UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Standing Committee on Access to Information, Privacy and Ethics:

Study on Collection and Use of Mobility Data by the Government of Canada

Submission by
Dr. Christopher Parsons
Senior Research Associate
Citizen Lab, Munk School of Global Affairs & Public Policy
University of Toronto

Introduction

1. I am a senior research associate at the Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto. My research explores the intersection of law, policy, and technology, and focuses on issues of national security, data security, and data privacy. While I submit these comments in a professional capacity they do not necessarily represent the full views of the Citizen Lab.

Background

2. I want to begin by recognizing and thanking the employees at PHAC, and other agencies, who have worked to combat the spread of COVID-19. My comments should not be taken to discredit the efforts that they have undertaken. Instead, my comments are meant to identify areas of data governance that need improvement with regards to the Government of Canada's use of mobility data, and personal and anonymized information more generally, as well as the management of such information by private organisations.

3. I define mobility data as location information that is derived from cellular networks, such as those operated by TELUS, as well as location information that is obtained by data brokers. Brokers often obtain information either by purchasing it from app vendors or by embedding tracking codes in smartphone applications, largely without the knowledge of the device owners.[1] With regards to PHAC's use of mobility data, information from TELUS and BlueDot was aggregated and anonymized prior to PHAC obtaining it.

A Chaotic Communications Environment

4. At the onset of the COVID-19 pandemic government agencies, nonprofits and academic units, and private organisations worked to help to mitigate the spread of the virus. The earliest days of the pandemic were chaotic in terms of information that was communicated by all levels of government. One area of confusion arose surrounding the extent to which these governments used mobility data and for what purposes.

5. As an example of this confusion, and as pertains to this study, on March 24, 2020, the Prime Minister addressed whether the government would seek information from telecommunications providers. He stated that "as far as I know that is not a situation

[1] https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

we're looking at right now."[2] He did leave open the potential that such information might be used in the future. The same day, Dr. Tam indicated that the option of using telecommunications mobility data should not be ruled out though did not indicate that such data was being used.[3] The day prior, March 23, 2020, Mayor John Tory stated the city of Toronto had access to telecommunications mobility data, though this was walked back in a statement: "The City of Toronto is not collecting cellphone location data, nor has it received any such data. The City of Toronto will not be using cellphone location data."[4]

6. A series of articles emerged by late April that considered how mobility data might be used to mitigate the spread of COVID-19. At the time, neither journalists or experts indicated a specific awareness that the Government of Canada was obtaining mobility data from telecommunications companies or BlueDot.[5]

7. Underscoring the challenges in understanding the Government of Canada's use of mobility data comes from looking at what, as an example, the Prime Minister stated about the government's use of mobility data versus what was revealed by non-government sources. The Prime Minister's remarks of March 23, 2020 do not indicate that location information was provided by BlueDot;[6] to understand the full nature of the agreement requires finding and reading a press release from the University of Toronto.[7] Of note, BlueDot's privacy policy does not indicate it is involved in collecting mobility data.[8]

---

[2] See: https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236.
[3] See: https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236.
[4] See: https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236.
[5] See as e.g.: https://ablawg.ca/2020/04/16/covid-19-and-cellphone-surveillance/; https://uwaterloo.ca/math/news/q-and-experts-privacy-vs-tracking-covid-19; https://theccf.ca/hed-police-are-using-phone-data-to-track-covid-patients-can-they-do-that/
[6] See: https://pm.gc.ca/en/news/news-releases/2020/03/23/canadas-plan-mobilize-science-fight-covid-19. "Support for BlueDot, a Toronto-based digital health firm, with a first-of-its-kind global early warning technology for infectious diseases. The company was one of the first in the world to identify the spread of COVID-19. The Government of Canada, through the Public Health Agency of Canada, will use its disease analytics platform to support modelling and monitoring of the spread of COVID 19, and to inform government decision-making as the situation evolves."
[7] See: https://www.utoronto.ca/news/u-t-infectious-disease-expert-s-ai-firm-now-part-canada-s-covid-19-arsenal. " … BlueDot will provide the federal government with insights and intelligence to help combat the virus – in part by using anonymous location data from hundreds of millions of mobile devices to see how the public health response is working. BlueDot is starting to produce metrics that allow the government to understand where social distancing has been effective, if people are following public health advice and where to deploy valuable resources."
[8] See: https://bluedot.global/privacy/

