) of the *Privacy Act*.[68] Section 8(2) of the *Privacy Act* outlines a variety of situations where personal information under government control may be disclosed including but not limited to – the purpose it was obtained, purposes in accordance with an Act of Parliament or regulations made thereunder, and to any person or body for research or statistical purposes if the head of the government is satisfied by certain criteria. The

[66] *Privacy Act*, s 4.
[67] *Privacy Act*, s 5(2).
[68] *Privacy Act*, s 7.

government can further refuse to disclose the information for a variety of reasons including instances involving law enforcement and investigation.[69]

See also the *Personal Information Protection Act* at Appendix A.

[69] *Privacy Act*, s 22.

Alberta Privacy Legislation

Alberta privacy legislation that may impact the protection, disclosure and use of energy consumption data includes the *Freedom of Information and Protection of Privacy Act* (FOIP), and the *Personal Information Protection Act* (PIPA) the latter of which focuses on private entities (and is summarized in Appendix A). [70] Further, utilities governed by the *Electric Utilities Act* and the *Gas Utilities Act* have specific rights and obligations around privacy under the *Code of Conduct Regulation.*[71]

Freedom of Information and Protection of Privacy Act (FOIP)

The FOIP deals mainly with obtaining access to information and protection of privacy.[72] The FOIP's privacy protection objectives are to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information; to control the disclosure by a public body of that information; and to allow individuals a right of access to personal information about themselves that is held by a public body.[73]

Personal information is defined as recorded information about an identifiable individual, including the individual's name, race, age, sex, an identifying number, fingerprints, information

[70] *Freedom of Information and Protection of Privacy Act,* RSA 2000, c F-25 [FOIP] and *Personal Information Protection Act,* SA 2003, c P-6.5 [PIPA].
[71] *Electric Utilities Act, supra* note 42; *Gas Utilities Act* RSA 2000, c- G-5; *Code of Conduct Regulation, supra* note 41.
[72] For the purpose of this paper we are focusing on the protection of privacy section. For access to information under FOIP see Astrid Kalkbrenner, ELC, *Environmental Rights Alberta: A Right to a Healthy Environment – Module 4: Access to Environmental Information* (Edmonton: ELC, 2017) online at <http://elc.ab.ca/wp-content/uploads/2017/07/EBR-Module-4-Access-of-Environmental-Information-July-19-2017.pdf>.
[73] FOIP, s 2.

about the individual's health, education and so forth.[74] Personal information may not be collected by or for a public body unless:

- the collection of that information is expressly authorized by an enactment of Alberta or Canada,
- that information is collected for the purposes of law enforcement, or
- that information relates directly to and is necessary for an operating program or activity of the public body.[75]

If the public body is authorized to collect personal information it must collect such information directly from the individual (with some specific exceptions).[76] Further, the public body must inform the individual about the purpose for which the information is collected, the specific legal authority for the collection, and the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.[77]

Generally, the head of a public body must protect personal information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or destruction.[78]

A public body may **use** personal information in the following instances: [79]

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

[74] FOIP, s 1(n).
[75] FOIP, s 33.
[76] FOIP, s 34(1). Exceptions to the manner of collection are for example if another method is authorized by the individual or an Act, regulation etc., or there is an emergency situation.
[77] FOIP, s 34(2).
[78] FOIP, s 38.
[79] FOIP, s 39(1).

- if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
- for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.

Also, a public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.[80]

Section 40 of FOIP enumerates several instances where a public body may **disclose** personal information, including:

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose;
- if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure; for the purpose of complying with an enactment of Alberta or Canada;
- for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure; or
- for the purpose of complying with a subpoena, warrant or order issued or made by a court.[81]

Furthermore, a public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes in a reasonable manner.[82]

[80] FOIP, s 39(4).
[81] FOIP, s 40(1).
[82] FOIP, s 40(4).

Determination of what disclosure will be viewed as "consistent with the purpose for which the information was collected or compiled" is guided by whether the use of the information "has a reasonable and direct connection to that purpose **and** is necessary for performing the statutory duties of, or for operating a legally authorized program".[83] In other words, the disclosure must be relevant to a specific public body's purpose for the collection and necessary to undertaking a statutory duty or for operating a program. Flexibility to use data for multiple purposes is thereby curtailed.

