CHAPTER 9

A Human Rights-Based Approach to Data Protection in Canada

Teresa Scassa

Abstract

The rapidly changing digital and data landscape has placed increasing pressure on Canada's existing data protection frameworks. Individual-oriented consent-based mechanisms no longer seem adequate or appropriate to address the challenges posed by the ubiquitous and continuous harvesting of massive amounts of data through the Internet of Things, and its use in big data analytics, artificial intelligence, and machine learning. This paper explores the potential for a shift in paradigm—to a human rights-based approach to data and privacy.

Canadian privacy law is at a crossroads. While data protection law stagnates, data collection continues to increase in volume and variety. New technologies are connecting our bodies, homes, vehicles, and even our cities, to the Internet of Things (IoT). There are ever fewer areas of human life untouched by rampant data collection. Not only is the collection of personal data ubiquitous and continuous, it is often of extraordinary detail and quality. In this sense, as noted in the Introduction to this book, individuals enact their citizenship in a digital context on a daily basis, and privacy is intrinsically intertwined with it.

In addition to dramatic changes in the scope and scale of data collection, the surging digital and data economy find new applications for data at an astounding rate. Big data analytics have developed into artificial intelligence (AI) and machine learning. These technologies rely on massive quantities of data, and many of the new applications are aimed at products or services customized for individuals or for "categories" of individuals. AI applications for government and private sector actors alike will profile, sort, categorize, and make decisions that both define and impact individuals and groups.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) of 2000, Canada's main private sector data protection law, was not built for the burgeoning data economy. The House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) held a number of hearings over the past two years that touch on privacy concerns, including hearings on the reform of PIPEDA (ETHI, 2018a), the applicability of privacy laws to political parties (Office of the Privacy Commissioner of Canada [OPC], 2018), the Facebook-Cambridge Analytica scandal (ETHI, 2018b, 2018c), and the Sidewalk Toronto's proposed smart city development (Vincent, 2019). Both the federal Smart Cities Challenge and the controversial Sidewalk Toronto proposal have sparked important debates about managing privacy in increasingly networked and technologically enabled public and private contexts (Canadian Press, 2018).

In May 2019, the federal government announced its *Digital Charter*, a political declaration articulating a set of principles for digital policy development. Among these principles, three touch on issues of importance to PIPEDA reform: control and consent; transparency, portability, and interoperability; and strong enforcement and real accountability. In addition, the government has released a discussion paper outlining some of the data protection reform issues it is considering (ISED, 2019).

Although there are signs that law reform is likely to occur at the federal level in Canada, it is not clear how extensive or transformative this reform will be. This chapter argues for a paradigm shift in Canadian data protection law—one that reframes privacy as a human right, rather than as a trade-off in the race to innovate or to carry out business in Canada.

The Need for PIPEDA Reform

There is no constitutional right to privacy in Canada beyond the Section 8 right in the *Canadian Charter of Rights and Freedoms* (1982) to be free from unreasonable search and seizure by government actors. In spite of this, courts have held that both the federal public sector *Privacy Act* (1985) and PIPEDA have quasi-constitutional status. This means that courts must interpret the rights protected by these laws generously (Curran, 2014). PIPEDA is a data protection law built around consent in consumer-business relationships. The law itself is premised upon a need to balance the privacy rights of individuals with the needs of businesses to collect, use, and disclose personal information (PIPEDA, 2000, s. 3). Although informed consent is, in many contexts, a means of preserving individual dignity and autonomy, in the contemporary data protection context it has become increasingly unmanageable as a basis for the collection, use, or disclosure of personal information. Individuals are overwhelmed by requests for consent, by lengthy and incomprehensible privacy policies, and by the reality of practical exclusion from digital services if consent is not granted (OPC, 2017). In addition, the speed and complexity of the data economy means that an organization's purposes for collection are often unclear and may shift over time. The implications or consequences of granting consent are not always evident, and these too may evolve.

