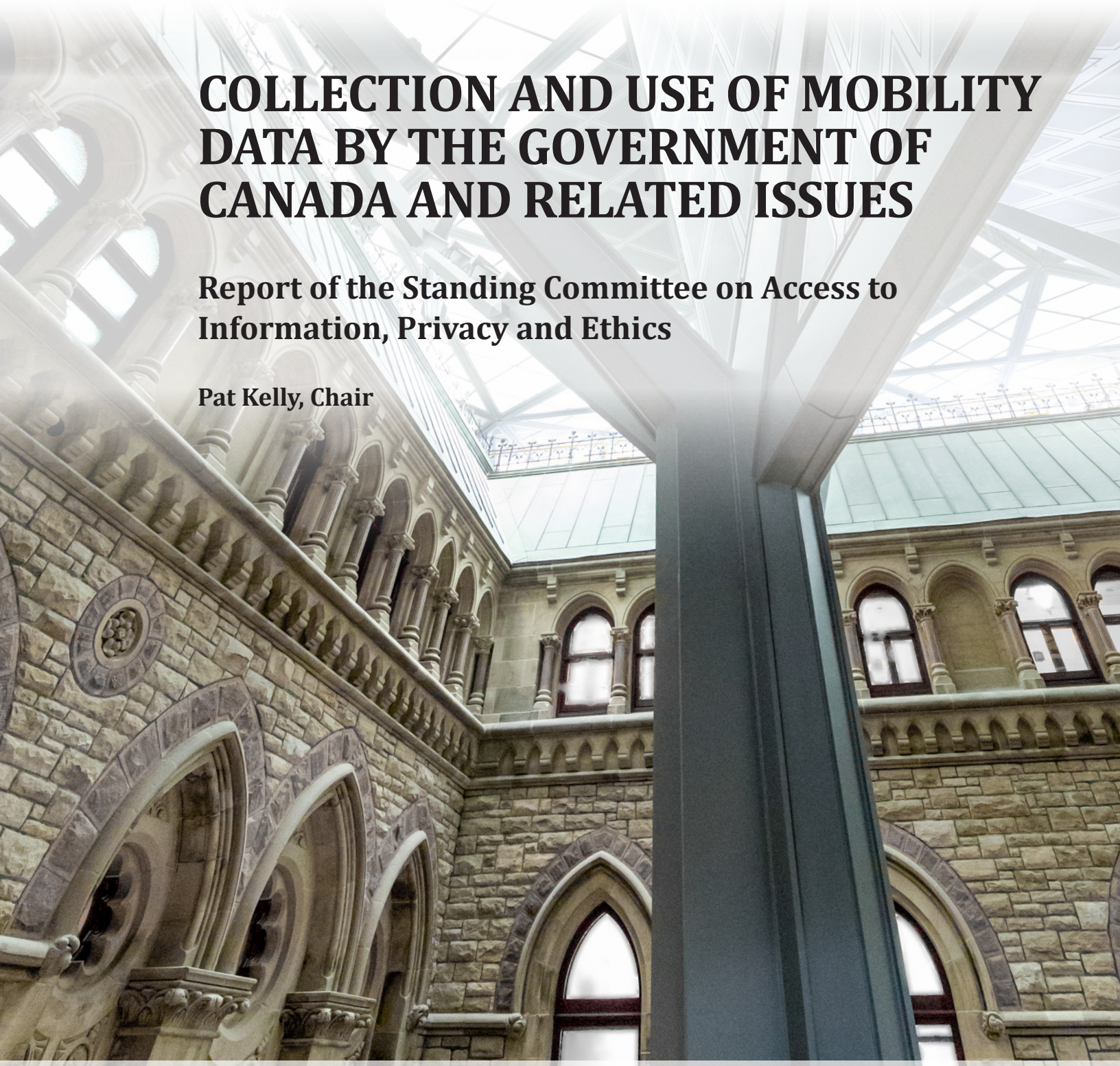
HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA



COLLECTION AND USE OF MOBILITY DATA BY THE GOVERNMENT OF CANADA AND RELATED ISSUES

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pat Kelly, Chair

MAY 2022
44th PARLIAMENT, 1st SESSION

COLLECTION AND USE OF MOBILITY DATA BY THE GOVERNMENT OF CANADA AND RELATED ISSUES

Report of the Standing Committee on Access to Information, Privacy and Ethics

Pat Kelly
Chair

MAY 2022

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIR

Pat Kelly

VICE-CHAIRS

Iqra Khalid
René Villemure

MEMBERS

Parm Bains
James Bezan
Hon. Greg Fergus
Matthew Green
Lisa Hepfner
Damien C. Kurek
Ya'ara Saks
Ryan Williams

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Richard Bragdon
John Brassard
Blaine Calkins
Julie Dabrusin
James Maloney
Jeremy Patzer
Sherry Romanado
Lianne Rood
Gerald Soroka
Len Webber

CLERK OF THE COMMITTEE

Nancy Vohl

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Sabrina Charland, Analyst

Alexandra Savoie, Analyst

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FOURTH REPORT

Pursuant to its mandate under Standing Order 108(3)(h), the committee has studied the collection and use of mobility data by the Government of Canada and has agreed to report the following:

TABLE OF CONTENTS

SUMMARY

During the COVID-19 pandemic, the government of Canada and other government around the world used technology to help them make public health decisions.

One such use of technology was by The Public Health Agency of Canada (PHAC) which used mobility data to assess population mobility patterns during the pandemic. On 17 December 2021, a tender was issued to allow PHAC to continue to have access to this type of data. It is in this context that the Committee sought to undertake a study on the collection and use of mobility data by the Government of Canada.

Government officials said that the use of mobility data respected privacy rights since the data was de-identified and aggregated and used to track the correlation between the spread of COVID-19 and population movement. They indicated that it was impossible to re-identify individuals with the data received. They also said that they were transparent, for example by making information about mobility data publicly available on the *COVIDTrends* webpage.

Companies that provided PHAC with access to mobility data reassured the Committee that no data identifying an individual was shared with government. They said that they use the best industry standards to share de-identified data responsibly.

Other witnesses agreed that based on the publicly available evidence on the PHAC case, it did not appear that the government had used anything other than properly de-identified data to assess mobility patterns.

Although there was wide consensus among witnesses that the use of mobility data for public health purposes was laudable, several witnesses did not believe that PHAC was sufficiently transparent.

One expert explained that there are reliable techniques to de-identify or anonymize data so that the risk of re-identification is very low. Some privacy experts noted that, since the risk of re-identification is never zero, de-identified data should fall within the scope of federal privacy laws.

Some witnesses highlighted the challenges of using mobility data and big data. They also discussed the social impacts that surveillance can have.

Finally, most witnesses agreed that federal privacy laws are in dire need of modernization.

In light of what the Committee heard, it makes several recommendations to ensure that there is an appropriate legal framework for data use in Canada.

