# Privacy Rights in the Digital Age: A North American Data Protection Framework

Jill Barclay, Bailey Cordrey, Gurleen Tak and Sarah Wyatt

## Issue

In the digital age, as personal data becomes ever more central to private and public sector operations, the legal and normative frameworks set up by domestic and international governments to protect privacy rights have become outdated.

## Background

The rapid proliferation of emerging technologies, along with advancements in data analysis, has created enormous opportunities for private and public sector organizations. Alongside these developments, an increase in predatory data practices has also occurred, due to intrusive technological systems becoming mainstream and widespread. In response to these challenges, Canadian digital privacy laws and enforcement mechanisms have not been adequately adapted to protect vulnerable populations in the digital age. Since the creation of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) 20 years ago, both technological advances and social change have altered the way personal data is collected, stored and used by industries, yet necessary changes have not been implemented. To hold data collecting enterprises accountable for violating international human rights, Canada has the opportunity to reform domestic data protection legislation and initiate the creation of a transnational data protection regime that addresses the interconnectedness of Internet infrastructure across North America.

A modern digital privacy regime can bring efficient and adaptable approaches to the governance of online information while protecting Canadian citizens from exploitation. A North American-wide approach allows for coherent online protection of personal data while avoiding a patchwork of differing, and potentially competing, privacy regulations between provinces. The creation of such a regime also promises to create a level playing field for innovation and commerce. Global Affairs Canada (GAC) has the opportunity to lead the remediation of Canada's personal information protection through an expanded and modernized North American-wide framework.

## The Right to Privacy in the Digital Age

The lives of Canadians increasingly revolve around data. From social media outlets, banks, retailers and governments, almost every industry we interact with involves the collection and analysis of granular personal information. These advancements have allowed for transgressions that include geolocation surveillance, misuse of biometric data, and many other breaches of personal security that threaten citizens' protection (Office of the Privacy Commissioner of Canada 2020). Although the right to privacy is internationally recognized, the global human rights regime was built prior to the widespread use of digital technology and therefore was not designed to protect people against the advanced surveillance and telecommunications technologies used by state and corporate actors. As former UN High Commissioner for Human Rights Navi Pillay explained in 2014, private enterprises have increasingly put themselves at risk of being complicit in human rights abuses through their

provision of personal data to states (UNHCHR 2014). Without the benefit of national legislative frameworks, oversight and enforcement checks, states have unchecked opportunities to infringe on privacy or restrict freedom of expression (ibid.). The government therefore has a role to play in safeguarding the privacy of its citizens as the centrality and profitability of their data grows and encourages the spread of hostile data practices.

## The Landscape of Data Protection in North America

Canada's internet infrastructure has undergone significant developments over the past decade. The Canadian Internet Registration Association states that the number of internet exchange points (IXPs) within Canada has increased from only 2 IXPs in 2012 to 16 IXPs in 2019, with new IXPs emerging in almost every major Canadian city, including Vancouver, Calgary, Winnipeg, Montreal, Quebec City and Halifax. While this added infrastructure has significantly improved Canada's internet connectivity, IXP growth has had to accommodate both a growing Canadian population, which had the highest growth rate among the G7 countries in 2018–2019, and the increased demands of citizens' personal internet usage. This has resulted in much of Canadians' data being routed through the United States, where it is beholden to the precarious standards of the American private and public sector and therefore vulnerable to misuse. US private sector entities are bound first by a patchwork of sectoral law and state-specific regulations, while the public sector is governed by intrusive data laws such as the 2001 Patriot Act, which later became the USA Freedom Act. This approach requires novel legislation each time a new technology is introduced, creating challenges for enforcement and leaving gaps over time where privacy is vulnerable (Banisar and Davies n.d.).