Where consent for the use and disclosure of information is required the process set out in the FOIP *Regulation* applies.[84] Consent for the use and disclosure of personal information must meet specific requirements and must specify to whom the personal information may be disclosed and how the personal information may be used.[85]

Code of Conduct Regulation under the *Electric Utilities Act* and *Gas Utilities Act*

The *Code of Conduct Regulation* outlines when a distributor, regulated rate supplier, retailer, officer, employee, contractor, or agent thereof can disclose customer information.[86] Disclosure can be made if the customer has consented to the disclosure, the disclosure is permitted within the regulation, or the disclosure is otherwise authorized under the FOIP or the PIPA.[87] The consent must be in writing, electronic, or recorded, and the information must be itemized in consent.[88] The *Regulation* also outlines in what circumstances customer

[83] FOIP, s 41.
[84] *Freedom of Information and Protection of Privacy Regulation*, Alta Reg 186/2008 s 7 [FOIP *Regulation*].
[85] FOIP Regulation, s 7(2). A written consent is only valid if the consenting person signed the consent. FOIP *Regulation*, s 7(4). For electronic consents see s 7(5) and oral consents s 7(6).
[86] The *Code of Conduct Regulation*, s 1(e), defines customer information as information about a customer that is uniquely associated with the customer; could be used to identify the customer, or is provided by the customer to a distributor, a regulated rate supplier or a retailer. *Code of Conduct Regulation*, s1 (e).
[87] *Code of Conduct Regulation,* s 10(1).
[88] *Code of Conduct Regulation,* s 10(2).

information can be disclosed without their consent, these include: to give to a customer retailer or regulated rate supplier, if required by law or by order of government agency, etc.[89]

A retailer may request in writing or electronic form the disclosure of a customer's historical electricity usage information from a distributor or regulated rate supplier for the previous 12 month period. However, the retailer must obtain prior consent from the customer before issuing the request.[90]

As a general rule, a distributor or regulated rate supplier shall not make aggregated information about its customers available to a retailer.[91] However, there are exceptions to this rule and conditions under which it is allowed to make available aggregated customer information.

Section 13 of the *Regulation* states that a distributor or regulated rate supplier shall: [92]

> (a) ...ensure that the information that is made available has been aggregated to a degree that the information of any particular customer or retailer cannot be readily identified,
>
> (b) ...place on its website a notice containing a clear description of the aggregated information and the price for obtaining the aggregated information at least 24 hours before the aggregated information is made available to a retailer, and shall keep the notice on its website for at least 30 days after the aggregated information is made available,
>
> (c) ...make the aggregated information available to all retailers for the same price and under the same terms and conditions, and

[89] *Code of Conduct Regulation*, s 10(3).
[90] *Code of Conduct Regulation*, s 12.
[91] *Code of Conduct Regulation*, s 13(1).
[92] *Code of Conduct Regulation*, s 13(2).

(d) … not charge more for the aggregated information than the costs incurred by the distributor or regulated rate supplier in aggregating the customer information and making it available.

The Regulations also stipulate the relationships among distributors, regulated rate suppliers and affiliated providers to prevent unfair competitive advantage. A distributor and an affiliated provider of the distributor, and likewise a regulated rate supplier and an affiliated provider of the regulated rate supplier are not allowed to make arrangements that create an unfair competitive advantage for the affiliated provider or for the regulated rate supplier, respectively.[93] In this way, an arrangement under which a distributor or regulated rate supplier shares information with an affiliated provider is deemed to create a competitive advantage for the affiliated provider, unless certain conditions are met to prevent the information being used for marketing or sales purposes.[94]

Energy consumption data disclosure of large emitters

Energy consumption information is found in a variety of areas and managed by various private utilities and public authorities. Disclosure to the public is limited. Power and natural gas consumption is tracked and administered by utilities and regulated (as set out above).

