Minding Your Business

A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law

By Amanda Cutinha and Christopher Parsons

NOVEMBER 22, 2022
RESEARCH REPORT #161

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Electronic version first published by the Citizen Lab in 2022. This work can be accessed through https://citizenlab.ca/2022/11/a-critical-analysis-of-the-collection-of-de-identified-mobility-data/.

Document Version: 1.1

- Updated heading for Recommendation 11.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the Authors

Amanda Cutinha contributed to this report while a Researcher at the Citizen Lab. She is currently a Litigation Associate at Miller Thomson LLP. She received her BA Hons. and JD from the University of Toronto.

Christopher Parsons is currently a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Bachelor's and Master's degrees from the University of Guelph and his PhD from the University of Victoria.

Acknowledgements

We would like to extend our gratitude to the people that have shared their thoughts, expertise, and time with us throughout the process of writing this report.

We want to specifically thank individuals inside and outside of government for the discussions we have had and which have enabled us to better understand Bill C-27. Thanks also to Benjamin Ballard for earlier work with us, which informed some of our thinking for this report. We greatly appreciate the time and expertise that Brenda McPhail and Adam Molnar provided when conducting peer review of this report. All remaining errors are our own.

Additionally, we would like to thank Mari Zhou for her assistance designing and formatting the report and Snigdha Basu for her communications support. Copyedits were performed by Joyce Parsons of Stone Pillars Editing and Consulting. This report was undertaken under the supervision of Prof. Ronald Deibert.

Corrections and Questions

Please send all questions and corrections to: chris@citizenlab.ca

Suggested Citation

Amanda Cutinha and Christopher Parsons. “Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law,” Citizen Lab Research Report No. 161, University of Toronto, November 22, 2022.

Table of Information Boxes

Table of Acronyms

C-11	*Bill C-11: Digital Charter Implementation Act, 2020*
C-27	*Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act*
CPPA	Consumer Privacy Protection Act, Part I of Bill C-27
CRC	Communications Research Centre
ETHI	Standing Committee on Access to Information, Privacy and Ethics
GPS	Global Positioning System
GAEN	(Google/Apple) Exposure Notification
ISED	Innovation, Science and Economic Development
OPC	Office of the Privacy Commissioner of Canada
OCAP	Ownership, Control, Access and Possession
PIPEDA	*Personal Information and Protection of Electronic Documents Act*
PMD	Privacy Management Division of Health Canada
PHAC	Public Health Authority of Canada
RFP	Request for Proposal
SARS	Severe Acute Respiratory Syndrome
UNDRIP	United Nations Declaration on the Rights of Indigenous Peoples

Table of Recommendations

Contents

Contents

Executive Summary

The Government of Canada obtained de-identified and aggregated mobility data from private companies for the socially beneficial purpose of trying to understand and combat the spread of COVID-19. This collection began as early as March 2020, and the information was provided by Telus and BlueDot. It wasn't until December 2021, after the government issued a request for proposals for cellular tower information that would extend the collection of mobility information, that the public became widely aware of the practice. Parliamentary meetings into the government's collection of mobility data began shortly thereafter, and a key finding was that Canada's existing privacy legislation is largely ineffective in managing the collection, use, and disclosure of data in a manner that recognizes the privacy rights of individuals. In spite of this finding, the federal government introduced *Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* in June 2022 which, if passed into law, will fail to correct existing deficiencies in Canada's federal commercial privacy law. In particular, Bill C-27 would make explicit that the government can continue collecting information, including mobility data from private organizations, so long as uses were socially beneficial and without clearly demarcating what will or will not constitute such uses in the future.

This report, "Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law," critically assesses the government's existing practice of collecting mobility information for socially beneficial purposes as well as private organizations' ability to collect and use personal information without first obtaining consent from individuals or providing them with knowledge of the commercial activities. It uses examples raised during the COVID-19 pandemic to propose 19 legislative amendments to Bill C-27. These amendments would enhance corporate and government accountability for the collection, use, and disclosure of information about Canadian residents and communities, including for so-called de-identified information.

Part 1 provides a background of key privacy issues that were linked to collecting mobility data during the COVID-19 pandemic. We pay specific attention to the implementation of new technologies to collect, use, and disclose data, such as those used for contact-tracing applications and those that foreign governments used to collect mobility information from telecommunications carriers. We also attend to the concerns that are linked to collecting location information and why there is a consequent need to develop robust governance frameworks.

Part 2 focuses on the collection of mobility data in Canada. It outlines what is presently known about how Telus and BlueDot collected the mobility information that was subsequently disclosed to the government in aggregated and de-identified formats, and it discusses the key concerns raised in meetings held by the Standing Committee on Access to Information, Privacy and Ethics. The Committee's meetings and final report make clear that there was an absence of appropriate public communication from the federal government about its collection of mobility information as well as a failure to meaningfully consult with the Office of the Privacy Commissioner of Canada. The Government of Canada also failed to verify that Telus and BlueDot had obtained meaningful consent prior to receiving data that was used to generate insights into Canadian residents' activities during the pandemic.

Part 3 explores the lawfulness of the collection of mobility data by BlueDot and Telus and the disclosure of the data to the Public Health Agency of Canada under existing federal privacy law. Overall, we find that BlueDot and Telus likely complied with current privacy legislation. The assessment of the lawfulness of BlueDot and Telus' activities serves to reveal deficiencies in Canada's two pieces of federal privacy legislation, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

In **Part 4**, we identify six thematic deficiencies in Canada's commercial privacy legislation:

1. PIPEDA fails to adequately protect the privacy interests at stake with de-identified and aggregated data despite risks that are associated with re-identification.
2. PIPEDA lacks requirements that individuals be informed of how their data is de-identified or used for secondary purposes.
3. PIPEDA does not enable individuals or communities to substantively prevent harmful impacts of data sharing with the government.
4. PIPEDA lacks sufficient checks and balances to ensure that meaningful consent is obtained to collect, use, or disclose de-identified data.
5. PIPEDA does not account for Indigenous data sovereignty nor does it account for Indigenous sovereignty principles in the United Nations Declaration on the Rights of Indigenous Peoples, which has been adopted by Canada.
6. PIPEDA generally lacks sufficient enforcement mechanisms.

The Government of Canada has introduced the *Consumer Privacy Protection Act* (CPPA) in Bill C-27 to replace PIPEDA. **Part 5** demonstrates that Bill C-27 does not adequately ameliorate the deficiencies of PIPEDA as discussed in Part 4. Throughout, Part 5 offers corrective recommendations to the *Consumer Privacy Protection Act* that would alleviate many of the thematic issues facing PIPEDA and, by extension, the CPPA.

The federal government and private organizations envision the *Consumer Privacy Protection Act* as permitting private individuals' and communities' data to be exploited for the benefit of the economy and society alike. The legislation includes exceptions to consent and sometimes waives the protections that would normally be associated with de-identified data, where such exemptions could advance socially beneficial purposes or legitimate business interests. While neither the government nor private business necessarily intend to use de-identified information to injure, endanger, or negatively affect the persons and communities from whom the data is obtained, the breadth of potential socially beneficial purposes means that future governments will have a wide ambit to define the conceptual and practical meaning of these purposes. Some governments, as an example, might analyze de-identified data to assess how far people must travel to obtain abortion-care services and, subsequently, recognize that more services are required. Other governments could use the same de-identified mobility data and come to the opposite conclusion and selectively adopt policies to impair access to such services. This is but one of many examples. There are similar, though not identical, dangers that may arise should private organizations be able to collect or use an individual's personal information without their consent under the legitimate interest exemption in the CPPA. Specifically, this exemption would let private organizations determine whether the collection or use of personal information outweighs the adverse effects of doing so, with the individuals and communities affected being left unaware of how personal information was collected or used, and thus unable to oppose collections or uses with which they disagree.

Parliamentary committees, the Office of the Privacy Commissioner of Canada, Canadian academics, and civil society organizations have all called for the federal government to amend federal privacy legislation. As presently drafted, however, the *Consumer Privacy Protection Act* would reaffirm existing deficiencies that exist in Canadian law while opening the door to expanded data collection, use, and disclosure by private organizations to the federal government without sufficient accountability or transparency safeguards while, simultaneously, empowering private organizations to collect and use personal information without prior consent or knowledge. Such safeguards must be added in legislative amendments or Canada's new privacy legislation will continue the trend of inadequately protecting individuals and communities from the adverse effects of using de-identified data to advance so-called socially beneficial purposes or using personal information for ostensibly legitimate business purposes.

Introduction

Mobility information can be intensely sensitive. It can reveal individuals' and communities' patterns of life and reveal associational trends before participants themselves are aware of them.[1] Moreover, researchers have regularly shown that even when geolocation information associated with individuals is subsequently de-identified, anonymized, or otherwise transformed to restrict insights into specific individuals, it can be technically possible to defeat these protective measures.[2] Laws that prohibit these kinds of activities can reduce risks so long as the parties that possess the data behave lawfully and never lose control of the data in their possession. Unfortunately, even in highly regulated health, law enforcement, and national security environments, government employees sometimes abuse access to sensitive and intimate information about members of the public.[3] Just like private organizations, governments can also experience data breaches, including those containing population-level information.[4] In the Canadian context, this

---

1 Katherine J. Strandburg. (2008). "Surveillance of Emergent Associations: Freedom of Association in a Network Society" in Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina De Capitani de Vimercati (Eds), *Digital Privacy: Theory, Technologies, and Practices.* New York: Auerbach Publications.

2 Boris Lubarsky. (2017). "Re-identification of Anonymized Data." *Georgetown Law Technology Review.* Available at: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/; Danny Bradbury. (2021). "De-identify, re-identify: Anonymised Data's Dirty Little Secret." *The Register.* Available at: https://www.theregister.com/2021/09/16/anonymising_data_feature/; Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye. (2019). "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models." *Nature Communications.* Available at: https://www.nature.com/articles/s41467-019-10933-3; *Anonyome Labs.* (2020). "Re-idedntification of Anonymous Data is Scarily Simple." Anonyome Labs. Available at: https://anonyome.com/2020/12/re-identification-of-anonymous-data-is-scarily-simple/.

3 The Canadian Press. (2020). "Ontario Police Used COVID-19 Database Illegally, Civil Rights Groups Find." *CBC News*. Available at: https://www.cbc.ca/news/canada/toronto/covid-police-database-1.5745481; Information and Privacy Commissioner of Ontario. (2021). "Stamping Out Snooping Once and For All." *Information and Privacy Commissioner of Ontario.* Available at: https://www.ipc.on.ca/stamping-out-snooping-once-and-for-all/; *CBC News.* (2018). "Alberta Nurse Fined for Snooping in Patients Information." *CBC News*. Available at: https://www.cbc.ca/news/canada/edmonton/health-information-unauthorized-access-badger-1.4737441; Sadie Gurman. (2016). "Across US, Police Officers Abuse Confidential Databases." *AP News*. Available at: https://apnews.com/article/699236946e3140659fff8a2362e16f43; Andrea Peterson. (2013). "LOVEINT: When NSA Officers Use their Spying Power on Love Interests." *The Washington Post.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/; Catharine Tunney. (2020). "Personal Information Belonging to 144,000 Canadians Breached by Federal Departments and Agencies." *CBC News*. Available at: https://www.cbc.ca/news/politics/privacy-breach-canada-1.5457502. Catharine Tunney. (2019). "RCMP Sent Confidential Details of Suicide Attempt to Wrong Email Chain: Report." *CBC News*. Available at: https://www.cbc.ca/news/politics/rcmp-privacy-breach-suicide-1.5203645.

4 Dean Beeby. (2017). "Massive Privacy Breach at Public Services Reveals Workers' Salaries." *CBC News*. Available at: https://www.cbc.ca/news/politics/privacy-breach-therrien-public-services-procurement-spreadsheet-personal-workers-1.4141297; Employment and Social Development Canada. (2018). "Canada Student Loans Privacy Breach Class Action – Notice of Settlement Approval." *Government of Canada*. Available at: https://www.canada.ca/en/employment-social-development/programs/canada-student-loans-grants/privacy-breach-notice.html; Heather Landi. (2021). "Fitbit, Apple User Data Exposed in Breach Impacting 61M Fitness Tracker Records." *Fierce Healthcare*. Available at: https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records.

very sensitive information was used to inform public health and policy responses to the COVID-19 pandemic and, should the *Consumer Privacy Protection Act* (CPPA) in Bill C-27 be passed into law, this sensitive information could be used for an expansive set of socially beneficial purposes to the potential detriment of individuals and their communities.

This report, "Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law," critically interrogates the federal government's use of mobility information over the course of the COVID-19 pandemic. In light of how information was used and critiques of that use, it assesses the proposed federal commercial privacy legislation that was introduced in 2022 and finds that it would authorize similar controversial data sharing. In particular, this report focuses on how this data sharing, under the auspice of a socially beneficial data sharing regime, could have significant negative impacts on individuals and communities that have their locational information obtained and used, without consent, by the federal government. Moreover, it could see private organizations collect and use mobility information without first obtaining prior consent under legitimate business exemptions, with the effect that such information might be used in ways individuals would oppose or disagree with. We offer a series of 19 amendments that are meant, in aggregate, to enhance the privacy protections provided to residents of Canada and their communities.

Part 1 of this report provides a background of key privacy issues that were linked to collecting mobility data during the COVID-19 pandemic. It pays specific attention to the implementation of new technologies to collect, use, and disclose data, such as those used for contact-tracing applications and that foreign governments used to collect mobility information from telecommunications carriers. We also attend to the concerns that are linked to collecting location information and why there is a consequent need to develop robust governance frameworks.

Part 2 focuses on how the federal government obtained and used mobility data from BlueDot and Telus over the course of the COVID-19 pandemic. This includes summarizing the meeting sessions of the Standing Committee on Access to Information, Privacy and Ethics (ETHI), which conducted a review of the collection of mobility data by the federal government in early 2022. We also identify key findings in the report ETHI published following its meetings.

Having outlined how mobility data can be and has been obtained and used by the federal government, **Part 3** shifts to assess the legality of these activities to conclude that the federal government and Telus and BlueDot likely complied with existing privacy law.

An assessment of the lawfulness of the disclosure of mobility data, however, raises a series of thematic deficiencies with Canada's existing federal privacy legislation as will be discussed in **Part 4**. Existing federal commercial privacy law has the following six deficiencies:

1. PIPEDA fails to adequately protect the privacy interests at stake with de-identified and aggregated data despite risks that are associated with re-identification.
2. PIPEDA lacks requirements that individuals be informed of how their data is de-identified or used for secondary purposes.
3. PIPEDA does not enable individuals or communities to substantively prevent harmful impacts of data sharing with the government.
4. PIPEDA lacks sufficient checks and balances to ensure that meaningful consent is obtained to collect, use, or disclose de-identified data.
5. PIPEDA does not account for Indigenous data sovereignty nor does it account for Indigenous sovereignty principles in the United Nations Declaration on the Rights of Indigenous Peoples, which has been adopted by Canada.
6. PIPEDA generally lacks sufficient enforcement mechanisms.

Part 5 analyzes relevant sections of the CPPA to ultimately argue that it does not address deficiencies in PIPEDA and, in fact, possesses a series of problems including:

- an absence of a strong rights-based framework
- an under-inclusive definition of de-identified information
- an introduction of overbroad exceptions to consent
- an absence of transparency and accountability requirements
- a lack of power provided to the Office of the Privacy Commissioner

Part 5 continues by proposing amendments that would ameliorate many of these weaknesses in the draft legislation.

If Bill C-27 is not amended, its impacts will be felt well after the COVID-19 pandemic has come to a close. It is already the case that access to certain forms of healthcare, including reproductive healthcare, is politicized in Canada. If the government is permitted to continue collecting geolocation information without the knowledge and meaningful consent of individuals, this information may be used to further stigmatize already marginalized communities as well as create the legal condition where geolocation information and other de-identified or aggregated information could be used in excess of socially beneficial health interventions. Moreover, private organizations may collect and use mobility information and use the legitimate interest exemption to

prevent individuals or communities from knowing about how these organizations are using this highly sensitive information. Remedying these prospective harms requires, at a minimum, restricting the conditions and terms under which private organizations can disclose sensitive information–be it de-identified or not–to government agencies as well as ensuring that individuals can at least know when private organizations are collecting or using this information to advance their business interests. Doing anything less runs the risk of structurally inscribing harm to vulnerable individuals and marginalized communities in Canada while the government and private organizations alike can assert that they are advancing so-called socially beneficial purposes, or using personal information in the pursuit of ostensibly legitimate business purposes.

1. Background

Historically, governments innovate and draw lessons in the face of novel emergencies such as health crises.[5] Key to these innovations are ways of collecting, using, and disclosing information to understand the spread of disease. In the Canadian context, the last time the federal and provincial governments dealt with a related health emergency was during the Severe Acute Respiratory Syndrome (SARS) outbreak in 2003.