8. Continuing to underscore the challenges facing Canadians about how mobility data was used emerges from information that Minister Duclos provided to this committee on February 3, 2022. He noted PHAC had partnered in March 2020 with the Communications Research Centre at ISED to use data from TELUS. He also noted that Canadians could determine that mobility data was used if they visited the COVID Trends website.

9. In addition to the comments by Commissioner Therrien before the committee, who noted that learning about the use of mobility data requires an individual to know that the COVID Trends website exists and then browse to the bottom of the page, it appears that this information was unavailable to Canadians until December 2020. This was months after TELUS and BlueDot had begun providing mobility data to the Government of Canada. We can determine this by using the Wayback Machine, which archives web pages. As of November 30, 2020, the site did not include information pertaining to mobility data;[9] this information only appeared in Wayback Machine archives in a December 6, 2020 snapshot that shows the website had been updated on December 3, 2020.[10] Visiting the website, as of February 9, 2022 does not indicate where mobility data specifically comes from, nor indicate how individuals might opt-out of data collection should they so choose.[11]

10. I raise these points not to indicate that the government misled Canadians, per se, but that the information environment was chaotic. I entirely agree with Commissioner Therrien that it is highly unlikely that most Canadians, or even a significant minority of them, were aware of the Government of Canada's acquisition of mobility data, or that such information was being used to inform COVID-19 related policy making. This opaqueness sets the stage for transparency and consent issues associated with the collection and provision of this information, by private companies, to the Government of Canada.

11. I have four recommendations concerning COVID Trends. First, I **recommend** that the website be updated to make clear that individuals know the specific sources of mobility data the government is using.

12. Second, I **recommend** that the COVID Trends website be updated to include a link to TELUS' opt-out for the data-for-good program,[12] so that individuals can remove themselves from TELUS' data sharing with the Government of Canada if they so choose.

[9] See: https://web.archive.org/web/20201130160833/https://health-infobase.canada.ca/covid-19/covidtrends/.
[10] See: https://web.archive.org/web/20201206160519/https://health-infobase.canada.ca/covid-19/covidtrends/.
[11] See: https://web.archive.org/web/20220209104023/https://health-infobase.canada.ca/covid-19/covidtrends/.
[12] See: https://insightsoptout.telus.com/opt-out/telus-lbs/index.xhtml?lang=en.

13. Third, I **recommend** TELUS be compelled to incorporate the opt-out mechanism into all their customer portals (e.g., TELUS, Koodo, etc) in obvious ways so individuals know they have this option. This might occur as part of *PIPEDA* reform proposed by the committee.

14. Fourth, I **recommend** that the COVID Trends website be updated to let individuals opt-out of BlueDot's data collection, though with the recognition that it is presently unclear how BlueDot is collecting mobility data or how to opt out of this data collection..

Using Telecommunications Networks and Data Analytics Services for Health Surveillance

15. As of September 2021, there were 34 million wireless subscriptions in Canada.[13] Most Canadians reasonably expect that telecommunications providers, such as TELUS, will obtain information about the location of mobile phones to maintain or operate their network (e.g., for planning or maintenance business purposes). However, the disclosure of subscriber location information to parties in excess of network development and maintenance purposes—even in situations where information has been ostensibly aggregated and anonymized, and permitted in privacy policies or terms of service—functionally transforms the nature of the technical data that TELUS receives by transitioning it from service maintenance information to a generalised data asset.