In order to recapture Canada's internet traffic within its borders, the Canadian Infrastructure Registration Authority and entities within the telecommunication sector have argued for further development of IXPs. Though this could be an effective tool to safeguard the data privacy of Canadians it would require extensive investments from the federal government or private sector, as start-up costs alone for a single IXP are considerable. To avoid rerouting Internet traffic through bordering states and proximal cities such as Seattle, New York and Chicago, Canada could pursue multi-state compromise in order to effectively protect Canadian privacy rights. International coordination on the North American scale currently exists in the form of trade agreements such as Canada-United States-Mexico Agreement. Beyond existing coordination on trade in North America, opportunities also exist regarding data privacy coordination due to the cross-border data transfers between Canada, the United States and Mexico. Having a North American framework therefore could fundamentally reshape North American cyber relations. This framework would offer opportunities for all parties involved, as data could be stored in Mexico for a fraction of the cost while creating job opportunities and economic gains for Mexico (Council on Foreign Relations 2020). The coordination and shared oversight could also promote action on privacy protection that would increase each state's capacity to monitor data within North American borders. Jim Balsillie, co-founder and retired co-CEO of BlackBerry, and chair of the Centre for International Governance Innovation, testified at the 2018 International Grand Committee hearings on Big Data, Privacy and Democracy: "Data governance is the most important public policy issue of our time. It is cross-cutting, with economic, social, and security dimensions. It requires both national policy frameworks and international coordination" (Balsillie 2019).

Last year, Innovation, Science and Economic Development Canada (ISED) released the Digital Charter, signalling the desire for change, but so far no significant improvements to Canada's digital regulatory landscape have been made (ISED 2019). Canada is well-positioned to strengthen existing legal instruments such as the Privacy Act (enacted in 1985) and PIPEDA, to bring them up to date. Privacy Commissioner Daniel Therrien has been advocating for these revisions for years, telling Parliament in 2018 that Canada's federal privacy regime is "sadly falling behind what is the norm in other countries" and gives companies wide latitude to use personal information for their own benefit. Currently, there is no comprehensive North American treaty regulating the protection of digital privacy. However, there have been international efforts such as the UN's adoption of the UN Right to Privacy in the Digital Age (UNHCR,2018), which establishes the responsibility of member states to protect citizens online. This legal instrument provides a universal framework, which can be used as a guiding principle for a North American treaty.

## Innovative Governance Solutions

In response to this global call to action, the European Union instituted the General Data Protection Regulation (GDPR) in 2018 as part of an effort to synchronize data privacy laws across member countries and affirm the online rights of EU citizens. The GDPR radically altered conventions around how data controllers and processors handle the personal information of data subjects. It limits how businesses and organizations can use individuals' data and assigns responsibilities to participants in the European data ecosystem. Under the GDPR, EU citizens have the right to request a copy of their data held by a corporate entity, withdraw their consent for further data collection, and, in some circumstances, ask that a controller or processor entirely erase all data held on the subject. Businesses and organizations are also required to appoint a "data protection officer" who is tasked with ensuring GDPR compliance and administering the entity's data protection strategy. Failure to comply with the GDPR can result in steep fines, of consequence to even the most profitable tech giants, ranging from two to four percent of their total revenue (Wolford 2020).

The GDPR is currently the world's most robust example of data protection legislation. As the first attempt at regulating data privacy at scale, it is far from perfect. However, it has set a new standard for internet privacy and initiated a long-overdue dialogue about how to ensure the rights of individuals are protected in digital spaces. Since its implementation, jurisdictions across North America have begun prospecting their own data privacy laws. California introduced the California Consumer Privacy Act of 2018, a privacy protection law based on the GDPR for citizens' personal data, which took effect in January 2020 (Petrova et al. 2019). After a series of data breaches exposed vulnerabilities in Quebec's privacy legislation, the province announced plans to update its Private Sector Act in the image of the GDPR. Should Quebec initiate these developments ahead of the federal government's data privacy modernization plans, it would further fragment the regulatory landscape in Canada. These local initiatives signal a desire for change and would be made much stronger by a cross-boundary agreement that speaks to the interconnectedness of internet infrastructure.

## Next Steps: What could a data protection framework look like in North America?

Using PIPEDA as a baseline, GAC has the opportunity to initiate a North America-wide framework for data privacy that better protects citizens' privacy rights. Modernizing domestic and international privacy legislation would strengthen Canada's governance of online data while ensuring compliance of enterprises' data collection in accordance with the rights of Canadians.