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

Recommendation 2

Recommendation 3

Recommendation 4

Recommendation 5

COLLECTION AND USE OF MOBILITY DATA BY THE GOVERNMENT OF CANADA AND RELATED ISSUES

INTRODUCTION

On 11 March 2020, the World Health Organization characterized COVID-19 as a pandemic.[1]

In response to the pandemic, the Public Health Agency of Canada (PHAC) used mobility data to assess population mobility patterns. Mobility data consists of aggregated indicators derived from cell-tower/operator location data, or in some cases aggregated and de-identified GPS location data, that allow for an analysis on the mobility (or movement) of populations in Canada.[2] Questions about this use and PHAC's intention to continue to use mobility data in the future led the Committee to undertake this study.

On 13 January 2022, the Committee unanimously adopted a motion to undertake a study on the collection and use of mobility data by the Government of Canada.

In addition to the case study involving PHAC, the Committee examined issues related to the use of de-identified data and big data and the modernization of federal privacy laws. It also looked at the impact of surveillance and the importance of transparency in government institutions to ensure public trust. This report summarizes the evidence heard and includes recommendations to ensure an appropriate legal framework for data use in Canada.

In total, the Committee held six public meetings and heard 20 witnesses. It also received three briefs. The Committee thanks all those who participated in the study.

1 World Health Organization, *WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020*.

2 Buyandsell.gc.ca, *Operator-based Location Data and Services for Public Health Mobility Analysis (1000236419)*; Standing Committee on Access to Information, Privacy and Ethics (ETHI), *Evidence*, Kamran Khan.

CHAPTER 1: USE OF MOBILITY DATA BY THE PUBLIC HEALTH AGENCY OF CANADA

Table 1 presents a chronological overview of key events relating to the use of mobility data by the Government of Canada during the pandemic, which will be discussed in this chapter.

Table 1—Key Events relating to the use of mobility data by the Government of Canada

Date	Event
23 March 2020	News release from the Prime Minister's Office announcing that the Government of Canada will provide support to BlueDot and through the Public Health Agency of Canada (PHAC), 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.
24 March 2020	The Privacy Management Division (PMD) of Health Canada and PHAC indicates that there are no privacy concerns regarding the data that will be provided by BlueDot considering it is anonymized and irrevocably stripped of all its identifiers, a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining information is very low. It determines that no personal information will be received.
21 April 2020	Innovation, Science and Economic Development's Communications Research Centre (CRC), informs the Office of the Privacy Commissioner (OPC) of its intention to access de-identified mobility data from Telus to answer questions for PHAC on mobility trends.
22 April 2020	PHAC briefs the Office of the Privacy Commissioner (OPC) of its work on mobility data in April 2020. The OPC indicates that it was notified by PHAC of its intention to use mobile location data in response to COVID-19 and of the fact that the activity did not engage the *Privacy Act*.
24 April 2020	Health Canada and Blue Dot enter a contract. The contract period start date was 26 March 2020.
22 September 2020	The PMD issues its analysis confirming that data from Telus (Data for good program) is not considered personal information and therefore does not engage the *Privacy Act*. The PMD concludes that publishing the mobility data on a dashboard does not create privacy concerns.
21 December 2020	The PMD, relying on its previous opinion, indicates that the data provided by Telus through CRC does not constitute personal information.
24 December 2020	PHAC and Telus enter a contract. The contract period start date is 24 December 2020.

Date	Event
25 January 2021	PHAC consults the Public Health Ethics Consultative Group (PHECG) to discuss the ethics of mobility data use.
October 2021	The Telus contract expires.
October 2021	PHAC consults with the PMD in preparation for a Request for proposal (RFP) for mobility data.
17 December 2021	The RFP is published on buyandsell.gc.ca. The RFP specifies the security and privacy measures that bidders must satisfy. The tender was originally scheduled to close on 21 January 2021.
January 2022	The OPC receives complaints regarding the collection and use of mobility data by PHAC and starts an investigation.
6 January 2022	PHAC provides a technical briefing to the OPC.
12 January 2021	An amendment to the RFP postpones the closing date of the tender to 4 February 2022.
4 February 2022	An amendment to the RFP postpones the closing date of the tender to 18 February 2022.
18 February 2022	The tender expires.
18 March 2022	The BlueDot contract expires.

Source: Table prepared by the Library of Parliament using information obtained from the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) and public sources; Office of the Prime Minister of Canada, News release, 23 March 2020; ETHI, *Evidence*, 3 February 2022 (The Hon. Jean-Yves Duclos, Minister of Health); ETHI, *Evidence*, 7 February 2022 (Daniel Therrien, Privacy Commissioner of Canada); Public Health Agency of Canada, written response distributed to the Committee on 25 February 2022; Public Health Agency of Canada, Letter to ETHI, 11 March 2022; Office of the Privacy Commissioner, Letter to ETHI, 14 March 2022; Government of Canada, Tender Notice, 3 February 2022; Government of Canada, Request for proposal; Government of Canada, Bluedot Inc. - Contract Details; Government of Canada, Telus Communications Company - Contract Details; Public Health Agency of Canada, communication, 5 April 2022.

December 2021 Tender Notice

On 17 December 2021, the government issued a tender notice to give PHAC access to anonymized cell tower location data to assist in the response to the COVID-19 pandemic and for other public health applications. The request for proposal provided that the contract period starts on the date of award and ends on 31 May 2023, with three additional one-year option periods.

Christopher Allison, PHAC's Acting Vice-President, Corporate Data and Surveillance Branch, said that the idea behind the contract is that mobility data can be very useful for examining a range of public health problems and could be useful as PHAC gains experience in using such data effectively, ethically and while protecting privacy. The intent was to explore what could be done after the pandemic, but without predisposing any decision PHAC might make.

Dr. Ann Cavoukian, Executive Director, International Council on Global Privacy and Security by Design, and former Information and Privacy Commissioner of Ontario, said that it is critical to place specific limits on the use of data under the new contract; otherwise, it will always be used for other purposes. The Privacy Commissioner of Canada (the Commissioner), Daniel Therrien, said that he was not consulted about the tender, but that he did request and receive some information about PHAC's process surrounding the tender.

Heath Minister, the Hon. Jean-Yves Duclos, said that delays in acquiring mobility data could impact ongoing pandemic epidemiological monitoring activities. Chief Public Health Officer Dr. Theresa Tam said that gaps in mobility data reduce PHAC's ability to look at important policy measures in place, but that it can be retrospectively looked at. However, she noted that a retrospective analysis is not as good as a prospective analysis.

The tender was originally scheduled to close on 21 January 2022. An amendment dated 12 January 2022 postponed the closing date to 4 February 2022.

On 31 January 2022, the Committee unanimously adopted the following motion:

> That the committee call upon the government to suspend the Public Health Agency of Canada's cellular data tender upon adoption of this motion, and that the tender shall not be re-offered until the committee reports to the House that it is satisfied that the privacy of Canadians will not be affected, and that the committee report the adoption of this motion to the House at the earliest opportunity.

On 2 February 2022, the Committee presented its First report to the House of Commons. It reported the adoption of the above motion.

On 4 February 2022, a further amendment to the request for proposal pushed the closing date to 18 February 2022.