16. While individuals may not perceive a violation of privacy when locational information is collected to service or maintain the network, they may when how the information is used changes, and especially when this takes place without their knowledge or meaningful consent. Privacy scholar Helen Nissenbaum refers to this situation as one where the norms pertaining to informational privacy have been violated; using data in different consequences can functionally have the effect of generating a privacy harm.[14]

17. I have no doubt that employees at TELUS and the Government of Canada were working in what they saw as the interests of Canadians when mobility data was shared with the Government of Canada in an aggregated and anonymized format. However, even aggregated or anonymized information can have population level effects when that information is used to guide policy making. Some communities may be forced to travel more frequently during the pandemic to fulfil essential work, and other communities may be less represented in mobility data if not all members in a household have a mobile

[13] See: https://www.cwta.ca/facts-figures/.
[14] "Privacy as Contextual Integrity" at https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr.

phone, and governments might modify how they allocate policing or service resources as a result of such mobility data. All of which is to say that even aggregated and anonymized data can have impacts on communities. It is insufficient to just consider whether an individual privacy violation has taken place—though it is possible that one may have occurred—and is imperative to also consider the community impacts of how data is collected or used in policy making or resource allocation.[15]

18. Turning to BlueDot, less information is available on the origins of their mobility data. From public information it seems to be from "using anonymous location data from hundreds of millions of mobile devices to see how the public health response is working."[16] More information is needed to know exactly how this location information is collected. If it is derived from the data brokerage economy—which largely operates unknown to the individual's who have their information is collected, and where that information is regularly and routinely re-identified[17]—then it would be troubling to see the Government of Canada participate in this arguably unethical, if ostensibly legal, brokerage economy.

19. I offer two recommendations. First, I **recommend** that the committee proposes a reform to the *Privacy Act* to require private vendors which provide either anonymized, aggregated, or identifiable information to government agencies be mandated to prove that they have obtained meaningful consent from individuals to whom the information relates before it is disclosed.

20. Second, I **recommend** that the committee propose *Privacy Act* reform that captures anonymous or aggregated information that is collected, or received, by government agencies. As we move into a world of big data—as Dr. Tam has noted is of interest to PHAC— aggregated and anonymous information can be used to drive policies affecting individuals and communities, and those individuals and communities do not lose an interest in the data simply because it is anonymous. This proposal should make clear that the Government of Canada will include equity assessments as part of any privacy analysis of how government agencies might use aggregated or anonymous information that they obtain, and also that approval is received from the Privacy Commissioner before launching a program associated with such information.

---

[15] We expand on this argument in the Citizen Lab's report, *Pandemic Privacy*, available at: https://citizenlab.ca/wp-content/uploads/2021/09/092721_pandemic-privacy_v3.pdf.
[16] See: https://www.utoronto.ca/news/u-t-infectious-disease-expert-s-ai-firm-now-part-canada-s-covid-19-arsenal.
[17] "Estimating the success of re-identifications in incomplete datasets using generative models" at https://www.nature.com/articles/s41467-019-10933-3/.

Meaningful Consent for Private Collection, and Public Use, of Mobility Data

21. Many companies obtain mobility data for commercial purposes. Sometimes, individuals must consent to a collection of information, such as when they are prompted to authorise an app's access to location information. Few users realise that consenting to such access may permit an app developer to access location information, and also see that information sold or made available to other companies by way of code implanted in the app. In these cases, an individual provides meaningful consent to the app developer's collection and use of location information for the purposes of providing a service. The same cannot be said of the third-parties that also collect or receive the same information.

22. Relatedly, while telecommunications subscribers must recognize that they share location information with telecom providers to receive service, they are less likely to be aware of (or understand) how the same companies might use that information for commercial purposes in excess of providing telecommunications services.