A retroactive National Advisory Committee on SARS and Public Health recommended changes to public health governance and specifically found that the failure to provide information to the international community was the result of a lack of information sharing between federal and provincial governments. This failure occurred, in part, due to Canadian-specific constitutional and technological realities[6] and was not corrected between the issuance of the SARS report and discovery and spread of COVID-19.[7] Previously failing to collect and share relevant information historically in tandem with outlining how governments around the world were collecting mobility information to try and mitigate the transmission of COVID-19 sets the stage for how the federal government of Canada responded to the spread of COVID-19.

1.1. Contact Tracing

At the onset of the COVID-19 pandemic in 2020, many governments, including those of Australia, the US, the UK, Israel, Singapore, Saudi Arabia, Vietnam, New Zealand, and Canada, recognized that contact tracing could be essential to mitigating the spread of COVID-19.[8] However, traditional contact-tracing methods principally relied on health

---

5 This emphasis on the role of the state was reflected in the New York Court of Appeal's 1868 statement that argued that the state has "absolute control over persons and property, so far as the public health was concerned." See: J. F. Witt. (2020). *American Contagions.* Yale University Press at p. 82.

6 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada." *Government of Canada.* Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

7 Justin Ling. (2021). "Provinces are Working with Outdated Vaccine Tracking Systems, Hindering National Data." *The Globe and Mail.* Available at: https://www.theglobeandmail.com/canada/article-provinces-working-with-outdated-vaccine-tracking-systems/; Justin Ling. (2021). "Canada's Public Health Data Meltdown." Maclean's. Available at: https://www.macleans.ca/news/canada/canadas-public-health-data-meltdown/.

8 Dyani Lewis. (2020). "Why Many Countries Failed at COVID Contact-Tracing – But Some Got it Right." Nature. Available at: https://www.nature.com/articles/d41586-020-03518-4; Amnesty International. (2020). "Bahrain, Kuwait and Norway Contact Tracing Apps Among Most Dangerous for Privacy." *Amnesty International.* Available at: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/; James O'Connell. (2021). "Contact Tracing for COVID-19 – A Digital Inoculation against Future Pandemics." *New England Journal of Medicine.* Available at: https://www.nejm.org/doi/full/10.1056/NEJMp2102256; Marwah Hassounah, Hafsa Raheel, and Mohammad Alhefzi. (2020). "Digital Response During the COVID-19 Pandemic in Saudi

officials contacting affected individuals and, subsequently, those to whom they were proximate. This methodology did not scale well given the virulence of COVID-19.[9] In response, government officials and private technology companies developed and implemented semi-automated contact-tracing and exposure-notification technologies. These technologies relied on either tracking mobile phones or enabling smartphones to track other phones that were near to them using an always-on smartphone application.

Early contact-tracing applications used centralized technologies and often collected geolocation information. For example, Israel collected GPS information after their High Court ruled that the government's previous practice of relying on the Israel Security Agency, better known as Shin Bet, to track COVID-19 patients and their contacts severely violated Israelis' constitutional right to privacy.[10] Singapore's contact-tracing application, TraceTogether, required individuals to upload their entire contact log to a health-authority-administered server if they contracted the virus.[11] State media reported that refusing to share the app's data with the Ministry of Health could lead to prosecutions under the country's *Infectious Disease Act*.[12] The United Kingdom received criticism for its initial Test and Trace program that used a centralized contact-tracing mobile device application and also collected geolocation information to provide insight into the virus' spread.[13]

Arabia." *Journal of Medical Internet Research*. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7473704/; Ashkan Soltani, Ryan Calo and Carl Bergstrom. (2020). "Contact-tracing Apps are Not a Solution to the COVID-19 Crisis." *Brookings*. Available at: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/; L Ceci. (2021). "COVID-19 Contact Tracing App Adoption Rate 2020, by Country." *Statista*. Available at: https://www.statista.com/statistics/1134669/share-populations-adopted-covid-contact-tracing-apps-countries/.

9 Shawn Radclifee. (2020). "How Contact Tracing Can Help Stop COVID-19." *Healthline*. Available at: https://www.healthline.com/health-news/everything-to-know-about-contact-tracing; Susan Landau. (2021). People Count: Contact-tracing Apps and Public Health. MIT Press at p. 39; Samuel Altmann, Luke Milson, Hannah Zillessen et al. "Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study." *JMIR Mhealth Uhealth.* Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7458659/.

10 Tehilla Shwartz Altshuler and Rachel Aridor Hershkowitz. (2020). "How Israel's COVID-19 Mass Surveillance Operation Works." *Brookings*. Available at: https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/; Privacy International. (2020). "Israel's Coronavirus Surveillance is an Example for Others – Of What Not to Do." *Privacy International.* Available at: https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do.

11 Dongwoo Kim and Daniela Rodriguez. (2020). "There's an App for That: Use of COVID-19 Apps in Singapore and South Korea." *Asia Pacific Foundation of Canada*. Available at: https://www.asiapacific.ca/fr/publication/theres-app-use-covid-19-apps-singapore-and-south-korea; Singapore Government. (2021). "How Does TraceTogether Work?" *Trace Together.* Available at: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-TraceTogether-work-.

12 Grace Ho. (2021). "Critical need to rebuild the public's trust in TraceTogether". *The Straits Times.* Available at: https://web.archive.org/web/20210417083920/https://www.straitstimes.com/singapore/politics/critical-need-to-rebuild-the-publics-trust-in-tracetogether; Matthew Mohan. (2021). "Singapore Police Force can obtain TraceTogether data for criminal investigations: Desmond Tan". *CNA*. Available at: https://www.channelnewsasia.com/singapore/singapore-police-force-can-obtain-tracetogether-data-covid-19-384316; Philip Heijmans. (2021). "Singapore Police May Use Contact Tracing Data for Investigations." *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2021-01-04/singapore-police-may-use-contact-tracing-data-for-investigations.

13 James Ball. (2020). "The UK's contact tracing app fiasco is a master class in mismanagement." *MIT Technology Review.* Available at: https://www.technologyreview.com/2020/06/19/1004190/

Google and Apple developed a privacy-protective framework, the (Google/Apple) Exposure Notification (GAEN) framework, that governments could use to build applications designed for exposure notification.[14] The companies declined to make GPS functionality available in GAEN-enabled apps and instead relied on Bluetooth radios for phones to detect when they were proximate to one another.[15] The applications delivered notifications to smartphone owners under a narrow set of conditions. Namely,

1. The other person tested positive for COVID-19.
2. The other person also used the exposure-notification application.
3. The other person consented to sending an exposure alert to individuals with whom they were proximate while likely infected and contagious with COVID-19.[16]

The core benefit of GAEN-compatible apps to governments was that applications could run in the background and, thus, not incur security, usability, or battery problems that were associated with early-generation non-GAEN contact-tracing applications.[17] However, GAEN-compliant applications were less useful in generating geolocation information that might have been more broadly useful for contact-tracing efforts.[18]

In Canada, COVID Alert was designed using the GAEN framework. Individuals consented to its use by downloading the application and agreeing to its terms and conditions. The Office of the Privacy Commissioner of Canada (OPC) and Information and Privacy Commissioner of Ontario reviewed the application and found it to minimally intrude on individuals' privacy interests and noted that the risk of re-identification was low given the application's use of GAEN's privacy-preserving, decentralized technology.[19]

---

uk-covidcontact-tracing-app-fiasco/.

14 Apple. (2020). "Apple and Google Partner on COVID-19 Contact Tracing Technology." *Apple Newsroom.* Available at: https://www.apple.com/ca/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/; Google. (2020). "Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID–19." *Google*. Available at: https://www.google.com/covid19/exposurenotifications/.

15 Apple and Google. (2020). "Exposure Notifications: Frequently Asked Questions." *Apple*. Available at: https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf.

16 Google. (2020) "Exposure Notifications: Help slow the spread of COVID-19, with one step on your phone." *Google*. Available at: https://www.google.com/covid19/exposurenotifications/#grid-homepage-how-itworks.

17 Douglas Leith and Stephen Farrell. (2021). "Measurement-based evaluation of Google/Apple Exposure Notification API for proximity detection in a commuter bus." *Plos One*. Available at: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0250826.

18 Ryan Browne. (2020). "Why Coronavirus Contact-tracing Apps Aren't Yet the Game Changer Authorities Hoped They'd Be." *CNBC*. Available at: https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html; Shannon Bond. (2020). "Apple, Google Coronavirus Tool Won't Track Your Location. That Worries Some States." *NPR*. Available at: https://www.npr.org/2020/05/13/855064165/apple-google-coronavirus-tech-wont-track-your-location-that-worries-some-states.

19 Office of the Privacy Commissioner of Canada. (2020). "Privacy review of the COVID Alert exposure

Despite these assurances that the application preserved individual privacy and did not collect geolocational information, the application was downloaded only 6.9 million times.[20] According to a study in the *Canadian Journal of Public Health*, the application may have prevented 7,900 infections and 74 deaths from March to July of 2021, representing 1.6 to 2.9 percent of the total recorded infections in Canada during the time.[21] When the Digital Global Health & Humanitarianism Lab assessed the uptake and user engagement with contact-tracing and exposure-notification applications, they attributed their poor uptake to five major challenges, including, among others:

- fears of immediate and future surveillance
- privacy perceptions that may override privacy-by-design principles[22]
- poor perceptions of app effectiveness[23]

Ultimately, GAEN-compliant applications were built to avoid collecting precise geolocation or mobility information and to prevent governments from abusing the applications to illicitly monitor or coerce their populations. Even in the face of such protections, individuals regularly declined to install the applications and high rule-of-law countries were frustrated by the inability to collect more precise geolocation or mobility information about their residents from GAEN-compliant applications. In light of these limitations, some governments turned to obtaining mobility and geolocation information directly from telecommunications companies.

---

notification application." *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/. See also: Public Health Agency of Canada Privacy Management Division. (2021). "COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment." *Health Canada*. Available at: https://github.com/cds-snc/covid-alert-documentation/blob/main/COVIDAlertPrivacyAssessment.md; Office of the Privacy Commissioner of Canada. (2020). "Supporting Public Health, Building Public Trust: Privacy Principles for Contact Tracing and Similar Apps -- Joint Statement by Federal, Provincial and Territorial Privacy Commissioners." *Office of the Privacy Commissioner of Canada.* Available at: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

20 Jonathan Ore. (2022). "Where did Things go Wrong with Canada's COVID Alert App?" *CBC News*. Available at: https://www.cbc.ca/radio/costofliving/from-boycott-to-bust-we-talk-spotify-and-neil-young-and-take-a-look-at-covid-alert-app-1.6339708/where-did-things-go-wrong-with-canada-s-covid-alert-app-1.6342632; Tom Yun. (2022). "Why the COVID Alert App Never Took Off in Canada." *CTV News*. Available at: https://www.ctvnews.ca/health/coronavirus/why-the-covid-alert-app-never-took-off-in-canada-1.5951502.

21 Shuo Sun, Mairead Shaw, Erica EM Moodie, and Derek Ruths. (2022). "The Epidemiological Impact of the Canadian COVID Alert App." *Canadian Journal of Public Health*. Available at https://link.springer.com/article/10.17269/s41997-022-00632-w; Kerrisa Wilson. (2022). "COVID Alert app prevented 74 virus-related deaths in Ontario: study." *CTV News*. Available at: https://toronto.ctvnews.ca/covid-alert-app-prevented-74-virus-related-deaths-in-ontario-study-1.5984732.

22 For a summary of what constitutes Privacy by Design, see: Ann Cavoukian. (2011). "Privacy by Design: The 7 Foundational Principles–Implementation and Mapping of Fair Information Practices." *Information and Privacy Commissioner of Ontario*. Available at: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

23 Jennie Phillips, Petra Molnar, Rebecca Babcock, Tiana Putric, Dyllan Goldstein, Laksmiina Balasubsramaniam, Alisha Gauhar, and Sarah Quayyum. (2021). "Exploring User-Uptake of Digital Contact Tracing Apps - A Practitioner Guide." *Digital Global Health and Humanitarianism Lab.* Available at: https://figshare.com/articles/book/Exploring_User-Uptake_of_Digital_Contact_Tracing_Apps_-_A_Practitioner_Guide_-_Full/14423861.

1.2. Mobility Data Received from Telecommunications Companies

In addition to developing exposure-notification applications, some governments obtained mobility data from telecommunications companies. Mobility data refers broadly to location information that is derived from cellular networks as well as location information obtained by data brokers.[24] The UK government requested mobility information from telecommunications providers, such as O2 and EE, to enforce social-distancing regimes.[25] Swiss officials collected mobility data from Swisscom to determine compliance with social-distancing requirements.[26] Similar practices occurred in Austria, Belgium, Armenia, and the EU, among others.[27]

The Government of Canada also obtained mobility information. The Public Health Agency of Canada (PHAC) contracted with BlueDot and Telus' Data for Good program to obtain aggregate, de-identified data to support the government's "modelling and monitoring of the spread of COVID-19, and to inform government decision-making as the situation evolves."[28] Following the expiration of these contracts, PHAC posted a request for proposals in December of 2021 to continue receiving cell tower mobility data (the RFP).[29] This posting led the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) to hold committee sessions in the spring of 2022 to learn about the federal government's collection and use of mobility and geolocation information over the course of the pandemic. The Committee issued a report entitled "Collection and Use of Mobility Data by the Government of Canada and Related Issues" that concluded,

---

24 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons.* Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf.

25 Department of Health & Social Care. (2020). "Guidance: What the Coronavirus Bill will do." *Government of the United Kingdom.* Available at: https://www.gov.uk/government/publications/coronavirus-bill-what-it-will-do/what-the-coronavirus-bill-will-do.; Privacy International. (2020). "Telecommunications data and Covid-19." *Privacy International*. Available at: https://privacyinternational.org/examples/telecommunications-data-and-covid-19. Research and Information Service. (2020). "Briefing Paper: The Use Of Digital Measures To Combat COVID-19." *Northern Ireland Assembly*. Available at: http://www.niassembly.gov.uk/globalassets/documents/raise/publications/2017-2022/2020/health/2320.pdf. p. 26.

26 Swiss Info. (2020). " Mobile Phone Data Show Swiss Are Keeping Their Distance." *Swiss Info.* Available at: https://www.swissinfo.ch/eng/coronavirus_mobile-phone-data-show-swiss-are-keeping-their-distance-/45644704.

27 Human Rights Watch. (2020). "Mobile Location Data and COVID-19: Q&A." *Human Rights Watch*. Available at: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

28 Prime Minister's Office. (2020). "Canada's Plan to Mobilize Science to Fight COVID-19." *Government of Canada*. Available at: https://pm.gc.ca/en/news/news-releases/2020/03/23/canadas-plan-mobilize-science-fight-covid-19.

29 Public Services and Procurement Canada. Tender Notice (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada*. Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277.

amongst other things, that federal privacy legislation had to be modernized to meet the challenges of a highly digital society.[30]

1.3. Risks and Concerns Associated with Location Information

Governments' collection of mobility data raises human rights and civil liberties concerns because of the data's sensitivity and because the data might be used in excess of equitable and proportional responses to a given policy issue, such as responding to the COVID-19 pandemic. Mobility data can reveal sensitive details of the lifestyle and personal choices of the individual.[31] Such revelations occur when data sets explicitly contain identifiable information, linking movement to specific individuals. Even when personal information has been de-identified or aggregated, it can be possible to re-identify individuals by way of drawing inferences or correlations from the data or by overlaying it with known personal information. Notably, few individuals in highly-industrialized societies can genuinely opt-out of such data collection because mobile phones are essential to everyday life—both personally and professionally—and the applications installed on them voraciously collect location information.

To demonstrate the sensitivity of mobility data and the risk of re-identification, the *New York Times* conducted a study in which they re-identified a de-identified data set and tracked the movement of one individual.[32] Her mobility data revealed trips to Planned Parenthood and the length of those visits. Other studies have showcased that relatively few data points are required to re-identify deliberately de-identified data.[33] For example,

30 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

31 Mike Swift. (2021). "Sensitivity of Mobility Data Sparks Creation of Privacy Asssessment Tool by Think Tank, Standards Group." *MLex*. Available at: https://mlexmarketinsight.com/news/insight/sensitivity-of-mobility-data-sparks-creation-of-privacy-assessment-tool-by-think-tank-standards-group; Alexandra Kapp. (2022). "How is Mobility Data Sensitive Information?" *Alendara Kapp*. Available at: https://alexandrakapp.blog/2022/04/25/how-is-mobility-data-sensitive-information/; Rob Matheson. (2018). "The Privacy Risks of Comiling Mobility Data." *MIT News*. Available at: https://news.mit.edu/2018/privacy-risks-mobility-data-1207; GovLab, Cuebiq, Open Data Institute. (2021). "The Use of Mobility Data for Responding to the COVID-19 Pandemic." *ODI*. Available at: http://theodi.org/wp-content/uploads/2021/03/Data4COVID19_0318.pdf; Mohamed Maouche, Sonia Ben Mokhtar, Sara Bouchenak. (2018). "HMC: Robust Privacy Protection of Mobility Data against Multiple Re-Identification Attacks." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2018, 2 (3), pp.1-25.