The highly individualist orientation of the consent model is also no longer adequate to address all privacy concerns. Privacy rights are increasingly understood as having collective and not just individual dimensions. Titus Stahl notes that traditional conceptions of privacy focus on the collection of "specific information about specific individuals," whereas indiscriminate mass surveillance technologies affect almost everyone (2016, p. 33). Behavioural data collected from individuals can be used to profile individuals, groups, and communities. Alessandro Mantelero (2016) argues for a concept of "collective data protection" (p. 246), noting that "the most important concern in this context is the protection of groups from potential harm due to invasive and discriminatory data processing" (p. 249). He argues that collective privacy interests "have a supra-individual nature and a collective dimension, which are not adequately addressed by the existing data protection legal framework." An example of the collective dimension of privacy rights can also be seen in the Cambridge

Analytica scandal. There, although there was large-scale misuse of personal information, the most important harms were public ones: the manipulation of voters with a view to subverting democracy.

The traditional consent model reflected in PIPEDA creates an illusion of control that is typically exercised once and fleetingly. Yet dramatic increase in the importance of data has led to calls for data protection laws to provide new mechanisms for individuals to assert control over their data—ones that go well beyond the initial point of data collection. From the right of erasure to rights of data portability, new approaches to privacy attempt to address what has been a steady undermining of individual control over identity and autonomy in digital realms. In addition, privacy advocates maintain that without strong oversight and enforcement, data protection is largely meaningless. PIPEDA, built on a soft-touch ombuds model (Scassa, 2019; Stoddart, 2005), has come under fire for its relatively weak enforcement (Martin-Bariteau, 2019; Scassa, 2018).

Concerns over privacy in relation to the use of personal data or data derived from human activity in data analytics, AI, and related data-driven technologies extend to human welfare more generally. The use of data in profiling and targeting activities—whether it is of individuals or groups—can be biased, and can lead to discrimination, exclusion, and marginalization (Barocas & Selbst, 2016). The growing concentration of consumer data in the hands of major corporations and technology giants also raises competition law and consumer protection issues. Further, there are serious concerns that the changing nature of data processing, and in particular the use of AI and machine learning, make it difficult to understand how data is used and how decisions are made. Transparency, which has long been a core value associated with data protection, is significantly challenged in both public and private sectors. Joel Reidenberg states that "typically, democracies shield the privacy of citizens from the state and make the activities of the state transparent" (2015, pp. 449–450). He observes that rather than the traditional concept of a transparent government and a private citizen, governments and corporations are increasingly opaque, and citizens more transparent to them.

Canada's struggles with these issues do not occur in a vacuum. The EU's *General Data Protection Regulation* (GDPR) of 2016, which lays out the rules for data protection in all EU states, has set a new global standard—one which must be matched by those jurisdictions wishing to maintain transborder flows of personal data. The GDPR is

an ambitious law that seeks to balance the needs of government and industry to collect, process, and share data with the privacy rights of individuals. While it is not necessary to adopt the GDPR wholesale in Canada, there is no doubt that it will have a significant impact in driving reform of Canada's privacy laws. Yet these changes should not be motivated exclusively by the fear of being excluded from the economic benefits of continued transborder data flows. Given the significant actual and potential impacts of data-driven technologies in contemporary society, Canadians both need and deserve a principled human rights-based framework for privacy protection.

A Rights-Based Approach to Data Protection

Canada is a signatory to a number of international human rights instruments that recognize privacy as a human right. For example, Article 12 of the *Universal Declaration of Human Rights* (UNDHR) provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (UNDHR 1948). This same right is found in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR 1966). The UN Human Rights Committee (1988) has interpreted Article 17 of the ICCPR as requiring the protection of individuals from interference with their privacy not just by the state but also by other persons, both legal and natural. It also includes a right to the protection of the law against incursions on the right—in other words a right to effective legal recourse for breach of privacy rights. The New Zealand Human Rights Commission has stated that, as expressed in the UNDHR and the ICCPR, the right links "the human rights concepts of personal autonomy and dignity" (2018, p. 8).