On 8 February 2022, the House of Commons passed a motion to concur in the Committee's first report. The vote was divided: opposition parties voting for the motion; the governing party voting against.

The government did not suspend the tender. The tender expired on 18 February 2022.

Committee Observations and Recommendations

The Committee acknowledges that, under the mandatory technical criteria in the December 2021 request for proposal, the bidder's plan had to demonstrate that it "grants users the ability to easily opt out of mobility data sharing program."

The Committee believes that it is important to ensure that in any tendering process Canadians understand that they can opt out of data collection. It also notes that, as will be explained in this report, it is often hard for individuals to understand privacy policies. It therefore recommends:

Recommendation 1

That the Government of Canada stipulate in all future requests for proposals for collecting data of Canadians that Canadians have the option to opt out of the data collection and that instructions for the method for opting out be easily understood, widely communicated and remain publicly available.

However, the Committee acknowledges that, in some cases, opting out of data collection may not be in the public interest. Chapter 3 of this report discusses the use of data for socially beneficial purposes, and Chapter 4 discusses changes to federal privacy laws to better govern the use of de-identified data, among other things.

Initial Access to Mobility Data

Minister Duclos explained that, in March 2020, PHAC started using mobility data. In partnership with the Communications Research Centre (CRC) under Innovation, Science and Economic Development (ISED), PHAC used anonymized, de-identified, and aggregated location data. Data was provided under a sole-source contract with the Telus Data for Good program, which expired in October 2021. PHAC also entered into a contract with BlueDot. That contract was set to expire on 18 March 2022.

Minister Duclos said that, in April 2020, it was determined that the information used was not private or confidential, and followed the laws and regulations of Canada. In a letter to the Committee dated 14 February 2022, Dr. Harpreet S. Kochhar, President of PHAC, confirmed that government privacy experts conducted a privacy assessment to determine whether the data PHAC would receive should be considered personal

information under the *Privacy Act*. They concluded that the data did not contain personal information and that its use did not contravene the *Act*.

PHAC provided the Committee with documentation relating to the Privacy Impact Assessment that was conducted on the Government's use of mobility data. They show that in March 2020, the Privacy Management Division of Health Canada and PHAC (PMD) determined that the contract with BlueDot did not raise any privacy concerns given the nature of the data (anonymized) and the fact that Health Canada would not be receiving any personal information. The PMD noted that if personal information was received, then certain measures would have been included in the contract.[3]

In September 2020, the PMD's Privacy Analysis of the PHAC Mobility Data Dashboard Project concluded that given Telus's extensive aggregation process, the data received by PHAC did not meet the definition of "personal information" under the *Privacy Act* and therefore the Act did not apply. The PMD was of the view that the release of the data would not result in any subsequent privacy issues.[4] The PMD reiterated that the data provided by Telus through the CRC was not personal information in December 2020.[5]

Mr. Allison also said that experts consulted by PHAC and the Public Health Ethics Consultative Group (PHECG) concluded that no personal or private information was part of the mobility data accessed by PHAC or the December 2021 request for proposal. Dr. Tam confirmed that PHECG took note that PHAC used de-identified and aggregated data to prevent privacy breaches.

PHAC Executive Vice-President, Kathy Thompson, confirmed that PHAC's contracts with Telus and BlueDot, as well as the December 2021 request for proposal, included a number of requirements to protect the privacy of Canadians and to ensure that PHAC cannot identify any single individual.

In October 2021, while evaluating a Statement of Work for an anticipated request for proposal, the PMD determined that, unless the process for obtaining mobility data was modified, its prior analysis applied and that there were no privacy concerns related to

3 Public Health Agency of Canada, Letter to the Committee, 11 March 2022, p. 13.

4 Ibid., pp. 34-35. The Privacy Management Division of Health Canada and the Public Health Agency of Canada made reference to the Treasury Board of Canada Secretariat's *Privacy Implementation Notice 2020-03: Protecting privacy when releasing information about a small number of individuals*.

5 Ibid., p. 46.

the mobility data that the government would access as a result of the request for proposal.[6]

According to Minister Duclos, the government met the two conditions for protecting privacy: to ensure compliance with laws and to ensure "that the data collected cannot create any issue or risk in relation to the protection of privacy." When asked if the actions of the government were ethical, Minister Duclos said that "in the context of COVID-19, the Canadian government has an ethical, moral, economic and health obligation to protect the safety and health of people, while absolutely protecting the privacy of people."

Telus and BlueDot: Type of Access

Mr. Allison said that data was used from approximately nine million subscribers through the Telus Data for Good program. Mobility data from approximately five million mobile devices was used by BlueDot to provide reports to PHAC.[7]

Pamela Snively, Vice-President, Chief Data, and Trust Officer with Telus, said that the Data for Good program was launched in April 2020. She said Telus did not share "one iota" of personal information with the government. The datasets never left Telus's systems. The program operates on the Insights platform, which uses de-identified datasets from Telus's network to reveal movement trends and patterns while protecting individual privacy.

Mrs. Snively explained that Telus provides guided and supervised access on the Insights platform to its partners' data scientists. They can run queries that are consistent with the intended use and purpose, as long as they fit with the program. They are able to create derived data or "insights" such as a heat map or graph, a bar chart or line graph that shows movement patterns or trends. These "insights" can be downloaded after Telus reviews them to make sure that they are consistent, that they meet re-identification risk metrics and that they are consistent with the purpose of the contract.

Mrs. Snively explained that Telus built the technical platform and technical rules to de-identify the data and strip the identifiers. Rules govern how queries are made and control the frequency with which they are made. Administrative controls, such as guided and supervised access and strict contractual controls prohibiting re-identification,

6 Ibid., pp. 36 to 57.

7 Dr. Kamran Khan, BlueDot's founder and CEO, confirmed this figure.

are in place.[8] Mrs. Snively confirmed that Telus and experts conducted rigorous re-identification tests and attacks to ensure that the process was bulletproof. She also confirmed that Telus never provides real-time data because it increases the risk of re-identification.

Mrs. Snively said that the Insights platform is the only secure data analytics platform of its kind in Canada that is "Privacy by Design" certified, an international standard that goes beyond Canadian legislative requirements to entrench privacy protections into the design and operation of the IT systems, networks, and business practices of an organization.[9] The framework was created by Ms. Cavoukian who said that it is included in the European Union's General Data Protection Regulation (GDPR) and that it "builds privacy and embeds it into the code of your operations."

Dr. Kamrar Khan, BlueDot's founder and CEO, said the location data BlueDot receives is de-identified, sometimes also pre-aggregated, and sometimes delivered at the device level. He said that BlueDot has numerous procedures in place, both administrative and security procedures, to manage and keep the data in a secure environment. He said there is no conceivable way that the outputs that BlueDot analyzes, produces, and delivers to PHAC could be reassociated with any individual. BlueDot's two data providers are Pelmorex Corp and Veraset LLC.[10]

Dr. Khan explained that the information BlueDot has is in highly secure cloud environments, with full levels of encryption. He added that the company works with independent third parties to enhance its data security practices.