32 Richard Harris. (2018). "Your Apps Know What You Did Last Night and They're Not Keeping It to Themselves." *New York Times*. Available at: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

33 Ali Farzanehfar, Florimond Houssiau, and Yves-Alexandre de Montjoye. (2021). "The Risk of Re-identification Remains High Even in Country-Scale Location Datasets." *Patterns*. Available at: https://www.sciencedirect.com/science/article/pii/S2666389921000143; Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen and Vincent D Blondel. (2013). "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports*. Available at: https://www.nature.com/articles/srep01376; Yang Xu, Alexander Belyi, Iva Bojic and Carlo Ratti. (2018). "Human Mobility and Socioeconomic Status: Analysis of Singapore and Boston." *Computers, Environment and Urban Systems*. Available at: https://www.sciencedirect.com/science/article/pii/S0198971517304179.

re-identifying de-identified data has revealed movements of national security officials in the United States[34] and has exposed the physical location of gay men who use online dating applications.[35]

Mobility information can be used by government agencies to advance a range of policies, including assessing the efficacy of social-distancing recommendations during the COVID-19 pandemic, determining which parts of a population are more likely to avail themselves of reproductive health facilities, or identifying individuals who may have been proximate to reported criminal activities. Unlike private individuals and companies that can discriminate against individuals, the state can coercively use information it collects or develop policies or programs using mobility information that compel changes in how individuals or communities are treated by the state or parties regulated by the state. There is, in short, a qualitative difference in how states can potentially use mobility information as compared to private organizations.

1.4. Governance

The collection, use, and disclosure of personal information, including that linked with mobility information, is governed by data protection and privacy legislation. In Canada, this is governed by federal as well as provincial legislative instruments. The *Privacy Act*, which came into force in 1983, governs how the federal government manages personal information.[36] Its sister legislation, the *Personal Information and Protection of Electronic Documents Act* (PIPEDA), came into force in 2001 and governs federally regulated private organizations.[37] Both pieces of legislation precede the contemporary digital era. Calls for reforming both laws have been made by civil society, privacy law experts, and most recently, the Standing Committee on Access to Information, Privacy and Ethics in their review of the collection and use of mobility data by PHAC. As of writing, the federal government has introduced the *Consumer Privacy Protection Act* to replace PIPEDA, as

34 National Security Agency. (2020). "Limiting Location Data Exposure." *National Security Agency*. Available at: https://media.defense.gov/2020/Aug/04/2002469874/-1/-/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF; Justin Sherman. (2022). "The Open Data Market and Risks to National Security." *Lawfare*. Available at: https://www.lawfareblog.com/open-data-market-and-risks-national-security; Craig Timberg. (2014). "For Sale: Systems that Can Secretly Track Where Cellphone Users Go Around the Globe." *The Washington Post.* Available at: https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html; Samuel Gibbs. (2016). "US Congressman Calls for Investigation into Vulnerability that Lets Hackers Spy on Every Phone." *The Guardian*. Available at: https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping.

35 Brian Latimer. (2018). "Grindr Security Flaw Exposes Users' Location Data." *NBC News.* Available at: https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446.

36 See: *Privacy Act*, RSC 1985, c P-21.

37 See: *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

will be discussed in Part 5 of this report.[38] There is no legislation before the House at the time of writing to reform or replace the *Privacy Act*.

38 See: Bill C-27, "An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts" *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

2. The Collection of Mobility Data and ETHI Committee Findings

The Government of Canada issues a range of seemingly contradictory statements concerning its interest in and use of mobility information during the COVID-19 pandemic. The government initially suggested an interest in using this information to inform pandemic responses. It then appeared to avoid a strong commitment to obtain such data; however, it simultaneously worked to assuage privacy concerns that were associated with government data collection by emphasizing the privacy-protective nature of the COVID Alert application. While these public discussions and debates were taking place, the federal government quietly entered into agreements with BlueDot and Telus to obtain mobility data to inform government health policies.

Part 2 outlines how the federal government collected mobility information. In particular, it denotes the timeline of collection, explains the operations of Telus and BlueDot, and summarizes the content of the Standing Committee on Access to Information, Privacy and Ethics (ETHI) Committee's hearings and its corresponding report.

2.1. BlueDot and Telus' Data for Good Program

The federal government entered into contracts with two private companies, BlueDot and Telus, to obtain mobility information at the outset of the COVID-19 pandemic. The contract between PHAC and BlueDot was signed on April 24, 2020, and was backdated to start as of March 26, 2020.[39] In the case of Telus, on April 21, 2020, the Innovation, Science and Economic Development's (ISED) Communications Research Center (CRC) informed the Office of the Privacy Commissioner of Canada (OPC) that it planned to access mobility data from Telus.[40] Later that year, on December 24, 2020, PHAC contracted with Telus to obtain de-identified information through Telus' Data for Good program; this contract expired in October 2021, which led PHAC to post the RFP in December 2021 to continue receiving cell tower mobility data.[41] The RFP was amended on February 4,

39 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

40 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

41 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769; Public Services and Procurement Canada. Tender Notice. (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada.* Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277.

2022, to postpone the closing date of the tender to February 18, 2022.[42]

BlueDot purchased application data from third-party providers, and this data included mobility information.[43] The applications that collected mobility information required express consent from users, and the location data was de-identified prior to being provided to BlueDot.[44] BlueDot stated that it ensured that organizations they worked with adhered to Canadian privacy practices both by receiving assurances from said organizations and conducting their own due diligence.[45] Throughout the Committee meetings, however, no further information was provided with regard to BlueDot's diligence practices or the specific nature of the assurances received.

Telus launched its Data for Good program at the outset of the COVID-19 pandemic.[46] The purpose of the program was, in part, to aggregate and de-identify its customers' network mobility data[47] and then make it available to third parties, such as "researchers and data scientists acting for governments, health authorities, or academic institutions" to advance "socially beneficial purposes."[48] In developing the Data for Good program, Telus worked with de-identification experts and consulted with the OPC.[49]

The network mobility data in Telus' Data for Good program was derived from its subscribers' physical movements and collected in the course of providing mobile phone service to its subscribers. The collection of such information was discussed in Telus' privacy commitment for network management purposes.[50] The Data for Good program

---

42 Public Services and Procurement Canada. Tender Notice. (2021). "Amendment - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada.* Available at: https://buyandsell.gc.ca/cds/public/2022/02/04/5ba4b48a559dd61873987a9f95d818b2/rfp_amendment_2.pdf.

43 Kamren Khan, ETHI Hearing dated February 17, 2022.

44 Kamren Khan, ETHI Hearing dated February 17, 2022.

45 Kamren Khan, ETHI Hearing dated February 17, 2022.

46 Telus. (2020). "TELUS Program Receives Prestigious Global Privacy Recognition." *Telus*. Available at: https://www.globenewswire.com/news-release/2020/11/23/2132133/0/en/TELUS-program-receives-prestigious-global-privacy-recognition.html; TELUS. (Undated). "Data for Good Commitments." *Telus*. Available at: https://www.telus.com/en/about/privacy/data-for-good/commitments.

47 Telus. (Undated). "Telus About: Technology is Evolving and So Are We." *Telus*. Available at: https://www.telus.com/en/about/privacy/data-analytics.

48 Telus. (Undated). "Data for Good Commitments." *Telusa*. Available at: https://www.telus.com/en/about/privacy/data-for-good/commitments.

49 "If you are a TELUS customer, TELUS has some basic information about you. We understand that some of this information is private, which is why we collect personal information only for the following purposes … To manage and develop our business and operations. **For example, we analyze customer usage of our networks and facilities to help us manage them efficiently and plan for future growth**." Telus. (2014). "Our privacy commitment to you," *Telus*. Available at: https://static.telus.com/common/cms/files/get-help/privacy-policy/TELUS_Privacy_Commitment_En.pdf. Emphasis not in original. See also: Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022.

50 Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022. "The data that this is based off of at the point of collection is collected in the course of providing mobility services, so that consent is applied

used the same data for more extensive purposes than just network management insofar as it could be disclosed to researchers to facilitate health or economic research as well as to "commercial entities or innovators who are developing solutions, products or services designed for social good."[51] Telus' Vice-President and Chief Data and Trust Officer, Pamela Snively, noted that "if we were selling customers' personal information, it would require a separate and very expressed consent. We are not selling customers' personal information. We're not sharing customers' personal information."[52] Telus' website stated that it reserved the right to "determine whether to charge for such data sharing" and the company did not restrict itself to operating on a fee-recovery model.[53]

Telus subscribers could, at the time of writing, opt-out of the Data for Good program. However, experts, including the Privacy Commissioner of Canada, testified that finding the opt-out option was difficult.[54] Further, subscribers of Telus' Koodo Mobile and Public Mobile flanker brands, which are subsidiaries of Telus, also have their data collected for the Data for Good program. At committee, Ms. Snively stated that the privacy programs for these subsidiary brands are the same as for Telus subscribers, and communications have been similar.[55] However, as of August 3, 2022, Koodo Mobile still lacked any explicit reference to Telus' Data For Good program.[56] The closest the organization came to discussing that subscriber information might be used in the Data for Good program is when it wrote that, "we may de-identify certain network usage or location data for long term planning where individual customers' personal information is not required. We may also de-identify information prior to conducting analytics that don't require personal information."[57] Moreover, Koodo offered only a roundabout way to opt-out of data collection. The company's privacy policy informed subscribers they could visit Telus' website, navigate to part of Telus' privacy center that discussed data analytics, click a link under that heading, then navigate to the end of the page to finally click an opt-out link. Only

to its use for mobility services and to provide mobility services; however, when we de-identified the data, it was no longer personal information about our customers. Rather than relying on consent there, what we relied upon was ensuring that we had de-identified it. Our focus was to ensure that we had protected our customers' privacy and that we were transparent and clear about our use of that data."

51 Telus. (Undated). "Data For Good: Commitments." *Telus*. Available at: https://www.telus.com/en/about/privacy/data-for-good/commitments.

52 Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022.

53 Telus. (Undated). "Data For Good: Commitments." Telus. Available at: https://www.telus.com/en/about/privacy/data-for-good/commitments.

54 Daniel Therrien. (2022). ETHI Hearing, dated February 7, 2022; Martin French. (2022). ETHI Hearing, dated February 10, 2022.

55 Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022.

56 Koodo. (Undated). "Our Privacy Commitment to You." *Koodo Mobile.* Available at: https://www.koodomobile.com/privacy.

57 Koodo. (2017). "Our privacy commitment to you." *Koodo Mobile.* Available at: https://www.koodomobile.com/privacy.

at this point could Koodo Mobile subscribers opt-out of the data collection.[58] The statement that individuals could opt-out, however, was based on the privacy policy that was effective as of October 1, 2017, which significantly predated the launch of Telus' Data for Good program in early 2020.

In the case of Telus' other flanker brand, Public Mobile, its privacy policy extensively detailed how aggregated and de-identified mobility information might be used to "help governments and businesses make important decisions based on facts, not assumptions."[59] The policy was dated in 2018 and included an opt-out to Telus' Insights program, which is associated with the Data for Good program. Notably, it was only when accessing the .pdf version of the Telus privacy policy—as opposed to the policy summary first presented to visitors of Public Mobile's privacy policy landing page—that readers learned, on page 7, that "[u]nless you tell us otherwise, we will assume that we have your consent to continue to collect, use and disclose your personal information for the purposes we have identified to you."[60]

2.2. The Standing Committee on Access to Information, Privacy and Ethics Committee Meetings

The collection and disclosure of mobility information was the focus of a parliamentary study from January to May 2022. The ETHI Committee initiated the study following the revelation of the RFP to continue receiving cell tower mobility data.[61] The Committee heard from 20 witnesses, received 3 briefs, and asked questions of witnesses, as well as spoke amongst themselves about the topic in public and in-camera sessions.[62]

Over the course of the study, the Committee learned about issues associated with how the federal government collected, communicated about, and potentially used the mobility information from BlueDot and Telus. Some of the key issues that arose include the following items:

---

58 Koodo. (2017). "Our privacy commitment to you." *Koodo Mobile*. Available at: https://www.koodomobile.com/privacy.

59 Public Mobile. (2018). "Our privacy commitment to you." *Public Mobile.* Available at: https://www.publicmobile.ca/en/on/privacy-policy.

60 Public Mobile. (2018). "Our privacy commitment to you," *Public Mobile.* Available at: https://assets.ctfassets.net/g0l02radjx86/7fa0YlnX12PBE9hAjK5IBx/166cd81b34191f2761e38e96b3f32d46/PublicMobile_PrivacyCommitment_EN.PDF.

61 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769; Public Services and Procurement Canada. Tender Notice. (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada.* Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277.

62 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

- a lack of communication with the public about the collection of mobility data that inhibited members of the public from opting-out of the information collection
- a failure to adequately consult with the Privacy Commissioner
- a lack of transparency and accountability in ensuring that individuals had consented to the sharing of their mobility data
- an insufficiently stated purpose for collecting and retaining mobility data

These issues are discussed at length in parts 2.2.1 to 2.2.5.

2.2.1. Unclear Public Communication

On March 11, 2020, the World Health Organization declared COVID-19 a pandemic, and on March 23, 2020, the Prime Minister's Office announced that PHAC would use BlueDot's disease analytics platform to support modeling and monitoring of the spread of COVID-19 and to inform government decision making as the situation evolved.[63] No specific information, including no disclosure that the government was receiving de-identified mobility data from BlueDot, was provided about the dimensions of the partnership. The next day, the Privacy Management Division (PMD) of Health Canada and PHAC indicated that there were no privacy concerns regarding the data from BlueDot because it had been anonymized and irrevocably stripped of all identifiers; no code existed to enable future relinkage, and risk of re-identifying individuals was considered to be very low.[64] This analysis led the government to conclude that it was not receiving personal information—defined as information about an identifiable individual that is recorded in any form—from BlueDot.

There was also muddled communication concerning the Telus contract and the collection of telecommunications data generally. On March 23, 2020, Toronto mayor, John Tory, stated that the City of Toronto had access to telecommunications mobility data[65] though the City subsequently repudiated the statement.[66] The next day, March 24, 2020,

63 Prime Minister's Office. (2020). "Canada's Plan to Mobilize Science to Fight COVID-19." *Government of Canada.* Available at: https://pm.gc.ca/en/news/news-releases/2020/03/23/canadas-plan-mobilize-science-fight-covid-19.

64 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

65 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons.* Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf; Catharine Tunney. (2020). "Trudeau Leaves Door Open to Using Smartphone Data to Track Canadians' Compliance with Pandemic Rules." *CBC News*. Available at: https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236.

66 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons*. Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf.

Prime Minister Trudeau addressed whether the government would seek information from telecommunications providers and stated that, "as far as I know that is not a situation we're looking at right now."[67] That same day, Chief Public Health Officer, Dr. Teresa Tam, indicated that the option of using telecommunications mobility data should not be ruled out.[68] About a month later, on April 21, 2020, ISED's CRC informed the OPC that it planned to access de-identified mobility data from Telus to answer questions for PHAC about Canadians' mobility trends.[69] Subsequently, on April 22, 2020, PHAC informed the OPC that they did not believe that working with aggregated and de-identified mobility information engaged the *Privacy Act*.[70] This was confirmed by the PMD in late September.[71]

Between April and September of 2020, there were no public announcements concerning the federal government's use of mobility data, and in fact, it was during this time that the government emphasized the privacy-protective and location-agnostic nature of its exposure notification application, COVID Alert (discussed previously, in Part 1.1). The Minister of Health did state to ETHI that a federal government website, COVIDTrends, disclosed to Canadians that the government was using mobility information.[72] When we used the Internet Archive's Wayback Machine, however, it became apparent that this information appeared on the website as of December 6, 2020.[73]

2.2.2. Failure to Consult with the Privacy Commissioner of Canada

After hearing from the PHAC's PMD and ISED's CRC that they believed that privacy legislation was not applicable, given the nature of the information, the OPC stated that it would need to enter a formal advisory engagement with the CRC to determine if adequate safeguards had been adopted and whether the OPC's Framework to Assess

67 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons.* Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf.

68 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons.* Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf.

69 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

70 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

71 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

72 Minister Jean-Yves Duclos. (2022). ETHI Hearing, dated February 3, 2022.

73 Christopher Parsons. (2022). "Standing Committee on Access to Information, Privacy and Ethics: Study on Collection and Use of Mobility Data by the Government of Canada." *House of Commons*. Available at: https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11590677/br-external/ParsonsChristopher-e.pdf.

Privacy-Impactful Initiatives in Response to COVID-19 had been adhered to.[74] The CRC declined to pursue this process.[75]

According to Commissioner Daniel Therrien, when the OPC is engaged about an issue, it can receive detailed information about data flows and associated privacy and security protections. Once it is engaged, the OPC can move to assert that it has "looked under the hood" of a given program.[76] While the Commissioner was informed of the federal government's use of mobility information, he was not *engaged* by PHAC or the CRC, with the effect that the OPC could not certify PHAC's or CRC's assertions about the privacy or security of the mobility information in question.