23. The Privacy Commissioner provides guidance to companies on what meaningful consent entails. Specifically, it requires organisations to emphasise key elements of the data collection, use, and disclosure; to enable individuals to control the level of detail they get about how to control the collection, use, and disclosure of their personal information; to provide individuals with clear options to say 'yes' and 'no'; to be innovative and creative, such as by providing just-in-time notices or using interactive tools or developing customised mobile interfaces; to consider the consumer's perspective; to make consent a dynamic and ongoing process; and to be accountable by way of being ready to demonstrate compliance. Notably, the OPC has indicated that express consent is required in situations where there is a use or disclosure of information that a user would not reasonably expect to be occurring, inclusive of "certain sharing of information with a third party" or "the tracking of location".[18] In the case of TELUS, individuals are not provided with meaningful consent to authorise the use of their personal information for non-telecommunications services purposes. The same is true of data brokers that receive mobility data unbeknownst to users. It is notable that the Alberta Privacy Commissioner, in an analogous investigation of TELUS's Babylon Health, found that express consent cannot be obtained merely by agreeing to a privacy policy.[19]

[18] See: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.
[19] See: https://www.oipc.ab.ca/media/1165666/P2021-IR-02.pdf at 218-221.

24. I **recommend** that the Government of Canada, whenever it is receiving either identifiable or aggregated and anonymized information derived from individuals from private organisations, be required to demonstrate that such information was collected by those organisations after individuals meaningfully consented to the collection and disclosure.

Deficiencies With the *Privacy Act*

25. The Privacy Commissioner, along with other experts, has all recognized that the *Privacy Act* is in dire need of updates. *PIPEDA* is focused on issues of obtaining consent prior to the collection, use, and disclosure of information, whereas in contrast the *Privacy Act* enables and justifies the majority of the federal government's data handling on the basis that the collection, use, or disclosure of personal information directly relates to a government agency's operating program or is consistent with the program's purpose. As I and colleagues have written previously, ""[d]irectly related to an operating activity" has been applied in contrasting ways. While the Treasury Board and Office of the Privacy Commissioner have previously assessed "directly related to an operating activity" through determining whether the collection, use, or disclosure is 'demonstrably necessary,' more recently, the Federal Court of Appeal has found that the Privacy Act imposes no necessity obligation on government institutions.[20] Accordingly, consent largely plays a role where government agencies wish to act outside of their mandate or to repurpose data that was collected for a different purpose."[21]

26. The *Privacy Act* presently empowers the government to collect significant volumes of information without the explicit knowledge or consent of individuals. As noted by Minister Duclos, the government's position is that anonymized and aggregated information falls outside of the scope of the *Privacy Act*. The result, today, is that the government asserts it is free to collect such information and, also, can re-use it for other purposes in excess of those that drove the data's collection in the first place. In the case of this study, PHAC has not indicated a desire, need, or intention to subsequently re-identify datasets (perhaps in combination with other datasets held by PHAC). Nevertheless, it could change that policy tomorrow given the current status of the *Privacy Act*.

27. The procurement order that brought the government's use of mobility data to the public's attention underscores the need to update the *Privacy Act*. The contract description calls for PHAC to obtain cell-tower/operator location information to analyse mobility data of

[20] Canada (Union of Correctional Officers) v Canada (AG), 2019 FCA 212 at para 40.
[21] See: https://citizenlab.ca/wp-content/uploads/2021/09/092721_pandemic-privacy_v3.pdf, p 34.

Canadian populations for a broad range of purposes including to: "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."[22] The contract's language, alone, is largely unbounded, though under the *Privacy Act* PHAC's use of the information could be broader still and remain lawful so long as PHAC does not use the data in excess of the agency's mandate.

28. Some of the present limitations of the *Privacy Act* can be corrected by updating the legislation. I **recommend** that the legislation be updated to include necessity and proportionality requirements, which would compel government organisations to demonstrate that identifiable or anonymized information is required to fulfil a specific activity, and that the sensitivity of the data is proportional to the activity in question.

29. I also **recommend** that the government update the *Privacy Act* to restrict government agencies from re-using information that they have acquired, absent re-acquiring an individual's meaningful consent for re-use where appropriate.