Large greenhouse gas emitters are required to report emissions under the *Climate Change and Emissions Management Act* [CCEMA].[95] Only those emitters that are specified by regulation

[93] *Code of Conduct Regulation,* s 17.
[94] *Code of Conduct Regulation,* ss 18(1)-(3). See also ss 10, 11, 12, 13, 29 and 30. Without any exceptions a retailer that seeks or receives customer information from a current or former officer, employee, agent or contractor of a distributor or regulated rate supplier for sales or marketing purposes seeks or obtains an unfair competitive advantage.
[95] *Climate Change and Emissions Management Act,* SA 2003, c C-16.7 [CCEMA].

must report in accordance with the Specified Gas Reporting Standard.[96] At the time of publication (December 2017) this reporting standard was under review and sets out a decrease in the reporting threshold from 50,000 to 10,000 tonnes CO_{2e} per annum.[97] Further disclosure of this information by the Minister is governed by regulations.[98] Specifically, one can seek the reports from the emitter, and if the report was not provided within 30 days, from the Director.[99] Emitters may seek to have the reports or parts of the reports kept confidential for up to 5 years.[100]

As part of the Government of Alberta's *Climate Leadership Act* emissions are assessed and reported by emitters covered by the Act by virtue of their remittance of the carbon levy.[101] The Act provides for the gathering of information about remitters of the carbon levy and requires registration with the government.[102] Information under the Act can only be disclosed in limited circumstances, including (but not limited to):[103]

- Provincial, federal or territorial governments if used "solely for the purposes of administering or enforcing a taxation statute" or where there is a mutual sharing agreement among other Canadian governments;
- to the government for the purpose of enforcement of the Act or regulations;

---

[96] Government of Alberta, *Specified Gas Reporting Standard*, Draft Version 9.0- 2017 Emissions Reporting, (Edmonton: Government of Alberta, December 2017), online: Alberta Environment and Parks, online: <http://aep.alberta.ca/climate-change/guidelines-legislation/specified-gas-reporting-regulation/documents/ReportingStandard-DRAFT-Dec2017.pdf>.
[97] The revised standard has a variety of additional reporting details, much of it focused on aligning with federal requirements. *Ibid.*
[98] See CCEMA, s 6.
[99] See *Specified Gas Reporting Regulation*, Alta Reg, 251/2004, s 6.
[100] *Specified Gas Reporting Regulation,* s 4. The basis for agreeing to keep information confidential is based the Director's determination of whether the information in the report is "commercial, financial, scientific or technical information that would reveal proprietary business, competitive or trade secret information about a specific facility, technology or corporate initiative".
[101] See *Climate Leadership Act,* S. A. 2016, c C-16.9.
[102] *Ibid at* ss. 25 and 27.
[103] *Ibid* at s. 69.

- where the recipient of information requires it for the purposes of compliance or to determine if a registrant is complying with the Act.

- where the Minister discloses information gathered under the Act in accordance with the Regulations;

- to other government employees for the purposes of assessing tax, carbon levy and fiscal policy.

The *Climate Leadership Regulation* sets out the circumstances where disclosure of registrant information is allowed.[104] Specifically the Minster may disclose certain information:

- to allow a registrant to determine whether another registrant who holds a carbon levy exemption certificate or licence, and whether there have been suspensions or cancellations of exemption certificates (for the purpose of determining compliance);[105]

- to government of Alberta agents or employees any information required for an "inspection, investigation audit or examination" under the Act and the Regulations; and

- information related to the effective date of a registration, the state of a registration and the operating name and business contact information of a registrant; and[106]

- "the Minister may publish or disclose to any person for any purpose readily available summarized or statistical information that cannot, directly or indirectly, be associated with or identify a particular individual or other person."[107]

[104] See *Climate Leadership Regulation,* Alta Reg 175/2016, s 42.
[105] *Ibid.*
[106] *Ibid* at s. 42(4).
[107] *Ibid* at s. 42(6).

Additional regulations are expected in 2018 which may have implications for data gathering and disclosure.