The failure of agencies that received mobility information to engage the OPC raised a red flag to some experts who appeared before the ETHI Committee. Former Ontario Privacy Commissioner, Ann Cavoukian, stated: "if I wasn't consulted, I would be extremely concerned. I can't imagine why they didn't consult [...] it makes no sense to me."[77] Earlier in the meetings, Dr. Cavoukian said that the role of the Privacy Commissioner was to "trust but verify and, nowadays don't even trust."[78] Verification works to ensure that agencies are compliant with federal law and that appropriate privacy-preserving and security-enhancing mechanisms have been adopted.[79]

Minister Duclos referenced biweekly meetings that were held with the Privacy Commissioner to discuss the collection of mobility data when he was before the ETHI committee.[80] However, Commissioner Therrien noted that these meetings were held to discuss "various measures related to COVID and their impact on privacy" and did not exclusively focus on the collection of mobility data.[81] Finally, there was no formal advisory relationship between the OPC and the federal government with respect to the collection of mobility data.[82]

---

74 See: Office of the Privacy Commissioner of Canada. (2020). "A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19." *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/.

75 Office of the Privacy Commissioner of Canada. (2020). "Letter to the Standing Committee on Access to Information, Privacy and Ethics on their Study of the Collection and Use of Mobility Data by the Government of Canada." *Office of the Privacy Commissioner of Canada*. Available at: https://priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_sub_220301/.

76 Daniel Therrien. (2022). ETHI Hearing, dated February 7, 2022.

77 Ann Cavoukian. (2022). ETHI Hearing, dated February 10, 2022.

78 Ann Cavoukian. (2022). ETHI Hearing, dated February 10, 2022.

79 Ann Cavoukian. (2022). ETHI Hearing, dated February 10, 2022.

80 Minister Jean-Yves Duclos. (2022). ETHI Hearing, dated February 3, 2022.

81 Daniel Therrien. (2022). ETHI Hearing, dated February 7, 2022.

82 Daniel Therrien. (2022). ETHI Hearing, dated February 7, 2022.

2.2.3. Verification of Consent Was Not Obtained

BlueDot's employees who appeared before the ETHI Committee stated that they obtained mobility information from third-party providers.[83] While they noted that assurances were obtained from these providers and due diligence was conducted to ensure consent was in fact obtained, they at no point discussed the nature of the assurances or due diligence mechanisms while at Committee.[84]

Telus, in contrast, saw its Chief Data and Trust Officer state that the company obtained consent from customers to collect the mobile devices' mobility information as part of individuals signing up for Telus' mobile services.[85] Further, she asserted that this consent was transitive, meaning she believed that it enabled Telus to use collected information not just for network management or security functionalities but for other business activities, including their Data for Good program.[86]

When Kathy Thompson, Executive Vice-President of PHAC, was asked at the ETHI Committee about how PHAC protected the privacy of Canadian data in this collection, she stated that PHAC "put forward a number of requirements to protect the privacy of Canadians" with respect to the contracts with Telus and BlueDot as well as the RFP.[87] However, at no time during the Committee's public meetings was there a broader discussion of these requirements or whether they adequately addressed individual consent. Moreover, despite being repeatedly asked about whether valid user consent was obtained, Minister Duclos did not discuss what specific steps had been taken to ensure user consent.

2.2.4. Broad Purposes for Data Collection Can Lead to Problematic Uses of Data

As of writing and based on public records, Minister Duclos and Dr. Tam stated that mobility data was used for the following purposes:

1. To monitor the trajectory of the pandemic
2. To determine how the public responds to public health directives, and thus, determine the effectiveness of public health measures
3. To guide pandemic response
4. To provide outbreak information in specific locations[88]

Dr. Tam and Minister Duclos indicated that they had used or hoped to use mobility data to determine the effectiveness of public health directives by federal, provincial, and

83 Alex DeMarsh. (2022). ETHI Hearing, dated February 17, 2022.

84 Kamren Khan. (2022). ETHI Hearing, dated February 17, 2022.

85 Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022.

86 Pamela Snively. (2022). ETHI Hearing, dated February 17, 2022.

87 Kathy Thompson. (2022). ETHI Hearing, dated February 3, 2022.

88 Teresa Tam. (2022). ETHI Hearing, dated February 3, 2022.

territorial governments.[89] Provincially, governments implemented policies to reduce the population's mobility, with Ontario going so far as to empower police officers to fulfill these policies.[90] Using mobility information, the federal government could have, in theory, provided information or policy advice to relevant provincial and municipal governments so they could target enforcement actions at communities with higher-than-average mobility scores. There is no evidence that the government disclosed information for this purpose, nor that receiving governments used information for these ends.

When Professor Martin French was before the ETHI Committee, he discussed the risk that the government's envisioned uses of mobility information could disproportionately affect low-income workers that travel significant distances to get to their places of work.[91] Here, we see a theoretical situation in which using de-identified information for a widely perceived socially beneficial good—to, in this example, address a public health emergency—could disproportionately affect communities that are often significantly populated by racialized people who are already systematically discriminated against by government agencies, including law enforcement agencies.[92]

In the now-expired tender for cell-tower data, which was responsible for publicizing the federal government's use of mobility information in the first place, Health Canada wrote that PHAC "requires access to cell-tower/operator location data [...] to assist in the response to the COVID-19 pandemic **and for other public health applications**."[93] It went on to say that:

> [a]ggregated indicators derived from cell-tower/operator location data provide insightful information and allow for meaningful analysis on the mobility (or movement) of populations in Canada. These analyses and findings provide situational awareness and help inform policy, public health messaging, evaluation of public health measures, and **other aspects related to public health response, programming, planning and preparedness**.[94]

The contract was to last until May 31, 2023.[95]

---

89 Teresa Tam. (2022). ETHI Hearing, dated February 3, 2022.

90 Office of the Premier. (2021). "Ontario Strengthens Enforcement of Stay-at-Home Order." Available at: https://news.ontario.ca/en/release/61192/ontario-strengthens-enforcement-of-stay-at-home-order.

91 Martin French. (2022). ETHI Hearing, dated February 10, 2022.

92 Martin French. (2022). ETHI Hearing, dated February 10, 2022.

93 Public Services and Procurement Canada. Tender Notice (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada.* Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277. Emphasis not in original.

94 Public Services and Procurement Canada. Tender Notice (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada.* Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277. Emphasis not in original.

95 Public Services and Procurement Canada. Tender Notice (2021). "Tender Notice - Request for Proposal - Operator-Based Location Data and Services for Public Health Mobility Analysis." *Government of Canada*. Available at: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277.

Broadly, then, PHAC could have used mobility information it obtained following the completion of the RFP to undertake any activity that was coherent with PHAC's broad mandate. That mandate is to:

- promote health
- prevent and control chronic diseases and injuries
- prevent and control infectious diseases
- prepare for and respond to public health emergencies
- serve as a central point for sharing Canada's expertise with the rest of the world
- apply international research and development to Canada's public health programs
- strengthen intergovernmental collaboration on public health and facilitate national approaches to public health policy and planning[96]

While contractual terms may have delimited how PHAC could use information that it had previously obtained from BlueDot or Telus, the proposed tender was more expansive in nature. Specifically, PHAC was making it clear that its use of information might be used in excess of developing policies linked with the COVID-19 pandemic. This use could have included designing policies that collect information about Indigenous communities in order to advance policies to promote health without having first certified that meaningful consent had been obtained to collect mobility information. That information could then be transferred in an aggregated fashion for the federal government to use.

2.2.5. Retention Timeline is Unclear

It remains unclear from public records how long the federal government was authorized to retain or use the mobility information it obtained. During the ETHI meetings, public health authorities stated that they needed to obtain mobility information beyond the time period of the COVID-19 pandemic, but at the same time, they were uncertain how they might use the data. Dr. Tam noted that they would learn from how other governments used collected data to develop new ways of enhancing public health.[97]

One Committee member, Mr. René Villemure, raised concerns about how long mobility information would be retained by the federal government. Even should data be retained only until the end of the pandemic, he worried about the potential subjectivity of the timeline given uncertainty about when the pandemic would be considered over and who would be responsible for deciding to terminate the data collection in question.[98]

96 Government of Canada. (2021). "Public Health Agency of Canada - About the Agency." *Government of Canada*. Available at: https://www.canada.ca/en/public-health/corporate/mandate/about-agency.html.

97 Teresa Tam. (2022). ETHI Hearing, dated February 3, 2022.

98 Rene Villemure. (2022). ETHI Hearing, dated February 3, 2022.

2.3. The ETHI Study Recommendations

ETHI published their "Collection and Use of Mobility Data by the Government of Canada and Related Issues" report on April 28, 2022.[99] The report discussed the collection of mobility data by PHAC and Health Canada, made 22 recommendations for the collection of mobility data specifically and privacy law reform generally, and raised a series of concerns associated with the collection of mobility data. The following concerns were included:

- the lack of governance over de-identified data
- the use of data for socially beneficial purposes
- adapting legislation to the digital age
- the potential social impacts of mass data collection and surveillance[100]

The report's recommendations were directed toward the government's collection of mobility data and associated privacy law reforms. These recommendations are summarized in Appendix B.

99 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons*. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

100 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

3. Contemporary Federal Privacy Law and Mobility Information

Federal privacy law in Canada is bifurcated. The *Privacy Act* governs public agents' collection, use, and disclosure of personal information whereas the *Personal Information and Protection of Electronic Documents Act* (PIPEDA) governs the same for federally regulated private sector organizations.[101] Part 3 assesses the privacy interest in location information to determine the extent to which PIPEDA applies to the disclosure of aggregated and de-identified mobility data by Telus and BlueDot and evaluates whether the *Privacy Act* applies to the collection of the same type of mobility data by the federal government. We ultimately find that the current laws governing the collection of mobility information by private organizations and the subsequent disclosure of de-identified and aggregated locational information to federal government organizations reveal governance gaps that should be remedied through privacy law reform.

3.1. Privacy Rights and Mobility Data

Mobility information has the potential to be deeply revelatory about an individual's personal life or the activities undertaken by members of their community, such as the regularity at which parties visit health care facilities, obtain mental health services, sleep away from home (perhaps indicating an affair or other romantic relationships), visit adult entertainment clubs, attend religious services, or frequent paycheque advance businesses. This kind of data, itself, can, per the Supreme Court of Canada in *R v Tessling*, be designated as either informational or territorial. Informational and territorial data is central to one's biographical core as it connects bodily integrity to informational privacy.[102] When courts have applied privacy legislation and the constitutional right to privacy, they have found that individuals have a reasonable expectation of privacy in their cellphone records, including geospatial location data derived from cellphone companies,[103] largely because of the sensitivity of this data. Further and per *R v Spencer*, the right of anonymity can be impaired when or if government agencies obtain detailed mobility information. Even where information is de-identified, *Spencer* found that when information could be re-associated with an individual, such as by way of using legal powers, then privacy interests in the information remained.[104]

---

101 Some provinces have their own private sector legislation, which has been deemed to be substantially similar to PIPEDA, such as the Alberta Personal Information Protection Act, British Columbia's Personal Information Protection Act and Quebec's Act Respecting the Protection of Personal Information in the Private Sector, recently updated with the passing of Bill 64, the Act to Modernize Legislative Provisions respecting the Protection of Personal Information.

102 *R v Tessling*, 2004 SCC 67 at para 21-23.

103 *R v Rogers Communications Partnership*, 2016 ONSC 70 at para 31.

104 *R v Spencer*, 2014 SCC 43 at para 38.

Information Box 1: Canadian Privacy Interests Recognized by Law

Canadians have a quasi-constitutional privacy interest in their personal information. This interest is inclusive of location and information data. Canadian courts have determined that individuals may have a reasonable expectation of privacy concerning a given piece of information based upon multiple factors, including the biographical core analysis. Personal information that tends to reveal intimate details of the lifestyle and personal choices of the individual are essential to one's biographical core and are deemed necessary to protect.[105] There is also a need to balance the competing demands of the community's desire for privacy as well as its insistence on protection by the government.[106] The court in *Tessling* went so far as to identify three categories of privacy interests:

1. personal/bodily
2. territorial
3. informational[107]

As well, the court in *Spencer* considered three distinct and overlapping understandings of informational privacy, one of which included privacy as anonymity.[108]

It is imperative that the drafters of privacy legislation understand and incorporate the lessons from the court to protect human rights.

3.1. The Law Governing the Sharing of Aggregated and De-Identified Mobility Data

Telus' mobility information was originally identifiable but was transformed into aggregated and de-identified information before being provided to the federal government. BlueDot, in contrast, received de-identified location data from third-party providers.[109] The information the federal government received from either company was aggregated and de-identified. Both the *Privacy Act* and *PIPEDA* govern the collection, use, and disclosure of personal information, defined as information about an identifiable individual.[110]

3.1.1. PHAC's Collection of Information and the Application of the *Privacy Act*

The *Privacy Act* is intended to let individuals access personal information about themselves that is held by a federal government institution and to provide the right to

105 *R v Plant*, [1993] 3 S.C.R. 281at para 27.

106 *R v Tessling*, 2004 SCC 67 at para 17.

107 *R v Tessling*, 2004 SCC 67 at para 24.

108 *R v Spencer*, 2014 SCC 43 at para 38.

109 Kamren Khan. (2022). ETHI Hearing, dated February 17, 2022.

110 See: *Privacy Act*, RSC 1985, c P-21, s 3; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 2.

correct information about themselves and place boundaries on how, when, and under which circumstances the government can collect, use, or share individuals' personal information.[111] In the circumstances under discussion, PHAC and the CRC are federal government institutions that collected de-identified mobility data from Telus and BlueDot and sought to continue collecting such information as demonstrated through a RFP, which expired on February 18, 2022.

In this context, does the de-identified mobility data that was collected from companies engaged in commercial activity constitute personal information within the meaning of the *Privacy Act*?

Per s. 3 of the *Privacy Act*, personal information is information about an identifiable individual that is recorded in any form.[112] Courts have found that personal information should be given an elastic definition[113] and thus, the enumeration is not considered comprehensive. As per *Gordon*, de-identified information has been found to constitute personal information where there is a "serious possibility" that an individual could be identified through the use of that information, alone or in combination with other information.[114] By contrast, where a data set cannot be re-identified, it may not constitute or hold personal information as defined under the *Privacy Act*.

Without access to the data sets obtained by PHAC from Telus and BlueDot, it is difficult to determine whether there was a serious possibility that the government or other party with access to the mobility information could re-identify it. However, presuming that the information was, in fact, fully de-identified insofar as there were no obvious or intentional ways to re-identify it, the data sets would no longer constitute personal information and could fall outside the *Privacy Act*. Under this set of circumstances, the aggregated and de-identified information received by the federal government from Telus and BlueDot arguably may not have constituted personal information, and the government's reception of this data may not have been governed by the *Privacy Act*.

3.1.2. Telus and BlueDot's Disclosure of Information to PHAC and the Application of PIPEDA

PIPEDA governs every federally regulated organization that collects, uses, or discloses personal information in the course of commercial activities per s. 4(1)(a).[115, 116] The Act

111 *Dagg v Canada*, [1997] SCJ No 63, 148 DLR (4th) 385 at para 64; Privacy Act, RSC 1985, c P-21, s 2.

112 *Privacy Act*, RSC 1985, c P-21, s 3.

113 *Canada (Information Commissioner) v Royal Canadian Mounted Police Commissioner*, 2003 SCC 8 at paras 23-24.

114 See: Gordon v Canada, 2008 FC 258 at para 34.

115 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 4(1)(a): **4 (1)** "This Part applies to every organization in respect of personal information that (a) the organization collects, uses or discloses in the course of commercial activities …"

116 Some groups are excluded from PIPEDA's ambit. Excluded groups include those regulated by provincial

has been given quasi-constitutional status and is responsible for balancing interests between commercial access to information and an individual's privacy interests in that information.[117] The following subsections pose questions that are used to assess the responsibilities that Telus and BlueDot had to meet while handling the information that was, subsequently, disclosed to the federal government.

Were Telus and BlueDot collecting, using, or disclosing information?

Telus and BlueDot are private organizations that collected information either from customers or secondary parties. Telus used its own customers' mobility information to create aggregated data sets of de-identified information whereas BlueDot created similar kinds of data sets by obtaining mobility information from third-party data brokers. Both organizations disclosed the data to the government of Canada.

Does the disclosure of information occur in the course of commercial activities?

Telus and BlueDot contracted with the Canadian government to disclose de-identified mobility data. Both companies advertise that they use de-identified data on their respective websites. In the case of BlueDot, they state that organizations could request demos of BlueDot's services to see how these services could "empower [their] organization to make critical decisions with clarity and confidence."[118] This constitutes a commercial activity.