Alex DeMarsh, Director of Data Science with BlueDot, confirmed that the company provides analytic reports to PHAC. It also makes the same kind of metrics available through a dashboard, which PHAC can use to view this type of analysis directly. Only summary metrics are available on the dashboard.[11]

---

8 ETHI, *Evidence*, Pamela Snively (Vice-President, Chief Data, and Trust Officer, Telus Communications Inc.).

9 For more information on this standard, see Alexandra Savoie, Privacy by Design: Origin and Purpose, Library of Parliament, 9 December 2021.

10 Names obtained following a motion adopted by the Committee on 3 March 2022.

11 The Committee received two examples of weekly reports prepared by BlueDot for the Public Health Agency of Canada (PHAC) entitled "Canada Mobility Trends." The first, dated 4 October 2021, covered the period from 19 to 25 September 2021. The second, dated 13 December 2021, covered the period from 28 November to 4 December 2021. The reports provided statistics on mobility in Canada. Before joining BlueDot, Mr. DeMarsh worked in PHAC's Emergency Operations Centre, building and refining data systems used for more traditional public health data. He confirmed that he had no involvement in decisions leading to the contract with BlueDot.

Mr. DeMarsh explained that, when BlueDot receives data from an individual device, it contains only an approximate location and a time stamp (no identifying information). He clarified that the reference to a "home" in BlueDot reports is the primary location of the device. The analysis aims to distinguish between devices that are staying close to their primary location and those that are moving about as a proxy for contact rates in the population.

Mr. DeMarsh explained that, even in a rural setting, the smallest geographic boundary would be defined by the underlying population as calculated by Statistics Canada, and therefore relatively large. He also pointed out that BlueDot only reports statistical summaries, numbers of devices, and proportions and percentages; there would be nothing conceivably identifiable or associated with an individual device.

Utility of Mobility Data and Initiative Effectiveness

Minister Duclos pointed out that mobility data is used all over the world.[12] He said that experts and researchers from the U.S. Centers for Disease Control and Prevention and the European Commission's Joint Research Centre say that "mobility explains transmission and spread and can reduce mortality and mitigate the need for lockdowns." He pointed out that, in Canada, where the death rate from the pandemic was lower than any other G7 country except Japan, the use of scientific information and data saved tens of thousands of lives.

Minister Duclos added that the anonymized, aggregated mobility data was used to monitor the trajectory of the pandemic and how best to respond to it. This information helps governments determine how the public is responding to public health directives so that they can tailor their approach and communications.

Dr. Tam said mobility data is useful in the fight against the pandemic. She said de-identified, aggregated mobility data is an important tool now and moving forward. It helps determine whether there is an outbreak in a certain location. It can help determine how mobility patterns are changing between different areas and point to disease spread potential. It can also help jurisdictions look at the effectiveness of their public health measures.

12 ETHI, *Evidence*, Hon. Jean-Yves Duclos (Minister of Health). The Minister named the following countries: United States, United Kingdom, Australia, Spain, Germany, Argentina, Brazil, Colombia, Ecuador, Netherlands, Italy, Greece, Austria, Bulgaria, Croatia, Denmark, Estonia, Finland, Portugal, Slovenia, Sweden, and Norway.

Dr. Tam said that, in general, public health lacks information. In her view, public health is insufficiently capacitated, particularly as it relates to the use of big data. Dr. Tam reiterated that public health needs more capacity, more tools, and more platforms, including data platforms, to inform its decisions. She noted that the application of big data in public health is in its infancy.

Dr. Tam said that, given the newness of mobility data, indicators for success are at the initial stages of the set-up for this type of data. She also said that she could not point to a specific PHAC policy that was developed using mobility data, as provinces receive the data and use it for their own applications.

Dr. Khaled El Emam, Canada Research Chair in Medical Artificial Intelligence, confirmed that many countries around the world are using mobility data for public health surveillance purposes.[13]

Dr. Khan said he believes that analytics and technology can help us stay ahead of outbreaks that we will face again and protect lives, our way of life, and data privacy. He explained that mobility data, unlike traditional public health data, such as the number of cases or hospitalizations, allows for a shift from being reactive to being proactive and anticipatory. The goal is to estimate contact rates in the population—a leading indicator of what is coming next. The goal is to get in front of an outbreak, not to be behind one.

Dr. Khan said that in the past two years there have been many instances of the analytics that BlueDot has provided to PHAC being "precursors of subsequent surges or providing really important actionable insights." He said that not having that information is like fighting an outbreak with a blindfold on.

Consultation with the Privacy Commissioner

Minister Duclos said that the government had worked with the Privacy Commissioner from the start. He said:

> The experts, the legal experts, of the Government of Canada determined early in the process, with the collaboration of the various other experts, including comments made and advice provided by the Office of the Privacy Commissioner, that this information was not private and therefore did not follow the *Privacy Act*. Despite that, biweekly

13 Dr. Khaled El Emam said that, because of his type of expertise, he has had the opportunity to work with many departments and different parts of the federal government over the past 20 years, including Health Canada and the Public Health Agency of Canada.

> meetings have been held with the Privacy Commissioner since April 2020, and continue to today.[14]

Minister Duclos said that the Privacy Commissioner was informed about the data mobility initiative and that there was a conversation right at the start of the pandemic, in April 2020. He stated that the Privacy Commissioner and his office have an incredibly important job to do and that their advice, input and guidance are key to everything the government does. He repeated that PHAC was engaged from the very start of the pandemic with the Office of the Privacy Commissioner (OPC), starting in April 2020, and biweekly after that. He added: "We will continue to work with the OPC as we proceed through the crisis."

Mr. Therrien said:

> In the case of the government's use of mobility data, we were informed of their intent to use data in a de-identified and aggregated way. We offered to review the technical means used to de-identify data and to provide advice, but the government relied on other experts to that end, which is its prerogative.

Mr. Therrien specified:

> On the facts of whether we were consulted or informed, and what was the tenor of these discussions, we were informed by PHAC and a group within the innovation department that the government wanted to use de-identified information for the purposes outlined: i.e., use mobility data to determine trends in mobility for public health purposes.
>
> We were informed of this as part of regular meetings with government agencies on any number of COVID alert issues. At that time, we were heavily involved in the COVID Alert app, among other things, so we were informed of this particular project.

Mr. Therrien said that, on 21 April 2020, CRC informed his office that it intended to access de-identified data from Telus to answer questions for PHAC on mobility trends. The OPC wrote to CRC explaining that, to determine whether adequate safeguards were adopted and whether its *Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19* (the OPC's framework) was adhered to,

14 ETHI, *Evidence*, Hon. Jean-Yves Duclos (Minister of Health).

CRC would need to enter into a formal engagement with the OPC's Business Advisory Directorate. CRC opted not to pursue that process.[15]

Mr. Therrien indicated that, on 22 April 2020, PHAC contacted the OPC to notify them of its intention to use mobile location data in response to COVID-19 and that it believed the activity did not engage the *Privacy Act*.[16] Mr. Therrien noted: "We don't have a role to pre-authorize every government initiative, so we left it at that."