> In 2013, the UN General Assembly adopted its resolution on the *Right to Privacy in the Digital Age*. This resolution reaffirmed the rights set out in Article 12 of the UNDHR and Article 17 of the ICCPR, and noted as well that "the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society" (UN General Assembly, 2013, p. 1). The link to these other rights serves as a reminder that while privacy is an individual right, it has broader

> collective dimensions as well. As Mantelero (2016) notes, both privacy and data protection play an important role in safeguarding not only individual interests, but also the quality of society in general. Freedom of association, limits to disproportionate surveillance practises, and prevention of discrimination based on sensitive personal data are just few examples of the social effects of safeguarding the right to privacy and personal information. Values such as democracy and pluralism are strictly related to the protection of these rights. (p. 245)

A human rights-based approach to privacy not only recognizes a fundamental right to privacy, but also acknowledges the interrelationship between privacy and the right of individuals to exercise their other rights and freedoms with autonomy and dignity. Further, the human right to privacy must be supported by legislation that renders the right effective and realizable.

Privacy as a Human Right and PIPEDA

Although Section 3 of PIPEDA acknowledges the existence of a right to privacy, this is undercut by the almost simultaneous recognition of the need of organizations to collect, use, and disclose personal information. This brief mention of a simple privacy right can be compared and contrasted with the recitals of the GDPR—the introductory statement of principles of the regulation—which situate that instrument's regulation of data processing within the context of a much broader range of human rights. Reidenberg (2015, p. 460) suggests that "the GDPR [seeks] to match political rights to new economic issues such as profiling, data security breach, and corporate responsibility. Europe looks at citizen transparency from the perspective of privacy as a fundamental right."

Throughout a total of 173 recitals, the GDPR makes repeated references to fundamental rights of individuals in relation to data processing. These include the right to be protected in data processing, as well as the right to be protected against the multiple harms that can flow from the processing of personal data. The GDPR's second recital reads:

> The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should,

> whatever their nationality or residence, *respect their fundamental rights and freedoms*, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons. (emphasis added)

While the actual provisions of the GDPR establish the rules for data processing, the recitals ground these processes in an articulation of the rights. By contrast, Section 3 of PIPEDA casts the right to privacy narrowly by framing it solely as a privacy right, and by balancing it against the interest of organizations in the collection, use, and disclosure of personal data.

Although it might be easy to dismiss the GDPR's recitals as being a lofty excess of verbiage, the framing of legislation is important to its interpretation. For example, the GDPR introduces the concept of "legitimate interest" for data processing (GDPR, 2018, Recital 47). This is meant as a kind of workaround to consent in a rapidly evolving data economy. An organization may have a legitimate interest in processing data it has already collected, but it might be unduly burdensome to obtain fresh consents for this processing. While the GDPR allows organizations to assert "legitimate interest" as a basis for the use of personal data, it must be weighed against the human rights of affected individuals and will only be justified where the impact on those human rights is not disproportionate to the goals sought to be obtained. The concept of legitimate interest has been mooted in Canada as an aspect of PIPEDA reform, and if it were added it would benefit from being incorporated within a framework that acknowledges and gives priority to human rights.

It is also noteworthy that some of the new rights recognized in the GDPR are much easier to reconcile with a broader view of privacy as a human right than they are with the narrower concept of data protection. For example, the right to be forgotten is complicated when framed in terms of data protection, since it typically involves information that has entered the public domain. Yet the right to be forgotten is not simply a right to privacy in the sense of shielding one's personal information from public view; rather, it is also tied

to a right to self-actualize, and to potentially even redefine oneself to the world.

The right to data portability is similarly not strictly a right to privacy. Basic data protection law addresses an organization's need to obtain consent to the collection, use, or disclosure of personal information. But data portability is about an individual's right to control their personal data. The individual is entitled to ask for their data that is in the hands of an organization and to port it, in machine-readable formats, to another organization. It is not privacy in the narrow sense that is enhanced by such a right, but rather autonomy and freedom.