30. With regards to anonymized or aggregated datasets, I **recommend** that the *Privacy Act* be updated such that government agencies be required to ensure that meaningful consent is obtained before individuals are included in anonymised datasets, and that retention limits be placed on these datasets (commensurate with their level of de-identification and the sensitivity of the underlying data), that re-identification attempts be strictly prohibited, and that the Privacy Commissioner be empowered to assess the proportionality of any anonymised dataset programs.

31. I also **recommend** that in updating the *Privacy Act*, the government be required to establish a centralised location whereby individuals can assess the extent to which their own personal information has been collected, or received by, government agencies and the purposes for which it is being used. This location should also make clear where each government agency is receiving either personally identifiable information, or anonymized or aggregated information derived from personally identifiable information, and provide specific explanation of the programs for which the information was collected and used for.

---

22 https://web.archive.org/web/20220210191227/https://buyandsell.gc.ca/procurement-data/tender-notice/PW-21-00979277

32. Finally, I **recommend** that the committee, as part of its study, take up and again recommend its *Privacy Act* reforms that were in its 2016 study on the *Privacy Act*.[23]

Failures of Corporate Consent and Transparency Reporting

33. The reception and use of aggregated and anonymized information that is being investigated by this committee came from private companies which obtained information directly or indirectly from individuals. It is generally hard for individuals to understand how information is collected about them, how that information is used by the receiving organisation, or how those organisations share information with other parties. While individuals can read privacy policies these documents are known to be incredibly challenging to assess and understand. At the Citizen Lab we have run numerous projects where we investigate and analyse privacy policies, and routinely are left with questions as to whether information is actually being collected, used, or disclosed when organisations use words such as "may" or "could" in describing these kinds of activities.[24] It is rare for organisations to disclose identifiable third-parties with whom information is shared.

34. How private organisations govern the information in their possession is often contentious. One way they explain their governance involves publishing 'transparency reports'. These began as a way for organisations to disclose how often law enforcement and intelligence agencies sought information from them, the legal authority backing requests, the extent to which organisations provided information, and the number of subscribers whose information was disclosed. Since then, these statistics have been supplemented to include information about copyright takedowns, and there are growing calls for companies to also provide information concerning their handling of harmful speech.[25]

35. Transparency reports might also be used to communicate, in statistical and narrative formats, how often individuals' information—in identifiable or non-identifiable formats—are disclosed to third-parties for commercial or non-commercial purposes. The intent would be to make clear to service users, as well as the public more broadly, how the data economy operates and the extent to which personal information was being shared with other parties. To be clear, this would not perfectly correct information asymmetries between individuals and private organisations which collect their personal

[23] See: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP8587799/ethirp04/ethirp04-e.pdf.
[24] See as example: https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf; https://citizenlab.ca/2020/05/we-chat-they-watch/.
[25] For more, see: https://www.newamerica.org/oti/reports/transparency-report-tracking-tool/.

information or disclose it to other parties, but would provide some additional and important information to Canadians about how their information was being used.

36. I **recommend** that the committee proposes reforms to *PIPEDA* that would require private organisations to obtain meaningful consent from individuals before they can disclose either identifiable, or anonymous or aggregated, information to other third parties.

37. I **recommend** that the committee propose reforms to *PIPEDA* which would mandate private organisations to specify whether they, or third-parties they partner with, collect information, as opposed to using language such as 'may' or 'could', as well as specify the exact other organisations with whom information is disclosed, as well as the uses that the other organisations intends to use the information for.

38. I also **recommend** that the committee propose reforms to *PIPEDA* to mandate private companies to develop transparency reports. Such reports should build on existing optional reporting templates provided by ISED,[26] and more comprehensively include information about copyright takedowns, the handling of harmful speech the services identify using their services, and manners in which private organisations disclose identified and anonymous information alike to third-parties.

Organisational Information

39. The views I have presented are my own and based out of research that I and my colleagues have carried out at my place of employment, the Citizen Lab. The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and 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.

40. We use a "mixed methods" approach to research combining practises 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 practises that impact freedom of expression online, analysing 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.

[26] See: https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html.