According to PHAC, it briefed the OPC on its work on mobility data in April 2020. The OPC did not express concerns or request further information. PHAC continued to meet with the OPC every two weeks to provide updates, including on the initiative noted above. PHAC stated that, other than raising concerns at one meeting about Statistics Canada's plan to publish data, the OPC did not inquire about the initiative again until December 2021.[17]

Mr. Therrien explained that, when the OPC is engaged in an initiative, it receives information so as to be able to say not only that in principle privacy is protected, but also that it has looked "under the hood" to ensure that personal information is indeed protected. M. Therrien added:

> We offered to provide advice. Is it normal that we not intervene in every case? I think the reality is that we, as an office, cannot be involved in pre-authorizing or reviewing every case of data collection or disclosure that occurs in Canada. We give general advice that we hope is followed. We investigate complaints.
>
> I think that in the new law our office should have greater powers to proactively audit the practices of governments and the private sector, but unfortunately it is just not realistic to expect that we will pre-approve every use or disclosure of data in this country. At the end of the day, it is to the benefit of Canada that data is shared, obviously for good reasons—for legitimate commercial interests, for the public good, and not for illegitimate surveillance as we've seen in certain cases.
>
> Because these practices occur all the time, we just cannot be there all the time.

15 Office of the Privacy Commissioner of Canada (OPC), *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*, 14 March 2022 (OPC Letter of 14 March 2022). The OPC's framework was published in April 2020.

16 Ibid.

17 Public Health Agency of Canada, written response prepared by the Public Health Agency of Canada distributed to the Committee on 25 February 2022.

Mr. Therrien confirmed that in PHAC's case the information provided to his office was, in principle, consistent with his office's framework, but that he offered "to go under the hood to determine if the data had indeed been de-identified properly, but the government declined that offer."[18]

M. Therrien however, noted that he is not the only privacy expert; the government and telecommunications companies also have experts.

Mr. Therrien indicated that the OPC has received complaints regarding the use of mobility data by PHAC. He explained:

> Now that we have received complaints, we will investigate and turn our attention to the means chosen for de-identification and whether they were appropriate to safeguard against re-identification. Since this is under investigation, we will not be able to provide you with advice on this aspect of your study.

Mr. Therrien said that he could not confirm that the government did receive anonymized or de-identified data:

> I cannot, because that is the subject of the investigation we are going to have to conduct as a result of the formal complaints we have received under the law.
>
> What I can say is that we have had discussions with PHAC. They informed us, again, that they intended to use de-identified or aggregated data for public purposes, such as public health. This is consistent with our understanding of privacy principles.
>
> As to whether the data was de-identified properly, we don't know yet. We will investigate.

Committee Observations and Recommendations

The Committee notes the Commissioner's comments on his role but believes that when the government engages in data collection it should meaningfully consult with the OPC. It therefore recommends:

Recommendation 2

That the Government of Canada fully and meaningfully consult with the Privacy Commissioner of Canada before engaging in a data collection program and continue to do so on an ongoing basis for the duration of the program.

18 ETHI, *Evidence*, Daniel Therrien (Commissioner).

Transparency and Trust

Government Transparency

Minister Duclos argued that PHAC's access to mobility data during the pandemic was fully transparent as the Prime Minister announced it in March 2020 and the data is publicly available on the *COVIDTrends* webpage.[19] He noted that, since 2020, 1.7 million Canadians have been able to see the data on the webpage and that the process is public.[20] Despite the government's efforts, many witnesses thought that the process was not fully transparent.

Mr. Therrien said:

> There is then the question of transparency and consent. Did the government or its private-sector partners adequately inform users that their mobility data would be used for public health purposes? While there is a reference to the "data for good" program somewhere in Telus's privacy policies, and while the government does make an effort to inform citizens of its use of mobility data on its *COVIDTrends* web page, I do not think anyone would seriously argue that most users knew how their data would be used.

Mr. Therrien noted that "consent is not a silver bullet or a solution for all cases." According to him, "most Canadians whose data was used did not know their data was used." Consequently, he was of the view that "both the government and the private sector, could have done more to inform users that their data was used for these purposes."

Dr. Cavoukian did confirm that the government was not surveilling Canadians. She praised the Telus Data for Good program, noting that she had no problem with the Insights platform. She indicated that her concerns were with the government's lack of transparency.

Dr. Cavoukian said that PHAC showed a complete lack of transparency. She said that if she hadn't been consulted about such an initiative when she was the Information and

---

19 On 23 March 2020, the Prime Minister published a news release on Canada's plan to mobilize science to fight COVID-19 in which it indicates that the Prime Minister announced: "Support for BlueDot… The Government of Canada, through the Public Health Agency of Canada, will use its disease analytics platform to support modelling, to monitor the spread of COVID-19, and to inform government decision-making as the situation evolves." The news release does not mention Telus.

20 Dr. Christopher Parsons, Senior Research Associate with Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, said the COVIDTrends webpage only began publishing public information about the source of mobility data in December 2020.

Privacy Commissioner of Ontario she would have been extremely concerned. She explained:

> I want to be clear that they did go to great lengths to strongly de-identify the data and then use it in aggregate form. That does minimize the risk of reidentification. I don't want to suggest otherwise. I'm just saying that with mobility data—your cellphone, which lives with you and basically goes everywhere with you—there is such sensitivity associated with that and all the locations you go and who you may associate with, if the data were able to be reidentified and connections made on the part of the government, I think that would be extremely troubling.
>
> So at the very least, the government should have provided notice to the public saying, "This is what we're doing. Here's why we're doing it. We want to track your movements in this COVID pandemic world." Is that a sufficient reason? Would people have felt the return was sufficient? We have to have some debate about these issues. PHAC can't just decide to do that… without telling anybody. That's what I objected to the most—the total lack of transparency.

Dr. Cavoukian suggested that alerting the Commissioner and asking for his input and assistance in making sure the public was aware of what was taking place would have allowed the Commissioner to confirm that the data was de-identified and aggregated or even give consent.

Dr. David Murakami Wood, Director of the Surveillance Studies Centre and Associate Professor, Department of Sociology, Queen's University, said that at no stage was there any suspicion of tracking or surveillance of individual Canadians, nor was there any indication that the mobility data was de-anonymized or disaggregated.[21] He said the problem in the PHAC case was "a lack of coherent communication and transparency by all levels of government involved."

Jean-Pierre Charbonneau, a former Quebec parliamentarian and speaker on ethics, suggested that if the government had been transparent, the Committee would likely not have had to conduct its study relating to mobility data. He was of the view that the government should have used the mechanism that is in place, the Privacy Commissioner, to verify that the processes were adequate. He suggested that the reason the government may not have wanted to involve the commissioner may have been because it was too complicated or because it was afraid of the advice it might receive. However, Mr. Charbonneau stated: "if you're not afraid, why not act transparently?"