The rights in the GDPR around transparency of automated processing of data and the right to an explanation of automated decision-making are similarly not privacy rights in the strict sense. Rather, they are rights that enable individuals to protect themselves against potential bias and injustice.

Although a human rights-based approach to privacy is an important aspect of basic data protection, it is clear that it is also valuable because it both includes and extends beyond privacy rights. For example, the GDPR, in Recital 4, acknowledges the importance of "the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity." The recognition of other rights and freedoms directly impacted by the protection of privacy shifts the GDPR away from a narrower, consent-based paradigm of classic data protection in which an individual negotiates for the collection, use, or disclosure of their personal information in exchange for products or services.

Models for a Human Rights-Based Approach

In addition to the GDPR, there are several past and current models that offer some insights into how a human rights-based approach might be structured for people's digital lives. In 2001, Senator Sheila Finestone introduced Bill S-21, *An Act to guarantee the human right to privacy* (*Privacy Charter*). The bill's preamble declared that privacy was "a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada

is a signatory." It also linked privacy to the public good because of the role it plays in establishing "relations of mutual trust and confidence that are fundamental to the Canadian social fabric." Finally, the preamble linked privacy to the preservation of democracy and to the "full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*" (*Privacy Charter*, 2001).

The bill's stated purpose was to give effect to basic principles that highlighted the importance of the right to privacy, the existence of a legal right to privacy, and the limitations on privacy rights. Section 3 defined the right to privacy as including physical privacy, the freedom from surveillance, the freedom for interception and monitoring of communications, and "freedom from the collection, use and disclosure of their personal information" (*Privacy Charter*, 2001). Section 4 gives individuals the right to claim and enforce their privacy rights; in Section 4(3), it also prohibits the unjustifiable infringement of a person's right to privacy (*Privacy Charter*, 2001).

Limitations on the right to privacy were acknowledged in the *Privacy Charter*. Although Section 5 began with the principle that any interference with an individual's privacy is an infringement, infringements can be justified if they are "reasonable and can be demonstrably justified in a free and democratic society" (*Privacy Charter*, 2001). To be justifiable, an infringement would have to be lawful and necessary to achieve a sufficiently important objective linked to the public good or to the need to respect another human right. The objective that motivates the infringement must not be capable of being achieved by a less privacy-infringing means and the importance of the objective and its beneficial effects would have to outweigh the detrimental privacy impacts. The consent of the impacted individual will also negate infringement.

The rights in the bill were to be given substantive effect in a number of ways. The Minister of Justice was tasked with overseeing all government bills and prospective regulations to ensure that they were consistent with the *Privacy Charter* (2001, s. 6). Private sector actors were also bound to comply with it in all of their contracts (s. 6). The *Privacy Charter* was to prevail over any inconsistent federal legislation unless another statute expressly declared that it operated notwithstanding (s. 11). This feature sought to import some of the weight of constitutional rights without the need for a painful and potentially fruitless constitutional amendment process. Past experience with the

Canadian Bill of Rights (1960) suggests that such a framework might not be particularly helpful (Hogg, 2007). However, the *Privacy Charter* may have sought to avoid the weaknesses of the *Canadian Bill of Rights* by incorporating a provision (s. 4) that would give Canadians the ability to claim and enforce their rights.

In 2004, the British Columbia Information and Privacy Commissioner (BC Commissioner) recommended the adoption, in the province, of some form of a "privacy charter" that would more deeply embed privacy considerations into government law and policy-making. The recommendation was to require government bodies to assess the privacy impacts of any "law, policy, program or technology under consideration" (Office of the Information and Privacy Commissioner [OIPC], 2004). The assessment would be guided by a privacy charter that either would become part of the *Freedom of Information and Protection of Privacy Act* (FIPPA) or be found in a freestanding statute. Although privacy impact assessments (PIAs) were required by FIPPA at the time, the BC Commissioner believed that all they did was assess technical compliance. The BC Commissioner was concerned that "a PIA that only assesses technical compliance fails to account for the wider risks that initiatives can raise for the personal privacy of individuals whose lives and personal information are affected" (OIPC, 2004, p. 26). The recommendation was never adopted.