Telus does not always charge third-parties for access to Telus' data analytics, though the company has recognized that "fees may be charged on a case-by-case basis depending on a number of factors, including whether the third party seeking access is commercial in nature and how broadly Canadians may benefit from the proposed initiative."[119] Moreover, data sets that are disclosed are derived from the data of individuals who used Telus' services. The potential for fees to be imposed—a kind of commercial activity—means that Telus' Data for Good program arguably constitutes commercial activity in at least some circumstances.

Is mobility data personal information?

Courts have found that personal information under PIPEDA should be given a broad and expansive definition that should be interpreted in a fashion to give effect to the

---

legislation, political parties, and many activities undertaken by non-profit organizations. See: Office of the Privacy Commissioner of Canada. (2018). "Summary of Privacy Laws in Canada – What Does PIPEDA Not Apply To?" *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2-2.

117 *Eastmond v Canadian Pacific Railway*, 2004 FC 852 at para 100; *Nammo v Transunion of Canada Inc*, 2010 FC 1284 at para 74; *TA v Globe24h.com*, 2017 FC 114 at para 93.

118 BlueDot. (Undated). "Government." *Blue Dot*. Available at: https://bluedot.global/government/.

119 Telus. (Undated). "Data For Good: Commitments." *Telus*. Available at: https://www.telus.com/en/about/privacy/data-for-good/commitments.

purpose of the Act.[120] PIPEDA and the *Privacy Act* should not be interpreted in reference to each other but should instead be based on the language of their respective provisions.[121] However, the finding in *Gordon* has been judicially considered in the application of PIPEDA.[122] Accordingly, for PIPEDA to apply here, there must be a serious possibility that an individual could be identified through the use of the information in question, either on its own or in combination with other information. In a case where de-identified or aggregated information cannot be re-identified to an individual, however, the de-identified or aggregated information may not be considered personal information under PIPEDA.

Telus collected mobility data from its approximately 9 million mobile phone subscribers prior to de-identifying the data.[123] Mobility data, or location data, has been found to constitute personal information within the meaning of PIPEDA.[124] Such information, at the time of collection, can be revelatory about an identifiable individual because it can reveal geo-temporal location patterns and potentially be correlated with other identifying information. Thus, Telus was arguably collecting personal information in the course of its normal commercial activity. As a result, PIPEDA would apply to the collection of this information. Telus then processed the information it had collected to de-identify it and then disclosed the de-identified and aggregated information to the federal government. Assuming the risk of re-identification was low, it is likely that the disclosed de-identified information would not be considered personal information under PIPEDA, with the effect that it likely was not subject to PIPEDA.

BlueDot stated that it had obtained de-identified and aggregated data from a variety of sources, including application data from third-party providers.[125] The company relied on the suppliers of the data to have obtained consent.[126] Without access to the data set(s) that BlueDot obtained from third-parties, it is difficult to determine the likelihood of whether the received data could be re-identified. Accordingly, it is unclear whether BlueDot collected personal information in the course of its commercial activity, with the result of making it unclear whether PIPEDA necessarily applied to BlueDot's collection of mobility information. Subsequent to obtaining the mobility information, BlueDot disclosed some in aggregated and de-identified formats to the federal government. Assuming the risk of re-identification was low, it is likely that the disclosure of the

120 *Gordon v Canada*, 2008 FC 258 at para 34; *Citi Cards Canada Inc. v. Pleasance*, 2011 ONCA 3.

121 Blood Tribe Department of Health v Canada (Privacy Commissioner), 2008 SCC 44 at para 29.

122 PIPEDA 2009-018; PIPEDA Decision 2014-011; PIPEDA Decision 2022-00.1.

123 Christopher Allison. (2022). ETHI Hearing, dated February 3, 2022.

124 PIPEDA Case Summary No 351. See also: PIPEDA Report of Findings No 2020-004 at para 24, 152.

125 Kamren Khan. (2022). ETHI Hearing, dated February 17, 2022.

126 Kamren Khan. (2022). ETHI Hearing, dated February 17, 2022.

de-identified information would not have been assessed as being personal information under PIPEDA and, as such, PIPEDA may not have applied to the disclosure of de-identified and aggregated mobility information.

Ultimately, while Telus and BlueDot were involved in commercial activities and though residents of Canada retain a privacy interest in their mobility information, PIPEDA likely stopped applying to the mobility data held by Telus and BlueDot after it had been de-identified and aggregated in ways that could not be reversed or lead to the re-identification of the data, assuming that was the case. The de-identified and aggregated information that the companies respectively disclosed to the federal government, while revelatory of Canadian residents' aggregated habits, likely fell outside of PIPEDA's auspice on the basis that it no longer constituted personal information.

4. Critiques of Current Privacy Law

As evident in the analysis conducted in Part 3, the de-identification and subsequent disclosure of personal information is arguably not adequately governed by existing federal privacy legislation on the presumption that there is not a serious risk of re-identification. Part 4 unpacks why this creates governance failures broadly and specifically as it relates to mobility data. These deficiencies in governance and privacy law can be alleviated through legal reform.

4.1. Failure to Adequately Govern De-Identified Data

First, there is no requirement that an organization which provides access to de-identified or aggregated data must be able to demonstrate that the individuals whose data was used to create the data set have meaningfully consented to its collection in the first place.[127] Without such a requirement, it is possible for organizations to commit an original violation of not obtaining consent for collecting personal information and, subsequently, benefitting from the de-identified data outside of the governance associated with federal privacy law.

Proponents opposed to regulating de-identified data sets have asserted that de-identified data need not be governed to the same extent as personally identifiable information because the risk of re-identification is generally remote.[128] Assessment of re-identification risks, however, are based on the technologies or processes that exist at the time of such assessments; as new technologies or statistical processes are developed or deployed, the potential to re-identify data may change significantly. Absent law or regulation, de-identified data can serve as a free pass to the disclosure of information without the recognition that efficacious re-identification is an evolving area of research.[129] Should information be released and subsequently re-identified, the resultant harm may be directly or indirectly

---

127 Office of the Privacy Commissioner. (2021). "Guidelines for Obtaining Meaningful Consent." *Office of the Privacy Commissioner of Canada.* Available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

128 See for example: Chantal Bernier. (2021). "Governance for Innovation and Privacy: The Promise of Data Trusts and Regulatory Sandboxes." *Centre for International Governance Innovation.* Available at: https://www.cigionline.org/articles/governance-innovation-and-privacy-promise-data-trusts-and-regulatory-sandboxes/.

129 Boris Lubarsky. (2017). "Re-identification of Anonymized Data." *Georgetown Law Technology Review.* Available at: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/; Danny Bradbury. (2021). "De-identify, re-identify: Anonymised Data's Dirty Little Secret." *The Register.* Available at: https://www.theregister.com/2021/09/16/anonymising_data_feature/; Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. (2019). "Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models." *Nature Communications.* Available at: https://www.nature.com/articles/s41467-019-10933-3; Anonyome Labs. (2020). "Re-identification of Anonymous Data is Scarily Simple." *Anonyome Labs.* Available at: https://anonyome.com/2020/12/re-identification-of-anonymous-data-is-scarily-simple/; Yves-Alexandre de Montjoye, Sébastien Gambs, Vincent Blondel, et al. "On the privacy-conscientious use of mobile phone data." *Scientific Data* 5, 180286 (2018). Available at: https://doi.org/10.1038/sdata.2018.286.

experienced, and it may be challenging or impossible to reverse these harms or impose subsequent privacy protections on data in the wild. Moreover, as more de-identified data is made available, it is increasingly possible for data sets to be combined and analyzed against one another to re-identify them.[130]

Information Box 2: The Risk of Re-Identifying De-Identified Data

The risks of re-identification are very real. A 2019 study that was published by the Imperial College of London and the Belgium Université Catholique de Louvain showcased a method capable of correctly re-identifying 99.98% of individuals in anonymized data sets with just 15 demographic attributes.[131] Another study used a data set containing smartphone location data of 1.5 million people over the course of 15 months, where the location of individuals was specified hourly. With this data set, researchers could uniquely identify 95% of the individuals in a data set with just four spatio-temporal points.[132] In yet another analysis, when Boris Lubarsky of Georgetown Law reviewed a number of examples of re-identification in the American context, including data sets released by AOL, New York Taxi, Netflix, and government officials, he demonstrated that contemporary techniques of re-identification regularly reversed the privacy protections that were meant to ensure that de-identified data stayed de-identified.[133] Combined, these studies demonstrate the de-identified data sets are under constant risk of being re-identified given new statistical methods, data sets, or technical innovations.

Preventing re-identification of de-identified data sets may demand creating or adopting technological standards along with regularly reassessing approximate likelihoods that de-identified information might ever become re-identified. In the context of government collections of mobility data, there may be intentions to never re-identify data. This might mean that, at a policy level, the risk of re-identification is considered low, but where re-identification is technically possible, the actual risks may be heightened in excess of what a policy or contractual assertion might indicate. Such risk assessments can be at least partially captured in Privacy Impact Assessments, which are designed to gauge risks based on planned as well as unplanned uses of collected information,[134] though if these

130 Boris Lubarsky. (2017). "Re-identification of Anonymized Data." *Georgetown Law Technology Review*. Available at: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

131 Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, and Alex Pentland. (2015). "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata" *Science*. Available at: https://www.science.org/doi/full/10.1126/science.1256297?siteid=sci&keytype=ref&ijkey=4rZ2eFPUrlLGw.

132 Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen and Vincent D. Blondel. (2013). "Unique in the Crowd: The Privacy Bounds of Human Mobility" *Scientific Reports*. Available at: https://www.nature.com/articles/srep01376#Abs1.

133 Boris Lubarsky. (2017). "Re-identification of Anonymized Data." *Georgetown Law Technology Review.* Available at: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

134 Government of Canada. (2020). "Directive on Privacy Impact Assessment." *Government of Canada.* Available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308.

assessments are not regularly conducted, then new technological or statistical re-identification techniques that modify the relative levels of risk may not be taken into account. Given the vast stores of personal information that are accessible to government agencies along with the ability to sometimes compel such information from residents of Canada, some degree of heightened risk of government re-identification of personal information will almost always exist.

4.2. Meaningful Consent of Secondary Uses

Second, there are no requirements that individuals be informed of the ways in which their data is de-identified and used for secondary purposes. Even if individuals meaningfully consent to the sharing of their personal information, and know how their personal information is being used and by whom, they must also be informed about who else might use this information. Only by clarifying the secondary parties who might use the information will it be possible for individuals to gain or develop trust in how their information is being collected and who might use or retain it. In the case of the collection of mobility data, this concern was raised by the Privacy Commissioner in his appearance before the ETHI Committee where he doubted that many residents of Canada knew that their data was being used as part of Telus' Data for Good program and then provided to the Public Health Agency.[135] Even if consent had been obtained, the lack of knowledge surrounding the uses of individuals' data can lead individuals to lose trust in data-handling organizations and the laws governing the handling of personal information.

4.3. Negative Social Effects of Health Surveillance

Third, there is the issue that privacy law alone is insufficient to restrict potentially problematic uses of de-identified or aggregated data. Mobility data, as an example, might be used to guide government policy-making decisions that can have adverse effects on different communities, some of which may already be marginalized by law. This may include policies that police low-income communities that travel often and work in-person amid lockdown rules or policies that affect individuals who access reproductive health care. While an individual's privacy interest in the data may be limited as a result of de-identification, there remains an individual or community equity interest in how data sets might be used, especially when such uses are regarded as counter to an individual's or community's self-regarded interests. While privacy law alone cannot assist with these broader impacts, approaching privacy law with an equity lens is imperative to ensuring that all individuals' privacy and other rights are adequately protected.

135 Daniel Therrien. (2022). ETHI Hearing, dated February 7, 2022.

4.4. Consent and Accountability Requirements

Fourth, as evident from PHAC's collection of mobility data, there is a lack of transparency surrounding how information is shared between public and private entities. The Privacy Commissioner noted that while there is a reference to the Data for Good program in Telus' privacy policies and the government's COVIDTrends website had publicly disclosed the government's use of mobility data, most residents of Canada did not know how their data would be used.[136]

Normatively and as best practice, government agencies should validate that meaningful consent has been obtained from individuals before contracting with private institutions that are making available either identified or de-identified personal information. For consent to be meaningful, people must understand to what they are consenting.[137] Recommendation 12 of the ETHI Committe's Report directs the Government of Canada to ensure that private companies have obtained meaningful consent from their customers for the collection of mobility data before contracting to use their services or obtain data they possess.[138]

Moreover, trust is gained when robust accountability measures exist. Data-sharing practices should be embedded in a broader accountability regime. Such a regime might require that:

- governments confirm or verify that individuals have provided meaningful consent to collection and dissemination of information being shared by a private entity
- there be clear and public declarations of the specific purposes for a data collection
- private and public organizations that handle personal information, de-identified information, or aggregated information derived from personal information clearly explain how long they retain information and with whom they may specifically share the data
- an explanation of how private or public organizations that receive either personal information, de-identified information, or aggregated information derived from personal information will use the information in question and denote the extent to which there are risks in light of a possible data breach

136 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

137 Office of the Privacy Commissioner of Canada. (2020). "PIPEDA Fair Information Principle 3 - Consent." *Office of the Privacy Commissioner of Canada.* Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/.

138 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

It is only by taking the effort to clearly explain how private and public organizations handle personal information that trust in these kinds of organizations can be enhanced and that they can be held accountable in cases that they breach that trust with individuals and communities in Canada.

Information Box 3: The Ineffective Management of the Life Cycle of New Technology

Bianca Wylie, a government accountability advocate, has written about the need for governments to be measured and deliberate when they develop and deploy new technological systems. In assessing the COVID Alert application, she has noted that despite early assurances that the application would be overseen and assessed by an advisory council, that very council was disbanded prior to the application being wound-down.[139] This failure of governance signals a lack of accountability, and has Wylie argued that if the government wants new technological processes or systems to be taken seriously and trusted by the public, then the government must comprehensively manage the life cycle of government services and applications.[140] It is important to keep these lessons in mind when assessing governmental adoptions of new technologies or data-mining projects.

4.5. Indigenous Sovereignty

Fifth, there may be sovereignty claims associated with the data in either an identifiable or non-identifiable format. Indigenous communities across Canada are actively working to establish and operate their own critical infrastructure, in part to own or control the data their populations generate. In particular, First Nations principles of Ownership, Control, Access and Possession (OCAP) are a set of standards that establish how First Nations' data should be collected, protected, used, or shared, and it is the de facto standard for how to conduct research with First Nations Groups.[141] As well, privacy interests may differ between Indigenous groups; some communities may possess privacy interests in types of information that are not commonly considered by settler-colonialists, such as information associated with ceremonies, traditional and contemporary practices, or support for community development projects.[142] While there is no single Indigenous perspective

139 Bianca Wylie. (2022). "Canada's COVID Alert App Needs to be Shut Down. Here's Why." *Bianca Wylie.* Available at: https://biancawylie.medium.com/canadas-covid-alert-app-needs-to-be-shut-down-here-s-why-dc5037ecdcf.

140 Bianca Wylie. (2022). "Canada's COVID Alert App Needs to be Shut Down. Here's Why." *Bianca Wylie.* Available at: https://biancawylie.medium.com/canadas-covid-alert-app-needs-to-be-shut-down-here-s-why-dc5037ecdcf.

141 First Nations Information Governance Centre. (2022). "About Us – What Does FNIGC Do?" *First Nations Information Governance Centre.* Available at: https://fnigc.ca/about-fnigc/.

142 Kimberly Gee. (2019). "Introduction to Indigenous Canadian Conceptions of Privacy: A Legal Primer." *Canadian Bar Association*. Available at: https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2019/Runner-up-of-2019-Privacy-and-Access-Law-Student-E#_ednref32; See also: Megan Vis-Dunbar, James Williams, and Jens H. Weber Jahnke. (2011). "Indigenous and Community-Based Notions of Privacy." *University of Victoria*. Available at: https://www.researchgate.net/profile/Jens_Weber6/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy/

of privacy, where meaningful and informed consent has not been provided between (and by) these individuals and groups and the data is then used (in either an identifiable or de-identified format) by the federal government, doing so may run counter to the interests of Indigenous populations.

The Canadian Government could act contrary to the spirit of reconciliation should it fail to recognize Indigenous data sovereignty. In 2015, Canada vowed to fully implement the 94 Calls to Action of the Truth and Reconciliation Commission of Canada.[143] Calls to Action 19 and 65 reference the increasing need for data pertaining to Indigenous communities, calling on the federal government to "identify and close gaps in health outcomes between Aboriginal and non-Aboriginal communities" and "establish a national research program with multi-year funding to advance understanding of reconciliation." Relatedly, Canada fully implemented the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) into Canadian law in 2021. Article 19 of UNDRIP includes a requirement for states to obtain free, prior, and informed consent of Indigenous peoples on any decisions that may impact them. UNDRIP also includes a right to Indigenous sovereignty, which includes the right to exercise authority over data and information.[144] Collecting data from private organizations, like Telus or BlueDot, may lead the Canadian government to sidestep its commitment to Indigenous people to obtain free, prior, and informed consent, especially since mobility data can be used by the Canadian government in a manner that could have adverse effects on Indigenous communities.[145]

4.6. Enforcement Mechanisms

Sixth, existing federal privacy legislation lacks sufficient enforcement mechanisms. Notably, neither the *Privacy Act* nor *PIPEDA* empower the Privacy Commissioner to make orders, nor do they permit the Commissioner to impose Administrative Monetary Penalties, or assert a private right of action for breaching the respective Acts.

links/582f93e408ae138f1c03595c/Indigenous-and-Community-based-Notions-of-Privacy.pdf.