To support the necessary administrative and oversight functions of a North American data protection framework, we recommend the creation of a multilateral organization made up of government, private industry and civil society representatives across North America. Achieving the domestic and interstate objectives we have outlined here will require formal coordination between a network of actors that largely operate in disparate spheres. Uniting these communities under a singular institution would create the space for open dialogue and integrative governance solutions that speak to the myriad of interests captured by a continental data privacy framework.

This institution would need to bring together state delegations to establish mutually agreeable terms and domestic actions. To meaningfully participate, governments would need to build the technological expertise and legislative capacity within their agencies to implement the objectives of the data privacy agreement. The institution would be responsible for mediating and consulting between corporate entities and special interest groups. Additionally, the institution would be obliged to supervise and act on the reports of a network of data protection officers stationed across the private and public sectors and administer fines for noncompliance. Relevant civil society groups would be requisitioned for their expertise in the creation of institutional standards, and potentially contracted to perform research, monitoring and educational functions on its behalf (ISED 2019).

## Recommendations

1. **Canada should improve domestic legal instruments on surveillance and privacy.** With the Digital Charter, Canada is well-positioned to enhance its Privacy Act and PIPEDA to adopt a more cohesive, nation-wide legal instrument that addresses digital privacy. This would allow for stronger enforcement power over public and private online data storage regimes.

2. **Canada should pursue a North American data protection framework.** As IXPs used by Canadians are not entirely contained within national borders, any amendment to our current privacy and data protection regulations must take into account the internet infrastructure overlap between Canada, the United States and Mexico.

3. **Canada should create a North American data privacy organization to provide administrative support and oversight functions.** This institution will be responsible for managing the continental data protection framework, coordinating necessary technical and human resources, and ensuring compliance among involved parties. It will also convene regular meetings between government delegations, corporate actors, special interest groups and civil society representatives from Canada, the United States and Mexico.

## About the Authors

**Jill Barclay** is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the BSIA.

**Bailey Cordrey** is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the BSIA.

**Gurleen Tak** is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the BSIA.

**Sarah Wyatt** is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the BSIA.

## Acknowledgements

The authors would like to thank Peter Johnson for his guidance and mentorship as a supervisor. Additional thanks to the BSIA and GAC for their consistent support in revising and finalizing the brief.

## References

Balsillie, Jim. 2019. "Data is not the new oil — it's the new plutonium." *Financial Post*, 28 May. https://business.financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium.

Banisar, David, and Simon Davies. n.d. "Privacy and Human Rights: an International Survey of Privacy Laws and Practice." Global Internet Liberty Campaign. http://gilc.org/privacy/survey/intro.html.

Canadian Internet Registration Authority. 2020. "Canada's Internet Infrastructure: Internet Exchange Points." https://www.cira.ca/improving-canadas-internet/initiatives/canadas-internet-infrastructure-internet-exchange-points.

Council on Foreign Relations. 2020. "NAFTA and the USMCA: Weighing the Impact of North American Trade." https://www.cfr.org/backgrounder/naftas-economic-impact.

ISED. 2019a. "Proposals to modernize the Personal Information Protection and Electronic Documents Act." https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

———2019b. "Canada's Digital Charter: Trust in a digital world." https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

Office of the Privacy Commissioner of Canada. 2020. "A Data Privacy Day Conversation with Canada's Privacy Commissioner." https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200128/.

Petrova, Anastasia, et al. 2019. "The impact of the GDPR outside the EU." Lexology, September 17. https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f.

UNHCHR. 2014. "Opening Remarks by Ms. Navi Pillay to the Expert Seminar: The Right to Privacy in the Digital Age." Geneva, February 24. https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E.

———2018. "The Right to Privacy in the Digital Age." https://undocs.org/A/HRC/39/29.

Wolford, Ben. 2020. "What are the GDPR Fines?" GDPR.EU. https://gdpr.eu/fines/.