The *Privacy Charter* was controversial, and it failed for a number of reasons (Shade, 2009). Canada's Privacy Commissioner at the time, George Radwanski, refused to endorse the bill because it "comports itself as if there were no privacy legislation in place, as if we did not have a *Privacy Act*, which is a good piece of law, and as if we did not have the new Bill C-6, the private sector act, which is also a good piece of law" (Radwanski, 2001, para. 12). Commissioner Radwanski was concerned that the bill would create two-track recourse, with the *Privacy Charter* creating broad and open-ended rights, and public and private sector data protection laws creating carefully constructed and balanced frameworks that would be marginalized by the new right. The Senate Committee that considered Bill C-6 was concerned about its interface with the *Criminal Code*, and saw a need for the scheme to be more integrated with the Office of the Privacy Commissioner.

The *Privacy Charter* was a product of its particular moment in history. It was introduced in the Senate at a time when PIPEDA was still in bill form, and thus there was no previous experience

with the oversight of private sector data collection, use, or disclosure. Governments were preoccupied with security in a post-9/11 environment, and there were new measures being proposed that would dramatically increase the surveillance capacities of the state. Public preoccupations with privacy were therefore primarily turned toward concerns over state surveillance. While state surveillance remains a significant concern today, the widespread and ubiquitous data collection by the private sector results in a convergence with the surveillance state, creating a much greater need to recognize the relationship between human rights and ubiquitous data collection. Further, private sector surveillance—labelled "surveillance capitalism" by Shoshana Zuboff (2015)—is a growing concern. The size and complexity of the GDPR is an indication that addressing data protection requires far more than a simple set of rules; what it may instead require is the situating of the data protection regimes within a human rights-based framework.

The *Privacy Charter* recognized that privacy rights were not absolute, but it provided no specific framework in which competing rights could be identified or weighed. Both PIPEDA and the *Privacy Act*, as data protection statutes, attempt to negotiate competing rights and interests in relation to the collection, use, and disclosure of personal information. In fact, the bulk of both statutes reflects a direct engagement with this balancing. This suggests that a broader human rights-based approach might most effectively be incorporated into each statute through an expanded statement of principles that provides a framework within which the legislation should be interpreted.

The Quebec *Charter of Human Rights and Freedoms* offers an interesting model that combines privacy with other human rights. This provincial law takes precedence over other legislation in the province unless another provincial statute specifically declares that it does not apply (Quebec *Charter*, s. 52). While the Quebec *Charter* is not a privacy charter *per se*, it contains several provisions that have a strong connection to privacy values. Article 1 establishes, "a right to life, and to personal security, inviolability and freedom"; Article 4 provides that "every person has a right to the safeguard of his dignity, honour and reputation"; and Article 3 provides for the "freedom of conscience, freedom of religion, freedom of opinion, freedom of expression, freedom of peaceful assembly and freedom of association." Each of these rights is linked to the values associated with privacy, and all would apply, for example, to the interpretation