143 Government of Canada. (2015). "Statement by Prime Minister on release of the Final Report of the Truth and Reconciliation Commission." *Goverment of Canada.* Available at https://pm.gc.ca/en/news/statements/2015/12/15/statement-prime-minister-release-final-report-truth-and-reconciliation.

144 The First Nations Information Governance Centre. (2019). "First Nations Data Sovereignty in Canada." *Statistical Journal of the IAOS*. Available at: https://content.iospress.com/articles/statistical-journal-of-the-iaos/sji180478.

145 For a discussion on how ostensibly well-intentioned government actions may reproduce the structural violence of settler-colonial governance in liberal democracies, see: Lara Fullenwieder and Adam Molnar. (2018). "Settler Governance and Privacy: Canada's Indian Residential School Settlement Agreement and the Mediation of State-Based Violence." *International Journal of Communication* 12.

4.7. Accessibility and Corporate Transparency

Seventh, privacy legislation and privacy policies are often inaccessible to citizens given the structure and complexity of specialized legal language. Experts have referred to PIPEDA as a "dog's-breakfast statute"[146] as different pieces of the legislation have come from a variety of sources and are expected to be read together; the Canadian Standards Association Model Code was simply appended at Schedule 1 and must be read together with the provisions outlined in Part I of PIPEDA. Judges have also recognized the difficulty in understanding and reading this legislation.[147] If individuals are unable to read and understand privacy legislation, loss of trust in how their personal information will be handled by private organizations is likely. Similarly, private organizations often adopt lengthy privacy policies that are filled with inaccessible jargon. The combination of the complexity of legislation and organizational privacy policies can make it difficult for individuals to understand how their data is being collected, used, and disclosed and whether organizational practices accord with privacy legislation.[148]

Ultimately, the *Privacy Act* and *PIPEDA* were both written for a pre-digital era. Experts and government committees alike have called for their respective reform.[149] None of these recommendations have yet led to law reform. However, since the start of the COVID-19 pandemic, the federal government has introduced a pair of bills meant to reform PIPEDA. In Part 5, we proceed to assess the extent to which the most recent bill addresses the governance gaps pertaining to personal information, mobility information, and de-identified and aggregated information that were highlighted in Part 4.

---

146 Teresa Scassa. (2018). "PIPEDA Reform Should Include a Comprehensive ReWrite." *Teresa Scassa.* Available at: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80.

147 Miglialo v Royal Bank of Canada, 2018 FC 525 at para 19; See also: Englander v Telus Communications Inc, 2004 FCA 387 which lays out the history of the Act.

148 See as an example: Jonathan A. Obar. (2022). "TELUS has policy materials reaching 123,049 words, which would take 10.2 hours to read. SaskTel's 86,804 words would take 7.1 hours, and Bell Aliant's 85,089 words, 6.8 hours." *The Biggest Lie On The Internet.* Available at: https://www.biggestlieonline.com/policy-length-analysis-2019/. See also: Jonathan Obar. (2022). "A Policy Complexity Analysis for 70 Digital Services," *The Biggest Lie On The Internet.* Available at: https://www.biggestlieonline.com/policy-complexity-analysis-2019/.

149 Standing Committee on Access to Information, Privacy and Ethics. (2016) "Review of the Access to Information Act." *House of Commons.* Available at: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP8360717/ETHIrp02/ETHIrp02-e.pdf; Standing Committee on Access to Information, Privacy and Ethics. (2016) "Protecting the Privacy of Canadians: Review of the Privacy Act." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-4/; Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." *House of Commons.* Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.

5. The Consumer Privacy Protection Act

The federal government has twice introduced legislation to replace the federal commercial privacy law, PIPEDA. The first, Bill C-11: *Digital Charter Implementation Act, 2020* (C-11), died on the order paper when an election was called on August 15, 2021. A revised version of the legislation, Bill C-27: *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* (C-27), was introduced on June 16, 2022.

We refer principally to elements of Part II of C-27, the *Consumer Privacy Protection Act* (CPPA), though sometimes also reference similar language that appeared in C-11. As previously argued in Part 4, the federal commercial privacy legislation that is in force at time of writing is deficient because it fails to adequately govern de-identified information, contains inappropriate exceptions to knowledge and consent, threatens to undercut Indigenous data practices, fails to include enforcement mechanisms, and, broadly, does not compel private organizations to explain their activities clearly to individuals. As C-27 is meant to replace the private sector privacy legislation, PIPEDA, we focus on the extent to which C-27 ameliorates these deficiencies.

5.1. Governing De-Identified Data

As discussed in Part 4.1, PIPEDA does not adequately govern de-identified data. C-11 would have governed de-identified data, which it defined as personal information that was created or modified "by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information to identify an individual."[150] This definition, adopted in C-11, was inclusive in that it would have governed de-identified information that removed both direct (e.g., names, phone numbers, social insurance numbers, etc.) and indirect (e.g., place of birth, race, religion, weight, unusual occupation, etc.) identifiers.

In contrast, C-27 introduced the concepts of de-identified as well as anonymous information. The former refers to data where direct identifiers have been removed such that an individual cannot be directly identified, but where there is still a possibility to re-identify information.[151] Anonymous information, in contrast, would have to be irreversibly and

150 Bill C-11, "Digital Charter Implementation Act, 2020." *LegisInfo*. Available at: https://www.parl.ca/LegisInfo/en/bill/43-2/c-11, s 2.

151 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s. 2(1): "de-identify means to modify personal information so that an individual cannot

permanently modified "in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means."[152] Where information has been anonymized, it is considered to fall out of scope of the legislation, though s. 2(3) of the CPPA includes a number of situations where de-identified data can be used or treated as though it were anonymous.

In the case of mobility data, if a private organization removed direct and indirect identifiers, C-27 would not govern such information. This would include situations where private organizations disclosed such information to government agencies such as PHAC, the Royal Canadian Mounted Police , or the Canada Border Services Agency, among others. C-27, then, would not necessarily remedy the governance issues that presently exist within PIPEDA.

While C-27 attempts to safeguard de-identified data by imposing prohibitions on re-identifying it, it also empowers the Privacy Commissioner to permit re-identification of information where it is clearly in the interests of the individual.[153] The very presence of re-identification exemptions suggests that data may not be irreversibly de-identified. While organizations may be administratively expected to not re-identify information, the information may, nonetheless, be re-identified. Should private organizations suffer data breaches, it is possible that their own information repositories may be sufficient to re-identify individuals. These risks mean that de-identified data should always enjoy strong privacy regulations and, as such, exemptions under s. 2(3) that would authorize private organizations to treat de-identified data as equivalent to anonymous data are ill-conceived.

To more appropriately safeguard de-identified information, we make the following three recommendations.

be directly identified from it, though a risk of the individual being identified remains."

152 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s. 2(1).

153 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 75, s116.

Recommendation 1: Adopt the Prior Definition for De-Identified Data under C-11

Adopting the prior definition of de-identified information outlined in C-11 would allow private sector privacy law to govern de-identified data by way of removing either direct or indirect identifiers.

Original C-27 Text

2(1) **de-identify** means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains. (dépersonnaliser)

Proposed Legislative Amendment

2(1) **de-identify** means to modify personal information ~~so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.~~ — or create information from personal information—by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual. (dépersonnaliser)

Recommendation 2: Remove Exemptions under Section 2(3)

Exemptions under s. 2(3), which would authorize private organizations to treat de-identified data as equivalent to anonymous data in some situations, should be removed in order to allow for better transparency and accountability standards.

Original C-27 Text

2(3) For the purposes of this Act, other than sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116, personal information that has been de-identified is considered to be personal information.

Proposed Legislative Amendment

2(3) For the purposes of this Act, ~~other than sections 20 and 21, subsections 22(1) and 39(1), sections 55 and 56, subsection 63(1) and sections 71, 72, 74, 75 and 116~~, personal information that has been de-identified is considered to be personal information.

Recommendation 3: Enable the Privacy Commissioner to Establish Regulations to Ensure Appropriate De-Identification

The Privacy Commissioner should be empowered to establish regulations to ensure that information is appropriately de-identified. Doing so would reduce the risk that data may be re-identified. This ability would extend beyond the discretion presently offered to private organizations to adopt technical and administrative measures.[154]

5.2. Knowledge and Consent

Private organizations can use exemptions to knowledge or consent requirements under PIPEDA where the collection, use, or disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way, or when there are concerns that consent would impact the accuracy of the information, among others.[155] These exemptions, along with new exemptions, are present in C-27. In particular, the exemptions in the CPPA under s. 39 about socially beneficial purposes and s. 18 about legitimate interest would broadly maintain and expand the ability of private organizations to disclose information to federal bodies, or to collect and use personal information for the private organization's purposes, without first seeking consent or explaining the organization's practices. The effect of these exemptions may be to let private organizations replicate activities that could broaden trust deficits in how private and public organizations handle personal (or de-identified or anonymous) information.

In the remainder of section 5.2, we assess the deficiencies associated with the socially beneficial purposes and the legitimate purpose exemptions. We ultimately conclude that, in their present form, they would not appropriately govern how private organizations could collect, use, or disclose information associated with, or derived from, individuals.. Specifically, individuals would continue to be unaware of data disclosures, such as of de-identified and aggregated mobility information from private organizations to government agencies, nor would individuals be in a position to oppose such data handling because they would not have provided meaningful consent to such private organizations' activities or because they had not been made aware that the disclosures of their information were occurring.

5.2.1. Socially Beneficial Purpose Exception

The collection, use, and disclosure of de-identified information between private organizations and government agencies would fall under the socially beneficial purposes

154 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://wrecoww.parl.ca/legisinfo/en/bill/44-1/c-27, s. 74.

155 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 7.

exemptions under C-27. The language is the same in both C-11 and C-27 and is reproduced in Information Box 4.

Information Box 4: Section 39 (1) - (2) of the CPPA

39 (1) An organization may disclose an individual's personal information without their knowledge or consent if

(a) **the personal information is de-identified** before the disclosure is made;

(b) **the disclosure is made to**

(i) **a government institution or part of a government institution in Canada**,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

(iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity; and

(c) the disclosure is made **for a socially beneficial purpose**.

(2) For the purpose of this section, socially beneficial purpose means a purpose **related to health**, the provision or improvement of public amenities or infrastructure, the protection of the environment **or any other prescribed purpose**.[156]

When we turn to the example of Telus and BlueDot disclosing de-identified and aggregated mobility information to government agencies, it is apparent that s. 39 would authorize such behavior. The information in question was de-identified by Telus and BlueDot before the disclosure was made (s. 39(1)(a)), made to a government institution (s. 39(1)(b)), and would likely be found to have been made for a socially beneficial purpose (s. 39(1)(c)), namely a purpose related to health (s. 39(2)) or any other prescribed purpose given that the intended use of mobility data was to survey and track disease. Consequently, under C-27, knowledge and consent need not be sought prior to disclosing de-identified mobility or geolocation information for socially beneficial purposes to government agencies.

Professor Teresa Scassa's assessment of the socially beneficial purpose exception found that it might have the effect of authorizing some research purposes and not others.[157]

156 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 39. Emphasis not in original.

157 Teresa Scassa. (2020). "Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill." *Teresa Scassa*. Available at: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-

Notably, socially beneficial purposes only extend to research about health, the provision or improvement of public amenities or infrastructure, or the protection of the environment.[158] While true that some socially beneficial research could be stymied by the current drafting language in C-27, the same language could authorize some problematic uses of the data.

While socially beneficial activities can have positive characteristics,[159] determining what constitutes a beneficial activity can be as much a political decision as a bureaucratic one that is ideally grounded in community consultation or public feedback. As an example, through one political lens, a health agency might assess the distance that people must travel to receive abortion care as a way of determining that there are an insufficient number of funded care facilities insofar as this is essential care that people have a right to obtain. Through a very different political lens, however, access to such services might be regarded as deleterious to fetal life, and mobility information could used to develop campaigns to promote anti-abortion policies that are regarded by governments as socially beneficial at the time. In the absence of stiff normative discipling functions in the legislation, such as rights-based tests, there is a risk that what is socially beneficial for some is not for others.[160]

Further, de-identified information may be used for "other prescribed purposes" in the future. While outside the scope of this report, the potential to expand what constitutes socially beneficial purposes means that there is no clear delineation of the conditions wherein the exemption might apply. Future governments could extend what constitutes socially beneficial purposes to include new policy objectives. Such objectives could change, expand, or contract with successive governments. Consider, as an example, that a future purpose might include the modernization of the border and thus that could entail tracking the movement of people close to federal borders or specifically monitoring regions where (often racialized) newcomers to Canada live. In such a situation, individuals and communities may be unable to resist data collection, such as when it is carried

exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80.

158 Teresa Scassa. (2020). "Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill." *Teresa Scassa*. Available at: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-exception-in-canada%E2%80%99s-private-sector-data-protection-law-reform-bill&Itemid=80.

159 See for example: Masataka Harada, Gaku Ito, and Daniel M. Smith. (2022). "Using Cell-Phone Mobility Data to Study Voter Turnout." *SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4205273.

160 See: Lindsay Clark. (2022). "Decisions on Health Data Sharing Should Not be Taken by Politicians, Citizen Juries Find." *The Register*. Available at: https://www.theregister.com/2022/08/31/uk_health_data_share/. "A report by England's National Data Guardian (NDG), an independent watchdog for health data appointed by the Secretary of State for Health and Social Care, found that in citizen juries consulted on health data, "very few jurors wanted decisions about the future of these initiatives to be taken by the minister or organization accountable for them. Most believed that an independent body of experts and lay people should assess the data sharing initiatives."

out by telecommunications providers or data brokers, nor restrict subsequent sharing of individuals' and communities' de-identified data with the federal government.

In light of the potentially problematic uses of de-identified data for socially beneficial purposes and the potential for socially beneficial uses to expand, unconstrained, over time, we make the following recommendations.

Recommendation 4: Inform Individuals and the Privacy Commissioner of the Disclosure, Recipient, Purpose, and Rights to Opt-Out of Socially Beneficial Purposes

Creating rights-respecting privacy legislation necessarily requires individuals to have some sense of control over their information. Informing individuals of the ways in which their information is disclosed and, subsequently, providing them with the option to opt-out recognizes their right to information and empowers individuals to decide whether the articulated beneficial purposes warrant the collection of their data.

Original C-27 Text

39 (1) An organization may disclose an individual's personal information without their knowledge or consent if

(a) the personal information is de-identified before the disclosure is made;

(b) he disclosure is made to

(i) a government institution or part of a government institution in Canada,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

(iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity; and

(c) the disclosure is made for a socially beneficial purpose.

Proposed Legislative Amendment

39 (1) An organization may disclose an individual's personal information without their ~~knowledge or~~ explicit consent if

(a) the personal information is de-identified before the disclosure is made;

(b) the disclosure is made to

(i) a government institution or part of a government institution in Canada,

(ii) a health care institution, post-secondary educational institution or public library in Canada,

(iii) any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or

(iv) any other prescribed entity; ~~and~~

(c) the disclosure is made for a socially beneficial purpose~~.~~;

(d) the individual is informed of the disclosure, the recipient of information, the articulated socially beneficial purpose, the disclosure and retention period, the opt-out process prior to the disclosure, and the adverse effect assessment in (3);[161]

(e) the receiver of the de-identified information confirms consent obligations have been complied with by the organization; and,

(f) the Privacy Commissioner is consulted and approves of the disclosure.

161 39 (3) is defined in Recommendation 5.

Recommendation 5: Require that the Socially Beneficial Purpose Be Publicly Disclosed and Approved by the Privacy Commissioner and that an Adverse Effect Assessment Be Conducted

Ensuring that the proposed purpose is genuinely socially beneficial is important to establish public trust. Publicly disclosing the purpose will let individuals understand why their data is being collected and help them make more informed choices as to their opt-out rights outlined in Recommendation 4. As well, requiring the Privacy Commissioner to sign off on these purposes provides an accountability measure to mitigate purposes that are vague or overly broad.

Additionally, requiring organizations to conduct assessments to determine the nature of these impacts prior to data collection, use, or disclosure would help to mitigate the negative social impacts of data sharing even where it is perceived to be of benefit. Prior to data sharing, the assessment should be reviewed by the Privacy Commissioner, who ought to be empowered to prevent data collection, use, or disclosure if they are unsatisfied that the proposed benefit is proportionate to the adverse effect.