Ontario's approach to privacy and energy consumption

Ontario's privacy legislation is similar to that of Alberta. The central acts are the *Freedom of Information and Protection of Privacy Act (FIPPA)* [108] and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).*[109] *MFIPPA* and *FIPPA* state that institutions shall not use personal information except if the person has identified that information and consented to its use, for the purpose for which it was obtained or compiled or for consistent purpose, or for a purpose which may be disclosed to the institution under section 32 *MFIPPA* or section 42 *FIPPA*.[110] Disclosure of personal information is permitted in certain instances.[111]

Unlike Alberta, Ontario has expanded information systems related to energy consumption of buildings and smart metering. Section 7 of the *Green Energy Act* empowers the Ontario cabinet to require disclosure of energy consumption and other metrics of consumption from prescribed persons in prescribed circumstances.[112] The passage of the *Reporting of Energy Consumption and Water Use Regulation* in 2017 requires the reporting of energy consumption information to the Minister.[113] The properties that must report are prescribed by the regulation, with a focus on buildings in excess of 50,000 square feet.[114] Section 7 of the *Regulation* sets out what information is reportable, including the "gross floor area of the property" and "the information respecting the property, including identifying information and information respecting energy

[108] *Freedom of Information and Protection of Privacy Act*, RSO 1990, Chapter R 31 [FIPPA].
[109] *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, C M.56 [MFIPPA].
[110] MFIPPA, s 31; FIPPA s 41(1).
[111] MFIPPA, s 32; FIPPA, s 42(1).
[112] *Green Energy Act*, 2009, S O 2009, C 12.
[113] *Reporting of Energy Consumption and Water Use Regulation*, O Reg 20/17.
[114] *Ibid.* at ss. 3, 4.

consumption, water use, performance metrics in respect of energy consumption and water use in respect of the property, that is set out in the document titled "Ontario's Large Building Energy and Water Reporting and Benchmarking Requirement: Data Elements".[115] There are a variety of exemptions to the reporting requirements set out in the regulations.[116]

The information gathered under the regulation may be published by the Minster or shared with other Ministries or agencies of the Government of Ontario.[117] Where the Minister has not made the information available there is a presumption of confidentiality.[118] Further the *Green Energy Act* requires the Ontario Energy Board to provide information to those with the reporting duty under the *Regulation*, upon request.[119]

On the utility regulation side, the agency that deals with how information may be gathered and disclosed in Ontario is the Ontario Energy Board (OEB). The OEB, when issuing or amending licences may stipulate conditions relating to the protection of privacy.[120]

The OEB is obliged, in the process of the establishment, implementation and promotion of a smart grid to follow specific policy objectives of the government, among other things, privacy. The Order in Council 1515/2010 explains privacy as "[r]espect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments."[121]

For the administration and management of smart meters (and its data) the Ontario Independent Electricity System Operator (IESO) is designated as the Smart Metering Entity.[122] The Smart Metering Entity has the exclusive authority to receive smart metering data for

---

[115] *Ibid.* at s 7.
[116] *Ibid.* at ss 10, 11.
[117] *Green Energy Act,* s 7.2.
[118] *Green Energy Act,* s 7.2 (2).
[119] *Ibid.* at s 7.3.
[120] *Ontario Energy Board Act*, 1998 SO 1998, c 15 Sch B, s 28.3(2)5, 28.5(1).
[121] Ontario Energy Board, *Order in Council 1515/2010*, 23 November 2010 at 4.(vi).
[122] *Smart Metering Entity*, O Reg 393/07, s 1.

purposes of carrying out functions of providing services – specified by the Smart Metering Entity - performed on smart metering data to produce billing quantity data, and *manage access rights to smart metering data* and data derived from smart metering data.[123] The *Electricity Act* assigns the Smart Metering Entity's objectives which are among other things to

- collect and facilitate the collection and management of information and data and to store the information and data related to the metering of consumers' consumption of use of electricity in Ontario, including data collected from distributors and, if so authorized, to have the exclusive authority to collect, manage, and store the data,

- establish, to own or lease and to operate one or more databases to facilitate collecting, managing, storing and retrieving smart metering data, and

- to ***provide and promote non-discriminatory access, on appropriate terms and subject to any conditions in its license relating to the protection of privacy, by distributors, retailers, the IESO and other persons: to information and data relating to consumers' consumption or use of electricity*** and, to the telecommunication system that permits the Smart Metering Entity to transfer data about the consumption or use of electricity to and from its databases, including access to its telecommunication equipment.[124]