of privacy rights under the *Civil Code*, or to data protection rights under Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*. The Quebec *Charter* also provides for specific privacy rights in Article 5: "Every person has a right to respect for his private life." The inviolability of the home is protected in Article 7, Article 8 provides a broad right against anyone entering on a person's property or taking anything therefrom without consent, and Article 9 states that "every person has a right to non-disclosure of confidential information." The Quebec *Charter* also includes the right to be free from discrimination, something that is becoming increasingly important in the context of data processing. Article 24.1 of the Quebec *Charter* provides for a right to be free from unreasonable search and seizure at the hands of the state. The document also contains a series of economic and social rights, among which is found, in Article 44, the "right to information to the extent provided by law." The provisions of the Quebec *Charter* apply broadly across public and private sectors alike: There is a right of action and a right to compensation, including punitive damages established by Article 49. While many of the rights and freedoms contain their own limitations in the wording of articles that establish them, the fundamental rights and freedoms found in Articles 1 through 8 of the Quebec *Charter* are made subject, in Article 9, to "a proper regard for democratic values, public order and the general well-being of the citizens of Quebec." The Quebec *Charter* has been relied upon to protect privacy rights on its own and in combination with separate privacy rights found in the Quebec *Civil Code*. The rights in the *Civil Code* are also in part implemented by separate public and private sector data protection laws in Quebec.

Both the *Privacy Charter* and the Quebec *Charter* offer examples of how a broader human rights perspective could inform a legislative approach to data protection law in Canada. Of course, Canadian federalism adds a layer of complexity to data protection, since privacy is neither exclusively a matter of federal or provincial jurisdiction (Kratchanov, 1995). PIPEDA is justified as federal legislation under the "trade and commerce" power, which limits its application to the collection, use, or disclosure of personal information to the context of commercial activity (s. 4.1.a). PIPEDA's odd constitutional status and its relationship to provincial private sector data protection statutes in Quebec, Alberta, and British Columbia make adopting a human rights-based approach through an independent legislative instrument complicated. However, the values that should guide the interpretation

of PIPEDA could be grounded in either the preamble of the statute or in a reworked Section 3.

Conclusion

More than ever, big data issues raise crucial privacy concerns as well as complex, interrelated human rights issues. Although acknowledged by the courts as quasi-constitutional in nature, PIPEDA is a data protection statute that makes only a brief nod to privacy rights in the same provision that balances them against the needs of organizations to collect, use, and disclose personal information. Further, it does not acknowledge the complex range of privacy interests in the big data era, nor does it acknowledge the relationship between the protection of privacy and the safeguarding of other human rights values. As we move toward reform of PIPEDA, it is time to recognize the important and interconnected human rights dimensions of privacy. Although a set of recitals in a preamble or a legislative provision setting out the human rights basis for the protection of privacy may seem like cosmetic changes, they would serve important goals. The first of these is to give legislative voice to the principles and human rights values that are meant to underlie data protection law in Canada. The second is to provide concrete direction for the interpretation of provisions that, while also serving to oil the machinery of commerce and innovation, should never do so at the expense of fundamental human rights.

Acknowledgements

This paper draws upon research that was funded by the Office of the Privacy Commissioner of Canada in early 2019. All views expressed are the author's own.

References

Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 (1993).

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*, 671–732.

Bill S-21, An Act to guarantee the human right to privacy [Privacy Charter]. (2001). 37th Parliament, 1st Session.

Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI]. (2018a, February). *Towards privacy by design: Review of the Personal Information Protection and Electronic Documents Act*. Report no. 12. 42nd Parliament, 1st Session. https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12/

Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI]. (2018b, December). *Democracy under threat: Risks and solutions in the era of disinformation and data monopoly*. Report no. 17. 42nd Parliament, 1st Session. https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf

Canada, House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI]. (2018c, June). *Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process*. Report no. 16. 42nd Parliament, 1st Session. https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf

Canadian Bill of Rights, SC 1960, c. 44 (1960).

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act of 1982, Schedule B of the Canada Act (UK), 1982, c. 11 (1982).

Charter of Human Rights and Freedoms, CQLR, c. C-12 (1975).

Civil Code of Quebec, CQLR, c. CCQ-1991 (1991).

Curran, B. (2014). Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401. *Alberta Law Review*, *52*(1), 185–197.

Freedom of Information and Protection of Privacy Act [FIPPA], RSBC, c 165 (1996).

Hogg, P.W. (2007). *Constitutional Law of Canada*, 5th ed., Carswell.