21 Dr. Harpreet S. Kochhar, President of the Public Health Agency of Canada (PHAC), said in a letter to the Committee dated 14 February 2022 that "PHAC does not have the ability to reverse engineer this data nor does it have any interest in doing so as the value of the data lies in the population level of mobility."

Dr. Michael Geist, Professor of Law, University of Ottawa and Canada Research Chair in Internet and e-Commerce Law, said the Commissioner should have been more actively engaged in the process. He also said the public needed to have been better informed, giving the COVID Alert app as an example of an initiative that was better communicated and explained to Canadians. He commented that, if you want people to trust in programs, you need to explain in as many forums as possible and as clearly as possible what data is collected and what is being used. In his view, that process did not happen in the PHAC case.

Dr. Martin French, Associate Professor in the Department of Sociology and Anthropology at Concordia University, said that PHAC and the governments are doing a good job, but could go further in terms of communication. He also gave the COVID Alert app as an example, whose privacy policy is posted online and is much more reader friendly than most policies.

Dr. Daniel Weinstock, professor of philosophy at McGill University, suggested that if the government had provided the same type of justification that it provides when it imposes restrictions, it is highly likely that the issue of trust and distrust would not have arisen.

Dr. Weinstock said that he was not "hypothesizing that the current use of data by the government is wrong and reprehensible" but was "wondering about the conditions that can inspire trust among the general public." He was of the view that an elected official should inform the public, as "decisions on issues as crucial and sensitive as data use should be entrusted to elected politicians." He also noted that excluding the OPC raises suspicion when there might not be anything to hide and said that "[i]t becomes increasingly paradoxical that the government chooses to sideline a trust-building institution."

Dr. Murakami Wood agreed that PHAC needed to use mobility data for public health purposes, but said that safeguards had not been made public or accessible in an adequate way. Dr. David Lyon, Professor Emeritus at Queen's University, agreed.

Dr. Christopher Parsons, Senior Research Associate at Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, said that the earliest days of the pandemic were chaotic in terms of the information that was communicated by all levels of government. For example, he noted that the Prime Minister's official announcement

on 23 March 2020 that the government was partnering with BlueDot did not specifically refer to mobility data.[22]

Dr. Parsons stated with respect to his comments on the chaotic nature of the information at the beginning of the pandemic:

> I raise these points not to indicate that the government misled Canadians per se, but that the information environment was chaotic and is yet to be adequately corrected. To begin this correction, I suggest that the committee recommend that the *COVIDTrends* website be updated to make clear the specific sources of mobility data the government is using, as well as including an opt-out from Telus's "data for good" program and enabling individuals to opt out of BlueDot's collection of information. Further, the committee should recommend that Telus incorporate the opt-out mechanism into all of its customer portals, for both Telus and Koodo, in obvious ways so individuals know they have this option.

Dr. Geist made a similar suggestion. Asked about the right to opt out of a data collection program during a temporary situation like a pandemic or an emergency, he said:

> I think it depends a little bit on the kind of data. It's an interesting question to pose: Can you opt out? Well, you can opt out, certainly, or you ought to have the right, I would say, to opt out of a program like this…
>
> We are anxious to get more data. The ability to opt out in those circumstances would seem to be appropriate. There might be circumstances, though, where the dependence of public health does require certain kinds of disclosures.

Dr. Alain Deneault, professor of philosophy at the Université de Moncton, criticized the opacity of the government's activities with respect to the use of mobility data, noting that this lack of transparency makes it difficult to know whether data was used in a fair way or for purposes other than those for which it was intended.

Transparency of Mobility Data Providers

With regard to Telus, Mrs. Snively noted that public communication about the Data for Good program was intentional and explicit. Telus published five core data use commitments on its website on how it would share de-identified data and protect privacy, along with a full description of the program, and frequently asked questions.

22 Christopher Parsons, *Brief to ETHI Committee: Study on Collection and Use of Mobility Data by the Government of Canada*, 18 February 2022, pp. 1-4 (Brief submitted by Dr. Christopher Parsons).

Mrs. Snively said that Telus also did op-eds and interviews with *The Globe and Mail* and other Canadian media outlets, published news releases and publicized a privacy award won in 2020.

Mrs. Snively also said that Telus consulted the OPC on its transparency plan, providing an overview of its five commitments and incorporating the OPC's feedback into its program.[23]

Mr. Therrien said that Telus informed the OPC on 8 April 2020 that it intended to share de-identified, aggregate data with governments, health authorities, and academic researchers in an effort to support work to respond to the COVID-19 crisis.[24] The OPC reviewed the public statement that Telus intended to issue and offered its comments. It suggested that Telus may wish to consult its Business Advisory Directorate if and when it had concrete proposals or initiatives with governments, researchers or third parties. It also expressed interest in receiving a technical briefing on Telus aggregation and de-identification methodology. Telus did not consult the OPC's directorate or provide a briefing.[25]

Increasing Public Trust in Government Institutions

Dr. Weinstock said that what increases trust in the process is if there are very clear, self-imposed limits by the government. For example, he recognized that there are important uses that could be made of data that in other circumstances Canadians would expect to be private. Publicity about the end use of data, limits on it such as how long it can be used, and what indicator shows the end of the emergency that justifies the extraordinary use of data, would help reduce some of the uncertainty people have.

Polarization can also have an impact on public trust. Dr. Weinstock said that this is a multi-player game and that the media "are always on the hunt for missteps to increase polarization or draw attention." He feels that elected officials should take steps to reduce polarization; throwing oil on the fire simply creates scandals where none exist. Dr. Weinstock said that, while it is highly likely the data used by PHAC is perfectly harmless, "hiding things and overlooking the Privacy Commissioner makes it look as though something is off, which has a tendency to fuel polarization rather than reduce it."

23 ETHI, *Evidence*, Pamela Snively (Telus).

24 OPC Letter of 14 March 2022.

25 Ibid.

Dr. Murakami Wood echoed Dr. Weinstock's comments, noting that the PHAC case risks decreasing trust directly because of the government's actions, which lead the public to suspect that something is wrong, but also by decreasing trust indirectly. He said that politicians have engaged in hyperbole and exaggeration for political gain. He gave the example of news reports saying that 33 million Canadians are being tracked, which leads people to believe that their individual conversations are under surveillance when that is not the case.

Dr. Murakami Wood added that partisanship and public health are unfortunately in a death struggle, which he believes is not beneficial. He said partisanship has played into ways the PHAC case is understood. Dr. Weinstock said that, in prolonged emergency situations, "people expect politicians to rise above partisan politics."

Mr. Charbonneau said that, in terms of ethics, the government acted in secret. As indicated above, he was of the view that by keeping the OPC at a distance, the government prevented it from playing its oversight role.

Mr. Charbonneau said:

> Let me emphasize once again that we have the Office of the Privacy Commissioner. Basically, the goal of that institution is to help political leaders and the public to see things clearly and, potentially, to find compromises or to assess risks for the public. It's impossible for everyone in Canada's population to provide an opinion. We have to have one entity representing the public and responsible for monitoring and protecting privacy—

Mr. Charbonneau noted that for political leaders to be trusted, they must behave in a trustworthy manner. He therefore questioned how a government can be completely trusted when it ignores the main body that Parliament has created to protect the privacy of Canadians, noting that: "One must not justify one's behaviour retroactively. One must be transparent from the outset."