(Emphasis added)

The Smart Metering Entity may "directly or indirectly collects information and data relating to consumption or use of electricity from consumers, distributors, or any other person" and may

[123] *Ibid.* at *s 1.*
[124] *Electricity Act, 1998*, SO 1998, c 15, Sch A, s 53.8.

manage and aggregate the data.[125] Distributors, retailers and other persons shall provide the Smart Metering Entity with such information as it requires to fulfill its obligations.[126]

Access to data through the entity is an ongoing initiative, as reflected in the October 2017 draft *Smart Metering Entity: Third Party Access Implementation Plan* which was initiated following two orders from the OEB to develop a plan to facilitate third party access to "de-identified" data.[127]

A path forward to balance data needs and privacy

The governments of Canada and Alberta have taken initiative to forward a climate mitigation policy agenda. This includes both regulatory and voluntary approaches to reducing greenhouse gas emissions from the broad range of emitters, from large industrial emitters to individuals. Some Alberta municipalities have also initiated programs and policies to contribute to provincial and federal climate policy goals. The effectiveness of these regimes requires ongoing economy wide measurement and evaluation of energy consumption and emissions – a daunting data collection and management challenge.

Current laws in Alberta have yet to evolve to reflect these new policy challenges. Current disclosure and data gathering is focused on larger emitters and utilities are limited in the scope of sharing of data with policy developers and program implementers. To maintain a balanced approach to privacy in the energy consumption realm there is a need to see this evolve.

---

[125] *Ibid.* at s 53.14.
[126] *Ibid.* at s 53.15(1).
[127] Independent Electricity System Operator (IESO), "Smart Metering Entity: Third Party Access Implementation Plan" (October 12, 2017). See ongoing consultation process at IESO, online at <http://www.ieso.ca/en/sector-participants/engagement-initiatives/engagements/smart-metering-entity-third-party-access-implementation-plan>. See also the recent court case in Ontario Court of Appeal in *R. v. Orlandis-Habsburgo, supra* note 50.

Federal, Alberta and Ontario privacy legislation are similar in their approach. However, in comparing Alberta's and Ontario's privacy framework relating to energy consumption in large buildings and collection and management of smart metered energy consumption data it can be noted that Ontario has established tailored legislation that recognizes privacy rights as a major policy principle while recognizing the need to mandate disclosure of energy consumption. This is absent in Alberta's legislative framework.

With technological advancements and new technologies, such as smart meters, it is questionable whether knowledge and consent are sufficient tools to provide an appropriate level of privacy.

Another aspect that is worth mentioning is neither Alberta nor Ontario have addressed so far is the question of who actually owns the energy consumption data – the individual or the utility company? Flowing from that question is who owns the pollution arising from that energy consumption and is there, or should there be, a broader obligation to disclose such information.

So far, the most commonly used tools for privacy protection in legislation are requirements that a person whose personal information is being gathered has sufficient notice and knowledge of the data being gathered, used and disseminated and have consented to the activity. With technological advancements and new technologies, such as smart meters, it is questionable whether knowledge and consent are sufficient tools to provide an appropriate level of privacy.

There are authors questioning the real value of notice and consent about the collection, use or disclosure of personal information.[128] Knowledge, notice and consent are part of the concept

[128] Fred H Cate, "Protecting Privacy in Health Research: The Limits of Individual Choice" (2010) 98:6 California Law Review 1765; Kuh, *supra* note 2 at 1602.

of individual choice. This means, an individual should have the choice whether their personal information is collected, used and disclosed. The critique is that notices are often inaccessible because they are too complex.[129] Only a few people read notices and in most cases grant consent to the service or product they want or need.[130] Fred Cate stresses that: [131]

> Individual choice is not the same thing as privacy protection and merely providing choice does not necessarily enhance privacy protection. Choice - and notice to support choice - have tended to become a distraction from, or even a substitute for, more meaningful privacy protections. As a result, the energy of data processors, legislators, and enforcement authorities is often expended on notices and choice opportunities, rather than on enhancing privacy. Compliance with data protection laws is often focused on providing required notices in proper form at the right time and acting on choices, rather than on ensuring that personal information is protected.