Innovation, Science and Economic Development Canada [ISED]. (2019). *Strengthening privacy for the digital age: Proposals to modernize the Personal Information Protection and Electronic Documents Act*. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

International Covenant on Civil and Political Rights [ICCPR]. New York, 16 December 1966, United Nations Treaty Series, vol. 999, no. 14668, p. 171.

Kratchanov, D. C. (1995). *Personal information and the protection of privacy 1995*. Uniform Law Conference of Canada. https://www.ulcc.ca/en/annual-meetings/430-1995-quebec-qc/civil-section-documents/246-personal-information-and-the-protection-of-privacy-1995?showall=1&limitstart=

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law and Security Review*, *32*, 238–255.

Martin-Bariteau, F. (2019, May 7). Qu'attendons-nous pour protéger la vie privée ? *Policy Options*. https://policyoptions.irpp.org/magazines/may-2019/quattendons-nous-pour-proteger-la-vie-privee/

New Zealand Human Rights Commission. (2018). *Privacy, data and technology: Human rights challenges in the digital age*. https://www.hrc.co.nz/files/5715/2575/3415/Privacy_Data_Technology_-_Human_Rights_Challenges_in_the_Digital_Age_FINAL.pdf

Office of the Information and Privacy Commissioner for British Columbia [OIPC]. (2004). *Submission of the Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act*. https://www.oipc.bc.ca/special-reports/1274

Office of the Privacy Commissioner of Canada [OPC]. (2017). *2016-17 Annual report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

Office of the Privacy Commissioner of Canada [OPC]. (2018). *Securing trust and privacy in Canada's electoral process: Resolution of the federal, provincial and territorial information and privacy commissioners*. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_180913/

Personal Information Protection and Electronic Documents Act [PIPEDA], SC, c. 5 (2000).

Privacy Act, RSC, c. P-21 (1985).

Radwanski, G. (2001, September 20). *Testimony to the Standing Senate Committee on Social Affairs, Science and Technology*. 37th Parliament, 1st Session. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/archive/02_05_a_010920/

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR], O.J., L. 119, 4.5.2016, p. 1–88.

Reidenberg, J. R. (2015). The transparent citizen. *Loyola University Chicago Law Journal*, *47*, 437–463.

Scassa, T. (2018, June 7). Enforcement powers key to PIPEDA reform. *Policy Options*. https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/

Scassa, T. (2019). Moving on from the ombuds model for data protection in Canada. *Canadian Journal of Law and Technology*, *1*, 90–98.

Shade, L. R. (2009). Reconsidering the right to privacy in Canada. *Bulletin of Science, Technology & Society*, *28*(1), 80–91.

Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics Information Technology*, *18*, 33–39.

Stoddart, J. (2005). *Cherry picking among apples and oranges: Refocusing current debate about the merits of the ombuds-model under PIPEDA*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2005/omb_051021/

The Canadian Press. (2018, December 7). Sidewalk Labs's vision and your data privacy: A guide to the saga on Toronto's waterfront. *The Globe and Mail*. Retrieved June 24, 2019, from https://www.theglobeandmail.com/canada/toronto/article-sidewalk-labs-quayside-toronto-waterfront-explainer/

United Nations General Assembly. (1948, 10 December). Resolution 217 A (III), *Universal declaration on human rights* [UNHDR]. http://www.un.org/en/universal-declaration-human-rights/

United Nations General Assembly. (2013, December 18). Resolution 68/167, *The right to privacy in the digital age,* A/RES/68/167. https://undocs.org/A/RES/68/167

United Nations Human Rights Committee. (1988, 8 April 1988). *CCPR general comment No. 16: Article 17 (right to privacy), the right to respect of privacy, family, home and correspondence, and protection of honour and reputation*.

Vincent, D. (2019, February 19). Waterfront Toronto officials to face grilling in Ottawa over Sidewalk Labs plans. *The Toronto Star*. https://www.thestar.com/news/gta/2019/02/19/waterfront-toronto-officials-to-face-grilling-in-ottawa-over-sidewalk-labs-plans.html

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89.