Original C-27 Text	Proposed Legislative Amendment
39(2) For the purpose of this section, socially beneficial purpose means a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose.	39(2) For the purpose of this section, socially beneficial purpose means a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose that has been publicly promulgated, disclosed, and approved by the Privacy Commissioner.
N/A	39 (3) Prior to collecting or using personal information under subsection (1), the organization must (a) identify any potential adverse effect on the individual that is likely to result from the collection or use through a review of the sensitivity of the data and an equity assessment; (b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; (c) record its assessment of (a) and (b) and provide a copy of the assessment to the Commissioner within a reasonable time period before collection or use under subsection (3); and, (d) comply with any prescribed requirements.

Recommendation 6: Institute Auditing of Information Sharing Under Section 39

Auditing measures would allow the Privacy Commissioner to ensure that the practices conducted by the parties collecting and disclosing information meet the required de-identification standard(s). In particular, the Commissioner could ensure that de-identification practices carry a low risk of re-identification, that the data has been used for only approved and well-defined purposes, and that data has been disposed of appropriately. Should the Commissioner find that the parties have acted inappropriately, they should be empowered to impose orders and penalties accordingly. This ability would create the necessary checks and balances to ensure public trust in data sharing for the social good.

Proposed Legislative Amendment

Auditing Practices

39 (4) After the noted disclosure period in subsection (1)(d),[162] the Commissioner may conduct an audit of whether consent was adequate, best practices for de-identification were followed, re-identification never occurred, information was used only for the disclosed purposes, and that information past the retention period was disposed of.

Recommendation 7: Empower the Privacy Commissioner to Prevent or Halt Data Sharing for Socially Beneficial Purposes

Prior to data sharing, the adverse effect assessment should be reviewed by the Privacy Commissioner, who ought to be empowered to prevent data collection, use, or disclosure if they are unsatisfied that the proposed benefit is proportionate to the adverse effect. In addition, it may be helpful to require the Commissioner to engage with every government body where the socially beneficial purpose exemption is claimed. This engagement process would include organizations proving to the OPC that, where required, meaningful consent has been obtained and, where not required, it was not possible to obtain consent prior to the disclosure of information. Where such evidence has not been provided to the Commissioner, the legislation should empower the Commissioner to require the data be immediately disposed of and individuals be notified of the unlawful collection of information if doing so is possible.

Proposed Legislative Amendment

39 (5) Where the Privacy Commissioner is not satisfied that the social benefit outweighs the potential adverse effect on a review of the adverse effect assessment in (3), they can prevent or terminate the disclosure of information.

39 (6) If at any point the Privacy Commissioner learns that consent was not adequately obtained, the Commissioner may order that the data be immediately disposed of and individuals shall be notified of the unlawful collection of information to the extent that this is possible. The Privacy Commissioner may also impose penalties and make orders as just.

162 39(1)(d) is defined in Recommendation 4.

5.2.2. Legitimate Interest Exception

Bill C-27 includes an exception to knowledge and consent where an organization has a legitimate interest that outweighs adverse effects. This exception may let organizations collect or use personal information without the knowledge or explicit consent of an individual, even when collecting, using, or disclosing the personal information for non-socially beneficial purposes. Information Box 5 reproduces the relevant parts of s. 18 of the CPPA.

Information Box 5: Section 18 (3) - (5) of the CPPA

18 (3) An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and

(a) a reasonable person would expect the collection or use for such an activity; and

(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

18 (4) Prior to collecting or using personal information under subsection (3), the organization must

(a) identify any potential adverse effect on the individual that is likely to result from the collection or use;

(b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and

(c) comply with any prescribed requirements.

18 (5) The organization must record its assessment of how it meets the conditions set out in subsection (4) and must, on request, provide a copy of the assessment to the Commissioner.[163]

Organizations regularly find novel uses for personal information. Some current uses, such as monitoring web activities and store visits[164] or the purchase of goods to assess the efficacy of targeted advertising165 or persistently monitoring online activities to generate business intelligence166 would have been largely unthinkable a few decades ago. Today, however, they are regular business activities and, in some cases, may be considered reasonable by many companies and some members of the public.

163 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 18.

164 Owen Ray. (2022). "How to Track Online and Offline Conversations in Google Ads." *Invoca*. Available at: https://www.invoca.com/blog/how-to-track-online-and-offline-conversions-in-google-ads.

165 Maya Kosoff. (2017). "Google is Secretly Monitoring Your Real-World Purchases, Too." *Vanity Fair*. Available at: https://www.vanityfair.com/news/2017/05/google-tracking-credit-card-data-advertisers.

166 Steve Dent. (2022). "Facebook and Instagram Apps can Track Users via Their In-App Browsers." *Engadget*. Available at: https://www.engadget.com/meta-can-track-facebook-and-instagram-users-on-ios-with-its-in-app-browsers-071834703.html; Karissa Bell. (2018). "'Highly Confidential' Documents Reveal Facebook Used VPN App to Track Competitors." *Mashable*. Available at: https://mashable.com/article/facebook-used-onavo-vpn-data-to-watch-snapchat-and-whatsapp.

The interpretation of the reasonableness provision in s. 18(3)(a) will have significant and ongoing implications for how private organizations handle personal information. Would the collection of information by Telus for the purpose of creating the Data for Good program constitute a "legitimate interest" given the unique ability of telecommunication companies to collect and use mobility data? Could such an interpretation pave the way for other private entities tracking location to establish data trusts of mobility data?

In effect, while the socially beneficial purposes clause opens the door to sharing de-identified information with third-parties, such as government agencies, the legitimate interest exception enables private organizations to determine whether the collection or use of personal information outweighs the adverse effects of doing so. While the information cannot be used for marketing purposes, which would be meant to influence an individual's behavior or decisions, it could be used to create datasets that facilitate business or policy developments. Moreover, the Privacy Commissioner would need to know that organizations were collecting or using information under this exception *and then* make a request for the organization's records about using the exception instead of organizations being required to notify the Commissioner. The effect is that unless the Privacy Commissioner is zealously engaged in asking private organizations about whether they are collecting or using personal information under the legitimate interest exception, it will be private organizations that will principally be the judges and juries of whether their collection falls under the legitimate interest exception.

Recommendation 8: Enhance Adverse Effect Assessments

Collecting and using data for even legitimate business interests may carry adverse effects for vulnerable and marginalized groups. Requiring organizations to carry out enhanced adverse effects assessments to determine the nature of these impacts prior to data collection or use can better mitigate the negative social impacts of data handling even where it is perceived to be of benefit to individuals or the private organization. Prior to collection or use, the adverse effect assessment should be reviewed by the Privacy Commissioner, who ought to be empowered to prevent data collection or use if they are dissatisfied that the proposed benefit is proportionate to the adverse effect.

Original C-27 Text

Conditions precedent

18 (4) Prior to collecting or using personal information under subsection (3), the organization must

(a) identify any potential adverse effect on the individual that is likely to result from the collection or use;

(b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and

(c) comply with any prescribed requirements.

Proposed Legislative Amendment

Conditions precedent

18 (4) Prior to collecting or using personal information under subsection (3), the organization must

(a) identify any potential adverse effect on the individual that is likely to result from the collection or use through a review of the sensitivity of the data and an equity analysis of such adverse effects;

(b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and

(c) comply with any prescribed requirements.

Recommendation 9: Inform Individuals and the Privacy Commissioner of the Collection, Use, Retention Period, and Rights to Opt-Out of Legitimate Interests

Creating rights-based privacy legislation necessarily requires providing individuals with some control over their information. Informing individuals of how their information is collected or used and providing them with the option to opt-out recognizes their right to information and empowers individuals to determine whether they consent to any use of their information for legitimate interests.

Original C-27 Text	Proposed Legislative Amendment
18 (3) An organization may collect or use an individual's personal information without their knowledge or explicit consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.	18 (3) An organization may collect or use an individual's personal information without their ~~knowledge or~~ explicit consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and (a) a reasonable person would expect the collection or use for such an activity; ~~and~~ (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.; (c) the individual is informed of the collection or use, the legitimate interest at stake, the timeline for collection or use, the retention period, the opt-out process as outlined in (6) and the adverse effect assessment.
Record of assessment **(5)** The organization must record its assessment of how it meets the conditions set out in subsection (4) and must, on request, provide a copy of the assessment to the Commissioner.	**Record of assessment** **(5)** The organization must record its assessment of how it meets the conditions set out in subsection (4) and must~~, on request,~~ provide a copy of the assessment to the Commissioner within a reasonable time period before collection or use under subsection (3).
N/A	**Opt-Out** (6) After the individual is informed in accordance with subsection (3), the individual must be informed of the ability to opt-out and have a reasonable time to do so. (7) All individuals whose information is collected or used must be able to opt-out of future collection and use of their data associated with a legitimate interest purpose.

Recommendation 10: Institute Mandatory Auditing of Information Collection and Use Under Section 18

Auditing measures would allow the Privacy Commissioner to ensure that the practices conducted by the parties collecting and using information are up to the required standards associated with the management of the collected or used data. In particular, the Commissioner could ensure that any de-identification practices which are adopted carry a low risk of re-identification, that the data has been used only for a legitimate interest that is well-defined, and that data has been disposed of appropriately. Should the Commissioner find that the parties have acted inappropriately in any manner, the Commissioner should be empowered to impose orders and penalties accordingly as discussed in Recommendations 14 and 15 as well as in Part 5.5 generally. This ability would create the necessary checks and balances to ensure public trust in data sharing for legitimate interest purposes.

Proposed Legislative Amendment

Auditing Practices

(7) After the noted disclosure period in subsection (3)(c),[167] the Commissioner may conduct an audit of data handling practices, including de-identification practices, the purposes for collection or use, and that information past the retention period has been disposed of.

Recommendation 11: Empower the Privacy Commissioner to Prevent or Halt Data Collection or Use for Legitimate Interests

Prior to data collection or use, the adverse effect assessment may be reviewed by the Privacy Commissioner, who ought to be empowered to prevent data collection or use if not satisfied that the proposed benefit is proportionate to the adverse effect.

Proposed Legislative Amendment

(8) Where the Privacy Commissioner is not satisfied that the legitimate interest outweighs the potential adverse effect on a review of the adverse effect assessment in (5), they can prevent the collection or use of information.

(9) If at any point the Privacy Commissioner learns that sufficient information was not provided to enable opt-out, the Commissioner may order that the data be immediately disposed of and individuals shall be notified of the collection of information. The Privacy Commissioner may also impose penalties and make orders as just.

167 18(3)(c) is defined in Recommendation 9.

5.3. Meaningful Consent for Secondary Uses

The intended purposes for data collection, use, or disclosure must be appropriate in the circumstances to avoid function creep. These purposes must be sufficiently specific that data cannot be used for extraneous reasons. In addition to recommendations made pertaining to socially beneficial purposes (Part 5.2.1) and legitimate purposes exceptions (Part 5.2.3), we suggest the following recommendation pertaining to the appropriate purposes provision.

Recommendation 12: Amend the Appropriate Purposes Provision

For purposes to be appropriate, the social impacts of data sharing must be well-understood. Including an assessment of the nature of privacy interests and equity interests associated with specific forms of personal information can clarify whether data collection is holistically appropriate. Moreover, appropriate purposes must be clearly defined and measured as opposed to being vague or overly broad so as to avoid the use of data for secondary purposes. Where organizations do conceive of secondary purposes for the data, knowledge and consent requirements must be renewed.

Original C-27 Text	Proposed Legislative Amendment
Appropriate purposes 12 (1) An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required under this Act.	**Appropriate purposes** 12 (1) An organization may collect, use or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances, whether or not consent is required under this Act.
Factors to consider (2) The following factors must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate: (a) the sensitivity of the personal information; (b) whether the purposes represent legitimate business needs of the organization; (c) the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;	**Factors to consider** (2) The following factors must be taken into account in determining whether the manner and purposes referred to in subsection (1) are appropriate: (a) the sensitivity of the personal information, based on: (i) an analysis of the sensitivity of the privacy interest in the information; and (ii) the sensitivity of quality-impacting inferences that could be derived from or associated with the personal information. (b) whether the purposes represent legitimate business needs of the organization; (c) the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;

(d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and (e) whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.	(d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and (e) whether the individual's loss of privacy is proportionate to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.
Purposes (3) An organization must determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.	**Purposes** (3) An organization must determine ~~at or~~ before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes with sufficient specificity, as set out in guidance by the Privacy Commissioner.
New purpose (4) If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose.	**New purpose** (4) If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose and renew its knowledge and consent obligations before using or disclosing that information for the new purpose.

5.4. Indigenous Sovereignty

C-27 does not engage on the principles we raise in Part 4.5. An amended version of the legislation should explicitly include language that demonstrates Canada's commitment to truth and reconciliation. Recognizing Indigenous sovereignty includes recognizing data sovereignty perhaps by way of providing Indigenous groups with rights over their information and ensuring that free, prior, and informed consent is obtained prior to collecting, using, and disclosing information concerning Indigenous peoples.

Recommendation 13: Consult with Indigenous Groups in the Amendment of Privacy Legislation

Amend the legislation in light of and following meaningful and substantive consultations with Indigenous communities, so as to ensure that the federal government meets its commitment to ensure data sovereignty for Indigenous groups.

5.5. Enforcement Mechanisms

Bill C-27 would enhance the ability of the Office of the Privacy Commissioner to provide guidance on or to recommend corrective measures pertaining to a regulated organization's privacy management program. It would also give the Commissioner order-making authority to direct an organization to:

- take measures to comply with the CPPA
- stop doing something that is in contravention of the CPPA
- comply with the terms of a compliance agreement entered into by the organization
- make public any measures taken or proposed to be taken to correct the policies, practices, or procedures that the organization has put in place to fulfill its obligations under the CPPA[168]

It also introduces a private right of action against organizations for damages for loss or injury where the Commissioner or Tribunal has found that an organization has contravened the CPPA.[169] The private right of action would let individuals seek financial relief from the Federal Court or a provincial superior court for various violations of the CPPA. As well, Bill C-27 establishes a Personal Information and Data Protection Tribunal, a new administrative tribunal to hear appeals of decisions made by the Privacy Commissioner under the CPPA.[170] The Tribunal would be governed by the *Personal Information and Data Protection Tribunal Act*, outlined in Part II of C-27.

C-27 also introduces Administrative Monetary Penalties that the Commissioner may recommend to the Tribunal.[171] These penalties could be levied to a maximum of the higher of $10 million or 3% of the organization's gross global revenue in its financial year.[172]

---

168 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 93.

169 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 107.

170 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, Part 2, s 4.

171 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, Part 2, s 94.

172 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, Part 2, s 95(4).

On their face, these are positive steps in ensuring more effective data governance. However, more needs to be done. In particular, the Office of the Privacy Commissioner of Canada has raised concerns regarding these changes. The private right of action was said to be too restrictive in that the right would apply only in cases where the OPC has made a final finding of a contravention of the CPPA, which could take many years.[173] As well, the creation of an administrative appeal tribunal would not allow for quick and effective remedies, and the Commissioner has argued that such a tribunal is unnecessary to achieve accountability and fairness.[174] We agree with the Commissioner's assessments.

Recommendation 14: Expand the Private Right of Action

The operation of the private right of action should be expanded to instances where the OPC has yet to make a final finding under the CPPA to allow for greater access to timely justice.

Recommendation 15: Do Not Establish the Personal Information and Data Protection Tribunal

The Privacy Commissioner should be independently empowered to investigate complaints, make orders, and impose administrative monetary penalties. Appeals of the Commissioner's decisions should be made to courts of competent jurisdiction.

While the issues of so many exemptions to informed and meaningful consent and deficiencies in the definition of de-identified data remain, expanding the Commissioner's ambit could alleviate some of the worse potential outcomes of the current framing and drafting of the legislation.

5.6. Accessibility and Corporate Transparency

C-27 includes requirements that organizations use plain language such that "an individual to whom the organization's activities are directed would reasonably be expected to understand."[175] Information about organizational activities, then, would need to be plainly communicated prior to organizations obtaining consent to collect, use, or disclose personal information. However, it is a well-studied and reported phenomenon

173 Office of the Privacy Commissioner of Canada. (2021). "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020." *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.

174 Office of the Privacy Commissioner of Canada. (2021). "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020." *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.

175 Bill C-27, "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts." *LegisInfo*. Available at: https://www.parl.ca/legisinfo/en/bill/44-1/c-27, s 15.

that individuals often cannot find or understand privacy policies or terms of service documents that private organizations present to individuals.[176] Organizations should be required to offer their policy or legal information in formats that the public is more likely to understand and that complies with the *Accessible Canada Act*. Presentation formats might include FAQs,[177] videos, or other formats to present information.[178]

Recommendation 16: Amend the Plain Language Provision to Require Accessibility

In addition to using plain language, privacy policies ought to be made accessible for consumers through accessible formatting.