It is suggested that, for consent to be meaningful, the procedures for obtaining it must be carefully designed, but even then some, privacy harms cannot be avoided.[132] Besides the basic tools of knowledge and consent applied in privacy legislation, special tools in particular for the generation of Big Data, should be considered by lawmakers and regulators.

One method to protect private data is anonymization. Data can be anonymized so that they cannot be associated with individual consumers.[133] Anonymization can be achieved through aggregation and de-identification, either separately or jointly.[134] Aggregation involves processing data in clusters to dilute individual-level records.[135] Aggregated data is less granular

---

[129] Kuh, *ibid* at 1771.
[130] Kuh, *ibid* at 1772.
[131] Kuh, i*bid* 1773, 1774.
[132] Kuh, *ibid* at 1602, 1603; Cate, *supra* note 113 at 1771-1778.
[133] Harvey, *supra* note 9 at 2080.
[134] Harvey, *ibid* at 2080.
[135] Harvey, *ibid* at 2080.

because it is data collected at community or regional level instead of at individual level.[136] The privacy concerns are less with this type of data provided that it was sufficiently aggregated. The drawback of this method is that the usefulness of the data could be reduced for third parties, in particular researchers.[137]

De-identification means the removal of

> personally identifying information, such as name, address, account number, and other billing information, from electricity records. Unlike aggregation, de-identification could make data available at the single-home level, although third parties would not be able to assign that profile to an actual customer or location. The result would be data that was not linkable to an individual but was still customer specific, and could therefore be analyzed at a granular and detailed level.[138]

However, the process of anonymizing of data may not sufficiently prevent re-identification and thus anonymization methods should be only a part of the solution to ensure data privacy.[139] Further, anonymization may be counter to specific goals of data collection in the first instance, i.e. driving behavioural changes by increasing transparency in energy consumption at a residential or individual level.

A further method to minimize privacy risks is the use of an energy data centre (EDC). An EDC functions like a repository or database, usually maintained by utility companies. The EDC provides access to energy data for third parties, the public and also policymakers. The energy

[136] Harvey, *ibid* at 2089.
[137] Harvey, *ibid* at 2080.
[138] *Ibid* at 2081.
[139] *Ibid.* at 2082.

data are anonymized. Some US States have established EDCs, such as New Jersey[140] and California.[141] In Canada, Ontario has installed an EDC.[142]

RECOMMENDATIONS

The information gathering and sharing powers for energy consumption data in Alberta's laws is in need of review and reform. Specifically, a statutory review should occur to ensure public authorities have the tools they need for policies to succeed while respecting the privacy of citizens. In this regard, the recommendations are mindful of the pressing nature and objectives of effective climate regulation and laws while also being mindful to avoid potential infringement of reasonable citizen expectations of privacy as set out in the *Charter*. Alberta laws should be amended to ensure:

1. Statutory powers to gather, use and disclose information on energy consumption exist for relevant public authorities (i.e., municipal, provincial, and federal).

2. Sufficient flexibility exists to allow sharing of energy consumption information among and within public authorities with clear limits on use and disclosure.

3. Clear disclosure rules exist for public authorities to access and use energy consumption data gathered by utilities. This data, once disclosed to public authorities, should be presumed to be confidential except where aggregated.

---

[140] State of New Jersey, "Energy Data Center", online at <http://pppolicy.rutgers.edu/ceeep/edc/>.
[141] California Public Utilities Commission, Decision (D.14-05-016) – Decision adopting rules to provide access to energy usage and usage-related data while protecting privacy of personal data May 1, 2014, online at <http://docs.cpuc.ca.gov/publisheddocs/published/g000/m090/k845/90845985.pdf>.
[142] Independent Electricity System Operator (IESO), "Smart Metering Entity", online at <http://www.ieso.ca/sector-participants/smart-metering-entity/governance-of-sme>.

4. Limit the use of energy consumption data for the purpose for which it is gathered or for the administrative, enforcement, and evaluation of climate relevant regulations, policies and programs.