Mr. Charbonneau was of the view that the government normalized the use of mobility data, which undermines public trust in political institutions. In his view, each time something happens that runs counter to the way leaders should behave, public trust goes down or it stagnates. He added: "[T]rust is one of the pillars of a real democracy. A social contract connects the public with the political leaders, the elected representatives. That trust is fundamental. The more it's undermined, the more people feel entitled to do what they want."

Dr. Geist noted that compliance with the law doesn't always foster trust. Mr. Therrien noted that incidents around privacy erode public trust. Dr. Cavoukian said it is essential for government to build public trust because it is fleeting right now.

Dr. Weinstock also reminded the Committee with respect to public information about the use of mobility data that:

> Two years of pandemic is a long time, and I think things that were said two years ago are worth repeating regularly… I don't think this matter can simply be removed from public debate once and for all, at the beginning of the pandemic, to never come back to it.

Committee Observations and Recommendations

The Committee recognizes that public information on mobility data is available on the *COVIDTrends* webpage. However, the Committee notes that many witnesses said that the government could have been more transparent. The Committee therefore recommends:

Recommendation 3

That the Government of Canada include explicit transparency obligations in the *Privacy Act*.

Recommendation 4

That the Government of Canada immediately update the *COVIDTrends* webpage to indicate where the data originates from, what data provider(s) are providing the government with information, and details on where Canadians can opt out of the data collection and surveillance program.

Recommendation 5

That the Government of Canada undertake measures that will inform Canadians of mobility data collection programs on an ongoing basis and that it does so in a manner that clearly outlines the nature and purpose of the data collection.

Consent

In response to questions about consent, Mr. Allison said that Telus and BlueDot collect data as part of their business and that they provide options for consent. He stated:

> [T]he question of meaningful consent isn't really one I can answer. Telus is transparent about what it is doing. The Government of Canada is being transparent about what it's doing and how it is using mobility data, but at the end of the day, it is up to users of the service to make the decision whether or not they would withdraw their consent from Telus.

Mr. Allison agreed that the average mobile phone user may not have known that he could opt out of the Data for good program, unless he was informed of it or had gone on the Telus website.

Mrs. Snively confirmed that Telus offers its customers the ability to opt out of the Data for Good program.

Mrs. Snively explained that the data used by the Data for Good program is based off of data collected in the course of providing mobility services, so that consent is applied to its use for mobility services and to provide those services. Once the data is de-identified, it is no longer personal information. Rather than relying on consent, Telus ensured that the data was de-identified. Dr. El Emam also noted that anonymizing or de-identifying data means that it is no longer personal information.

With respect to Telus customers' consent to having their information de-identified, Mrs. Snively noted that a lot of information about de-identification is in the company's privacy policy and on its website. Mr. Therrien indicated, however, that privacy policies that mention that mobility data may be used for the public good are not a good way of informing Canadians about how their data is used, as these policies are often long, complicated and difficult to understand. Nevertheless, Mr. Therrien acknowledged that, if information is properly de-identified, consent is not required.

Mrs. Snively noted that actively reaching out to customers to inform them of the Data for Good program is not a simple decision. For example, Telus tells customers not to respond to a text message that they are not expecting because it could be phishing, and a lot of customers don't want to be texted.

With respect to BlueDot, Dr. Khan said that users of applications that provide data to his company give their express consent to allow the application to access their location data and can withdraw their consent at any time.[26] Mr. Demarsh added:

> In this context, because the data are only de-identified location information, there's no degree of consent for additional information. We never receive anything beyond the de-identified location or aggregated summary metrics related to movement. For this

26 ETHI, *Evidence*, Kamran Khan (BlueDot).

purpose, there's no notion of degree of consent or additional information that we could obtain per device or in aggregate.

Christopher Parsons said that the activities of Telus and BlueDot "speak to the government's seeming willingness to receive mobility data without first confirming that individuals have meaningfully consented to such disclosures." He suggested that cellphone users expect that their mobility data will be used to maintain or operate networks, but not necessarily shared with third parties for other purposes, even if it is part of an aggregated, anonymized dataset, and technically permitted in privacy policies.

Ann Cavoukian was also of the view that there was no consent for the use of mobility data in this case. However, Dr. Weinstock noted that the goal in this case could only be met if a vast majority of the population were enrolled, making individual, express consent difficult.

Data Sharing

Mr. Allison said that PHAC has data sharing agreements with provinces, territories, and research institutions. Regarding mobility data, he said that the data received from vendors is not shared, but that reports and summaries of those reports are shared with provinces, territories, and other organizations for the purpose for which the information was gathered: to combat COVID-19. Dr. Tam and Ms. Thompson said the same thing.[27]

Mrs. Snively confirmed that Telus was aware that PHAC would be sharing the data obtained under its Data for Good program more broadly. If the data served the social purpose behind the program (containing COVID-19), sharing was permissible.

Dr. Khan said that his work with PHAC was for the agency to be able to support local, national, and provincial decisions, but that he was not entirely aware of how PHAC may have shared the data it accessed through its contract with BlueDot with other jurisdictions across the country.

With respect to the future use of mobility data by the government, Dr. Geist stated:

27 The Committee received an example of a report from Innovation, Science and Economic Development Canada's Communication Research Centre entitled "COVID-19 weekly mobility trends in Canada for the week of May 02 – May 08, 2021" that was sent to the provinces. The report provides statistics on mobility during the given week using charts and heat maps. The report indicates that the mobility metrics are derived using the location of cell towers rather than the geographic location of the mobile devices. A movement is inferred when a mobile device switches from one cell tower area to another.

> I'd start by saying that keeping that door open is something that we see both companies and perhaps governments trying to do in terms of potential multi-use of data down the road. That's partially where these problems really start to arise. I think that you can make a credible case in some circumstances, but trying to leave full flexibility down the road starts to really tear at the public trust that we've just been hearing about.
>
> If you have effective legal rules in place, then that simply isn't an option, because what you have to do when you have powerful legal rules in place is justify the use, and you try to circumscribe some of those uses so that they're more clear-cut and the consent itself is only valid for those narrow groups of uses, as opposed to essentially opening the door to alternative uses down the road as issues potentially arise.

Committee Observations and Recommendations

The Committee believes that Canadians should be guaranteed that the sharing of their data, even when it is de-identified or aggregated, is limited. Therefore, the Committee recommends:

Recommendation 6

That the Government of Canada ensure that use of the information collected through mobility data collection programs is limited to the requesting department or agency and any other department or agency specifically mentioned in the tender only if rationale is provided for the inclusion of multiple departments or agencies.