Original C-27 Text	Proposed Legislative Amendment
Plain language (4) The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand.	**Plain language and Public Accessibility** (4) The organization must provide the information referred to in subsection (3) in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand, in formats that comply with the *Accessible Canada Act* and that may rely on written or audio-visual formats.

As we have written about Bill C-11, which C-27 is modeled after:

> … drafting does not require organizations to adopt public facing language that will improve upon the current state of affairs. Instead, the legislation would require organizations to provide descriptions of the "type of personal information under the organization's control" and for "general" accounts of how organizations make use of personal information or

176 See: Andrew Hilts, Christopher Parsons, and Masashi Crete-Nishihata. (2018). "Approaching Access: A Look at Consumer Personal Data Requests in Canada." *The Citizen Lab*. Available at: https://citizenlab.ca/2018/02/approaching-access-look-consumer-personal-data-requests-canada/; Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall and Ron Deibert. (2020). "We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus." *The Citizen Lab*. Available at: https://citizenlab.ca/2020/05/we-chat-they-watch/; Andrew Clement and Johnathan A. Obar. (2016). "Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers." *Penn State University Press*. Available at: https://www.jstor.org/stable/pdf/10.5325/jinfopoli.6.2016.0294.pdf; Aleecia M. McDonald and Lorrie Faith Cranor. (2008). "The Cost of Reading Privacy Policies." *A Journal of Law and Policy for the Information Society*. Available at: https://kb.osu.edu/bitstream/handle/1811/72839/1/ISJLP_V4N3_543.pdf; Manuel Rudolph, Denis Feth and Svenja Polst. (2018). "Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior." *Springer*. Available at: https://link.springer.com/chapter/10.1007/978-3-319-91238-7_45; Anca Micheti, Jacquelyn Burkell and Valerie Steeves. (2010). "Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand." *SAGE Journals*. Available at: https://journals.sagepub.com/doi/abs/10.1177/0270467610365355.

177 Office of the Privacy Commissioner of Canada. (2018). "Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency." *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/02_05_d_56_tips2/.

178 Patrick Gage Kelley, Joanna Breesee, Lorrie Faith Cranor, and Robert W Reeder. (2009). "A Nutrition Label for Privacy." *Carnegie Mellon University*. Available at: https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

> how an organization uses automated decision systems to conduct actions which could significantly impact individuals. While an organization may, per 15(3)(e) [of Bill C-11], identify the other organizations with which they disclose personal information in public facing documents such as privacy policies or terms or service agreements before obtaining an individual's consent, they may also present that information as an individual is in the process of signing up for a service. This latter approach would have the effect of requiring individuals to begin to sign up to a service before they could learn with whom their personal information may be disclosed.[179]

The same problematic language is included in C-27, under s. 62. As such, we recommend the following changes to C-27.

Recommendation 17: Require Greater Specificity Around Privacy Practices and Policies

To establish public trust, there needs to be greater transparency surrounding the types of personal information that organizations have control over, the use of personal information, the ways in which personal information impacts automated decision-making, and the parties to whom information is disclosed. As well, given the risk of re-identification, retention periods should be clear for identifiable information as well as anonymous and de-identified information.

Original C-27 Text	Proposed Legislative Amendment
Policies and practices 62(1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.	**Policies and practices** 62(1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.
Additional Information (2) In fulfilling its obligation under subsection (1), an organization must make the following information available: (a) a description of the type of personal information under the organization's control; (b) a general account of how the organization uses the personal information and of how it applies the exceptions to the requirement to obtain an individual's consent under this Act,	**Additional Information** (2) In fulfilling its obligation under subsection (1), an organization must make the following information available: (a) a specific description of the type of personal information under the organization's control; (b) a specific account of how the organization uses the personal information and of how it applies the exceptions to the requirement to obtain an individual's consent under this Act,

179 Christopher Parsons. (2021). "Canada's Proposed Privacy Law Reforms are Not Enough: A Path to Improving Organizational Transparency and Accountability." *The Citizen Lab*. Available at: https://citizenlab.ca/2021/04/canadas-proposed-privacy-law-reforms-are-not-enough-improving-organizational-transparency-and-accountability-bill-c11/.

including a description of any activities referred to in subsection 18(3) in which it has a legitimate interest;

(c) a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them;

(d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;

(e) the retention periods applicable to sensitive personal information;

(f) how an individual may make a request for disposal under section 55 or access under section 63; and

(g) the business contact information of the individual to whom complaints or requests for information may be made.

including a description of any activities referred to in subsection 18(3) in which it has a legitimate interest;

(c) a specific account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them;

(d) whether or not the organization carries out any international or interprovincial transfer or disclosure of personal information that may have reasonably foreseeable privacy implications;

(e) the retention periods applicable to all ~~sensitive~~ personal information, de-identified information, and anonymous information;

(f) how an individual may make a request for disposal under section 55 or access under section 63; ~~and~~

(g) the business contact information of the individual to whom complaints or requests for information may be made; and

(h) a listing of all the specific third parties to whom the organization discloses data, and the specific personal information, de-identified information, or anonymous information disclosed to those third parties.

C-27 fails to adequately enable individuals to request access to information held by private organizations, challenge automated decision-making processes, or secure information individuals have requested from private organizations. As in previous writing,[180] we recommend the following changes to the draft legislation.

180 Christopher Parsons. (2021). "Canada's Proposed Privacy Law Reforms are Not Enough: A Path to Improving Organizational Transparency and Accountability." *The Citizen Lab*. Available at: https://citizenlab.ca/2021/04/canadas-proposed-privacy-law-reforms-are-not-enough-improving-organizational-transparency-and-accountability-bill-c11/.

Recommendation 18: Empower Individuals to Request Access, Challenge Decision-Making Processes, and Secure Information

For individuals to have greater rights over their information, they need to be able to contact organizations with access to their information as well as make requests for this information. As well, where organizations are using personal information to automate decision-making, individuals should be able to challenge those decision-making processes or opt-out of these systems.

Original C-27 Text	Proposed Legislative Amendment
Information and access 63(1) On request by an individual, an organization must inform them of whether it has any personal information about them, how it uses the information and whether it has disclosed the information. It must also give the individual access to the information.	**Information and access** 63(1) On request by an individual, an organization must inform them of whether it has any personal information about them, how it specifically uses the information, how long it retains the information and whether it has disclosed the information. It must also give the individual access to the information.
Names or types of third parties (2) If the organization has disclosed the information, the organization must also provide to the individual the names of the third parties or types of third parties to which the disclosure was made, including in cases where the disclosure was made without the consent of the individual.	**Names or types of third parties** (2) If the organization has disclosed the information, the organization must also provide to the individual the names of the third ~~parties or types of third parties to which the disclosure was made, including in cases where~~ party organizations to whom information has been disclosed, the business contact information of the individual to whom complaints or requests for information may be made, and must include cases where the disclosure was made without the consent of the individual.
Automated decision system (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the pre- diction, recommendation or decision.	**Automated decision system** (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the pre- diction, recommendation or decision.

N/A	(4) In cases where an individual disputes the use of the automated decision system, they can opt-out of the system. In any case where an organization is unable to fulfill an opt-out request, the organization must notify the Office of the Privacy Commissioner of Canada and explain their rationale.
N/A	(5) In cases where an automated decision system could produce legal effects concerning the individual or materially affect them, decisions cannot be made based solely on an automated decision system.
N/A	(6) In cases where an individual disputes the accuracy or result of a decision reached using an automated decision system, they can have the decision reviewed by a member of the organization who possesses knowledge of how the automated decision system operates.
Request in writing 64(1) A request under section 63 must be made in writing.	**Request in writing** 64(1) A request under section 63 must be made in writing or recorded oral communication.
N/A	**Provision of Information** 70(1) An organization that provides information as a result of a request under section 63 must transmit that information to the individual in a manner that prevents unauthorized parties from accessing the communicated information.

Developing trust in the collection, use, and disclosure of personal, de-identified, and anonymous information requires companies to be compelled to disclose when and under what conditions they disclose information to government agencies, and companies must also publish their data retention schedules. As such, we recommend changes in C-27 that mirror our recommendations concerning C-11.[181]

181 Christopher Parsons. (2021). "Canada's Proposed Privacy Law Reforms are Not Enough: A Path

Recommendation 19: Require Private Organizations to Disclose Information Sharing with Public Entities

Though data flows between public and private entities are becoming more commonplace, individuals should understand how their data is being used by governing bodies, especially since government agencies often make policies and laws that can exacerbate harm to specific groups of people. Understanding which government agencies have access to personal information can allow individuals to make more informed decisions about their personal information.

Original C-27 Text	Proposed Legislative Amendment
Policies and practices 62(1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.	**Policies and practices** 62(1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.
Additional Information (2) In fulfilling its obligation under subsection (1), an organization must make the following information available:	**Additional Information** (2) In fulfilling its obligation under subsection (1), an organization must make the following information available:
N/A	(i) an annual transparency report that denotes the regularity of requests for individuals' information from domestic and international organizations, the regularity at which an organization responds to such requests in part or in full, and narrative explanations that clarify the specific conditions under which the organization discloses information to government institutions or removes or modifies information based on requests from government institutions or private organizations. Specific templates for reporting may be specified by the Privacy Commissioner, and the Commissioner may compel classes of organizations to produce these reports.

to Improving Organizational Transparency and Accountability." *The Citizen Lab*. Available at: https://citizenlab.ca/2021/04/canadas-proposed-privacy-law-reforms-are-not-enough-improving-organizational-transparency-and-accountability-bill-c11/.

N/A

(j) a comprehensive account of how an organization receives, assesses, and takes actions when a government institution or private organization requests information from the organization or requests that an organization modify or remove information that has been provided to it by an individual. Specific templates for developing this account may be created by the Privacy Commissioner, and the Commissioner may compel classes of organizations to produce these guidelines

(k) a specific account of the period of time for which an organization retains specific types of information.

Conclusion

The Canadian government's collection of de-identified mobility data from private companies has laid bare the issue of how de-identified data is treated under the law and the opaque ways in which government agencies can obtain and use information associated with residents of Canada. Mobility data can lead to a privacy quagmire insofar as current authorizing legislation may see private companies and government agencies alike collect, use, or disclose information in ways that are lawful but that seem inappropriate when held up to the public eye.[182] The reasons for this are many, but to at least some extent, they can reflect how there are changing understandings and experiences of privacy as digital technologies and geolocation capacities become embedded in individuals' daily lives and lived experiences.

The current governance of identified and de-identified personal information has led to a governance gap insofar as the law is ambivalent to the problem of function creep in how data is used. Moreover, under proposed privacy law in Bill C-27, data could be used in ways that individuals or their communities may oppose. These challenges are magnified by present failures to establish comprehensive, meaningful consent requirements concerning the collection, use, and disclosure of personal information as well as for personal information that has been processed into de-identified data. All of these issues are compounded when cast through the lenses of non-consensual collections, uses, or disclosures of information collected from Indigenous persons and their communities.

The proposed privacy law reforms in Bill C-27 would largely codify existing practices as opposed to addressing existing and potential harms. The Bill, in effect, requires substantive and meaningful amendments if it is to protect the interests of individuals living in Canada or Indigenous territories instead of primarily advancing the interests of businesses and government agencies. The legislation should be amended or redrafted to adopt a rights-forward perspective. Prof. Colin Bennett has noted that the title of C-27's predecessor, C-11, signaled this commercial framing given its focus on individuals as "consumers" rather than persons, and that the difference was striking with how the European Union's General Data Protection Regulation is constituted.[183] Drafting legislation toward an economic purpose rather than a rights-based purpose can and has led to corporate-forward legislation that leaves behind individual and community privacy rights. This is the wrong approach.

---

182 Michael Geist. (2022). ETHI Hearing, dated February 28, 2022.

183 Teresa Scassa. (2018). "PIPEDA Reform Should Include a Comprehensive ReWrite." Teresa Scassa. Available at: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80; Colin Bennett. (2021). "Canada's New Consumer Privacy Protection Act (Bill C-11): Will it Be Adequate" *Colin Bennett*. Available at: https://www.colinbennett.ca/canadian-privacy/canadas-new-consumer-privacy-protection-act-bill-c-11-will-it-be-adequatei/.

If the government's goal is to pass privacy law that respects the rights and dignity of Canadian residents, it should consider withdrawing C-27 and subsequently re-introducing legislation that is written to reflect the need for privacy-related legislation that protects human rights and ensures that collections, uses, and disclosures of personal information, including de-identified information, follow after a detailed equity and gender-based policy assessment process. Failing that, however, the recommendations suggested within this report ought to be adopted to better protect individuals and communities. These protections would, in part, take the form of better governing identified and de-identified data by:

- setting out an expansive definition of "de-identified data"
- restraining exceptions to knowledge and consent
- fostering public trust and accountability principles by ensuring that individuals are generally knowledgeable about the ways in which their data is collected, used, or disclosed
- empowering the OPC with greater capacity to audit privacy practices, make orders, and issue administrative penalties

To be clear, even the modest amendments that we set out in this report would not address many of the glaring deficiencies in the legislation. But they may, however, mitigate some of the worst consequences of how C-27 would govern private and public organizations' handling of identified and de-identified personal information generally, and mobility information specifically.

If the government of Canada is truly serious about ensuring that individuals and communities are involved in developing policies pursuant to themselves and their communities, ameliorating disadvantages faced by marginalized residents of Canada, and committing to reconciliation with Indigenous populations, it will commit to serious amendments of C-27. Our recommendations are made in the spirit of addressing the gaps in this new legislation that are laid bare when assessing how it intersects with PHAC's historical use of locational information. They are, however, only a start toward the necessary amendments for this legislation.

Appendix A–Methodology

In preparing this report, we consulted academic and public literature concerning the sensitivity of mobility information as well as literature on how information is de- and re-identified to denote the risks that mobility information can pose to individuals and their communities. We also relied on public sources to understand the conditions upon which mobility data was shared between private organizations and the Government of Canada. In doing so, we reviewed the recorded meetings conducted by ETHI Committee between January 31, 2022 and April 25, 2022, and its corresponding report, and government releases, informational campaigns, and procurement documents. In aggregate, this data provided us with a factual basis for how mobility information has previously been shared between private and public organizations, as well as the prospective harms that may arise from such information-sharing activities.

Having collected and analyzed empirical information and academic literature, we then performed a legal analysis to assess the lawfulness of mobility data collections and disclosures that took place between private and public organizations during the COVID-19 pandemic. Next, we undertook a legislative analysis of recent federal private sector privacy law reform efforts. This analysis was designed to determine how proposed privacy law reforms would, if at all, differentially govern the collection, use, and disclosure of mobility data between the public and private sector amid emergency and non-emergency situations. We compared this legislative analysis of Bill C-27 against Canada's current federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) over the course of the COVID-19 pandemic to appreciate how it might modify future handlings of personal information in identifiable and de-identifiable formats.

Appendix B–Summary of Recommendations Made by the ETHI Committee

- Garner public trust in the collection, use, and disclosure of mobility data by:
  - Creating mechanisms to regulate the collection, use, disclosure, sharing, storage, and destruction of Canadian mobility data and ensure transparency in doing so (Recommendation 12)
  - Outlining clear guidelines regarding the use of mobility data by federal institutions, which among other things, ensure that collected information is limited to the requesting department (Recommendation 6, 22)
  - Updating the COVIDTrends web page to indicate where the data originates from, what data provider(s) are providing the government with information, and update the website to include opt-out information (Recommendation 4)
- Better inform individuals of the collection of information through:
  - Informing Canadians of the collection as well as of its nature and purpose (Recommendation 5)
  - Requiring the option to opt out of data collection (Recommendation 1, 14)
  - Investing in digital literacy initiatives (Recommendation 20) and creating public awareness of mobility tracking and disease-surveillance initiatives (Recommendation 21)
- Amend privacy legislation to allow for a "privacy by design" model (Recommendation 19) that would include:
  - An expanded definition of "personal information" to include de-identified and aggregated data (Recommendation 8)
  - Standards for de-identifying data and governing its collection, use, and disclosure (Recommendation 9)
  - Prohibitions on re-identifying de-identified data and corresponding penalties (Recommendation 10)
  - Definitions for terms that enable exemptions to knowledge and consent to operate such "commercial interest" and "public good" (Recommendation 7)
  - Enhanced powers for the OPC including consultation requirements, auditing, investigation, and enforcement powers (Recommendation 2, 11, 13)
  - Necessity and proportionality requirements (Recommendation 18), transparency obligations (Recommendation 3), and a public education and research mandate in the *Privacy Act* (Recommendation 17)
- Create accountability mechanisms for both private and public sector entities by:

- Creating a framework for companies that generate, manage, sell, or use data (Recommendation 15)
- Conducting a public audit of the source of data and meaningful consent, collection, transmission, and use of data (Recommendation 16)[184]

184 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Collection and Use of Mobility Data by the Government of Canada and Related Issues." House of Commons. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/news-release/11736769.