5. Privacy legislation should be amended to clarify the types and nature of energy consumption data that is sufficiently "de-identified" or anonymized to enable and allow for public disclosure.

CONCLUSION

The internet of things and the continued growth of smart grids are bound to further result in the evolution of privacy considerations and climate mitigation policies, whether at the federal, provincial or municipal level. The collection of individual energy consumption data at multiple scales is essential to the efficacy of climate mitigation policies and programs. However, as society and technology march forward, the level of data and the details it reveals about individual habits and preferences will only elevate the importance of balancing privacy.

As society and technology march forward, the level of data and the details it reveals about individual habits and preferences will only elevate the importance of balancing privacy.

As technology such as smart grids becomes more widely adopted, legislators, regulators and courts must understand the implications associated with the new smart technologies and carefully assess the risks.[143] The valuable and necessary access to energy consumption data must be properly guided by regulators in order to ensure that the privacy of individual

[143] Harvey, *supra* note 9 at 2090.

consumption data is not infringed while at the same time making these data accessible for stakeholders such as third party service providers and researchers that have a true and proper interest in the data for the purpose of environmental innovations and improvement of energy efficiency.[144]

At the centre of the privacy versus disclosure of energy discussion are issues of social choice and public benefit. This discussion must weigh fostering programs and policies that ameliorate greenhouse gas emission rates and other pollutants versus the expectation that the state will not conduct unreasonable interventions and monitoring of personal and private activity.

[144] Frisby & Trotta, *supra* note 12 at 330.

Appendix A: Federal and Alberta Privacy laws focused on private entities

Federal *Personal Information Protection and Electronic Documents Act*

The PIPEDA is federal legislation which applies to "organizations" that collect, use or disclose personal information in the course of "commercial activities" or personal information about an employee (or applicant for employment) with an organization related to a "federal work, undertaking or business".[145] Every organization that collects, uses or discloses personal information in the course of commercial activities is covered by the scope of PIPEDA.[146]

A Cabinet Order may be issued that indicates that the Act does not apply due to a province's laws being substantially similar in relation to personal information that occurs within the province.[147] Such an order exists for Alberta in relation, exempting application of the Act in lieu of the provincial *Personal Information Protection Act*, except when dealing with a "federal work, undertaking or business".[148] In this regard, PIPEDA only applies in a limited capacity in Alberta.

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

[145] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [PIPEDA]. PIPEDA requires that any provincial legislation that is created must be substantially similar in order to displace PIPEDA.
[146] PIPEDA, s 4(1)(a). However, PIPEDA does not apply to any government institution to which the *Privacy Act* applies. PIPEDA, s 4(2)(a).
[147] PIPEDA, s 26(2).
[148] *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219.

circumstances."[149] The PIPEDA defines personal information as information about an identifiable individual.[150]

The collection, use or disclosure of personal information can only be for purposes that a reasonable person could consider appropriate in the circumstances.[151] The general rule is that there is a requirement that individuals are aware of and consent to the collection, use, or disclosure of personal information.[152] The consent is only valid if it is reasonable to expect an individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information they are consenting to.[153] There are various exceptions to this general rule.

Collection of personal information without an individual's knowledge or consent is allowed if it is clearly in the interests of the individual and consent cannot be obtained in a timely way. [154] Also, the collection is allowed when it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.[155]

---

[149] PIPEDA, s 3.
[150] PIPEDA, s 2(1).
[151] PIPEDA, s 5(3).
[152] PIPEDA, schedule 1 (section 5), Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, s 4.3. The explanatory note to s 4.3 of Schedule 1 sets out that in certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Organizations that do not have a direct relationship with the individual may not always be able to seek consent. An example would be a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.
[153] PIPEDA, s 6(1).
[154] PIPEDA, s 7(1)-(3).
[155] PIPEDA, s 7(1).

The Act sets out both a general rule and exceptions to both the use of personal information and the disclosure of personal information. An organization may use personal information for purposes other than those for which it was collected in certain prescribed circumstances, including if:[156]

> (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;
>
> (b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
>
> (b.1) the information is contained in a witness statement and the use is necessary to assess, process or settle an insurance claim;
>
> (b.2) the information was produced by the individual in the course of their employment, business or profession and the use is consistent with the purposes for which the information was produced;
>
> (c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;
>
> (c.1) it is publicly available and is specified by the regulations; or

[156] PIPEDA, ss 7(2) and 7(4).

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

Disclosure of personal information without knowledge and consent is allowed:

- for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information,
- it is impracticable to obtain consent, and
- the organization informs the Commissioner of the disclosure before the information is disclosed.[157]

Also, an organization may disclose personal information for purposes other than those for which it was collected.[158]

[157] PIPEDA, s 7(3)(f).
[158] PIPEDA, s 7(5).

Alberta's *Personal Information Protection Act* (PIPA)

The PIPA's objective is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.[159] Personal information is information about an identifiable individual.[160] An organization includes a corporation, an unincorporated association, a partnership and an individual acting in a commercial capacity.[161]

The PIPA applies to every organization and in respect of all personal information in Alberta.[162] The PIPA does not apply to a public body or any personal information that is in the custody of or under the control of a public body.[163]

The PIPA sets out that an organization is responsible for personal information that is in its custody or under its control, and that it must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.[164]

Further, an organization is not permitted to collect, use, or disclose personal information without the individual's consent.[165] While consent is a requirement for personal information to be obtained and used, it cannot be coerced by making consent a requirement to obtain that organization's services or products beyond what is necessary to provide said product or service.[166]

---

[159] PIPA, *supra* note 55 at s 3.
[160] PIPA, s 1(k); *Leon's Furniture Ltd v Alberta (Information & Privacy Commissioner)* 2011 ABCA 94.
[161] PIPA, s 1(i).
[162] PIPA, s 4(1).
[163] PIPA, s 4(2). In addition, the Act further stipulates a variety of exceptions to which the PIPA does not apply including: personal or domestic purposes of the individual, journalistic purposes, information in the custody of FOIP, or information in the custody of the legislature etc. PIPA, s 4(3).
[164] PIPA, ss 5(1), 6(1).
[165] PIPA, s 7(1). The consent can be in writing or oral, s 8(1).
[166] PIPA, s 7(2).

Despite the requirement to obtain consent, an organization may collect, use or disclose personal information for particular purposes if:

- the organization provides the individual with a notice, in a form that the individual can reasonably be expected to understand, and
- where the individual is given a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for the purposes prescribed in the notice.[167]

PIPA sets out that the purposes and the extent to which information is collected, used and disclosure is to be limited to the reasonable use for the specified purpose.[168] The PIPA itself determines the standard as to what is considered to be reasonable or unreasonable as "what a reasonable person would consider appropriate in the circumstances".[169]

Where individual consent is required, an organization must notify in writing or orally the individual before or at the time of collecting personal information about the purposes for which the information is collected. [170] The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection must also be made available.[171]

PIPA stipulates a variety of exceptions that do not require consent from the individual.[172] The collection, use and disclosure of personal information without consent depends on criteria such as:

[167] PIPA, s 8(3).
[168] PIPA, ss 11, 16, 19.
[169] PIPA, s 2.
[170] PIPA, s 13(1).
[171] PIPA, s 13(1).
[172] PIPA, ss 14-21.

- a reasonable person would consider that the collection, use or disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent,

- the collection, use or disclosure of the information is authorized or ***required by a statute or regulation of Alberta or of Canada or a bylaw of a local government body***,

- the collection or use of the information is from a public body and that public body is authorized or required by an enactment of Alberta or Canada to disclose the information to the organization,

- the ***disclosure of the information is to a public body and that public body is authorized or required by an enactment of Alberta or Canada to collect the information from the organization,***

- the disclosure of the information is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information, or

- the disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result.

(Emphasis added)

The PIPA obliges an organization to make a reasonable effort to ensure that any personal information collected, used or disclosed by or on behalf of an organization is accurate and complete to the extent that is reasonable for the organization's purposes in collecting, using or

disclosing the information.[173] In addition, an organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.[174]

[173] PIPA, s 33.
[174] PIPA, s 34.