CHAPTER 2: DE-IDENTIFIED, ANONYMIZED, AND AGGREGATED DATA AND RISK OF RE-IDENTIFICATION

Mr. Therrien noted that de-identified datasets must protect against different types of re-identification risk. He said that the OPC's framework cautioned against the risk of re-identification and that technical means need to be implemented to protect de-identified information. He also said that consideration should be given to the nature, scope, context, and purposes of the processing in each instance de-identified data is released.[28]

Dr. Lyon noted the following with respect to the risks of re-identification:

28 OPC Letter of 14 March 2022. The Commissioner named three types of risk: "individualization (i.e., it must be impossible to isolate an individual from a dataset), correlation (i.e., it must be impossible to link two sets of data concerning the same individual), and inference (i.e., it must be impossible to infer new information about a data subject from a set of data)."

> I'm not an expert on de-indentified data, but high-level studies from various places, one from Imperial College London and the university in Leuven, show that 99.8% of Americans could be reidentified in a dataset that used 15 demographic attributes. There is potential for reidentification, and therefore reassurances are required that the data are really secure and are used only for appropriate purposes.

However, Dr. Lyon said although perfect anonymity is hard to obtain in practice there are ways of to be cautious at all stages, that is, during the data collection, the aggregation of data, and the analysis of data.

Dr. El Emam said terms like anonymization, de-identification, and aggregation are used interchangeably, but they don't mean the same thing. It is more precise to talk about the risk of re-identification, as the objective is to ensure that this is very small.

Dr. El Emam added that accepting a very small risk of re-identification is not controversial as those who transform data rely on precedents that have worked quite well in practice. If the standard is zero risk, then all data would be considered personal information. In his view, this would have many negative consequences for health research, public health, drug development, and the data economy in general in Canada.

Dr. El Emam explained that there are many kinds of transformations to reduce the risk of re-identification and that there is a toolbox of privacy-enhancing technologies for the sharing of individual-level data responsibly. For example, dates can be generalized (by using larger time intervals), geographical locations can be reduced in granularity (by using larger geographic areas), noise can be added to data values or synthetic data can be created (fake data that retains the patterns and statistical properties of the real data but for which there is no one-to-one mapping back to the original data). It is also possible to encrypt data and do the analysis on the encrypted data or even share summary statistics instead of individual-level data.

However, Dr. Khan said that synthetic data are useful in a very stable environment, which is not the case during a pandemic with constantly changing conditions.

Dr. El Emam added that the risk of re-identification is managed by a combination of data transformations and additional controls. He agreed that the risk is not going to be zero. Residual risks are managed by putting in place security controls, privacy controls, and contractual controls. He named best practices for responsible re-use and sharing of data: transparency (informing individuals about the purposes for which their data is used and can involve an opt-out), ethics oversight (having an independent review of the data-processing purposes) and re-identification attacks to test the risk of re-identification empirically.

Dr. El Emam stressed that, if the data is de-identified using good practices, then the re-identification risks can be very small.

CHAPTER 3: USE OF DATA FOR LEGITIMATE COMMERCIAL PURPOSES AND SOCIALLY BENEFICIAL PURPOSES AND THE ROLE OF CONSENT

Mr. Therrien said that, early in the pandemic, the OPC recognized that data can serve the public interest, such as protecting public health. As indicated above, he stated: "it is to the benefit of Canada that data is shared, obviously for good reasons—for legitimate commercial interests, for the public good, and not for illegitimate surveillance."

As to consent, Mr. Therrien recognized that organizations in both the public and private sectors constantly reuse data to new ends, which raises legitimate concerns by consumers, particularly when their personal information is used without their knowledge for purposes other than those they expected. However, he said that this does not mean that these practices should only be allowed with consumers' consent. In his view, as the PHAC case illustrated, this is neither realistic nor reasonable.

According to Mr. Therrien:

> In today's digital era, privacy protection cannot hinge on consent alone and in many cases securing individual consent is neither reasonable nor realistic. In fact, consent can be used to legitimize uses that, objectively, are completely unreasonable and contrary to our rights and values. And refusal to provide consent can sometimes be a disservice to the public interest.[29]

M. Therrien said:

> I believe that due to the limitations of the consent model in protecting privacy, a more appropriate policy would be to authorize the use of personal information for legitimate commercial interests and the public good within a rights-based law. That law should be enforced by the OPC, an independent regulator, to which would be conferred the requisite powers and resources to protect Canadians.

Dr. El Emam shared similar views. He believes it can be impractical to obtain consent a priori in cases like that of PHAC. That is why de-identification methods and the

29 Ibid.

additional controls, transparency, and ethics reviews all provide assurance that the data is no longer identifiable and it is being used responsibly.[30]

Dr. Theresa Scassa, Canadian Research Chair in Information Law and Policy and Professor of Law at the University of Ottawa, indicated that even though there is a need to facilitate the use of data for socially beneficial purposes, one can still question the validity of the consent, the quality of the collection practices, and the kinds of data that are collected. According to Dr. Scassa, privacy issues are very important, but the ability of governments to use the best available data to make important public policy decisions is also important but it is often impossible for the government to collect the data itself.

Like Mr. Therrien, Dr. Scassa conceded that there is such a huge volume of data being collected that it becomes impossible to rely on individual consent for all uses. That is why mechanisms have to be in place to supplement consent in some circumstances. The problem, according to Dr. Scassa, is that companies and governments are trying to do their best to address how to use data appropriately for socially beneficial purposes when there aren't frameworks for this type of activity in place.

Dr. Scassa noted that former Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (Bill C-11 (43-2)), "specifically defined de-identified personal information." That Bill sought to amend the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Consumer Privacy Protection Act (CPPA) provided exemptions allowing organizations to de-identify an individual's personal information in their possession and to use or disclose it in some circumstances, without their knowledge or consent.[31]

Dr. Scassa explained that section 39 of the CPPA would also have allowed the sharing of de-identified data with government actors for socially beneficial purposes, without the knowledge or consent of the individuals whose personal information is de-identified. She believes this provision would have applied to the situation with PHAC.

However, Dr. Scassa expressed concerns about the wording of section 39 of the CPPA. She said some questions need to be considered about the provision's scope, for example

30 ETHI, *Evidence*, Khaled El Emam.

31 See sections 20, 21, 22, 39, 74, and 75 of the Consumer Privacy Protection Act (CPPA) in Bill C-11 (43-2). The CPPA contains a definition of the term "de-identify" in section 2. Certain sections then refer to the de-identification of personal information of the fact that personal information is de-identified; For more information on Bill C-11 (43-2), see the *Legislative Summary of Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts* prepared by the Library of Parliament.

how "socially beneficial purposes" should be defined, the degree of transparency that should be required on the part of organizations that share de-identified information, how private sector organizations' sharing of information with the government for socially beneficial purposes would dovetail with any new obligations for the public sector, and the possibility of prior review or approval of plans to acquire and/or use the data.

Committee Observations and Recommendations

The Committee believes that, if companies can use information for legitimate commercial interests or socially beneficial purposes without consent, Canadians should be able to know exactly what those purposes are. The Committee therefore recommends:

Recommendation 7

That the Government of Canada amend the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to define what constitutes a 'legitimate commercial interest' and 'public good' in the collection, storage, use, transfer, and sale of private data, such as mobility data, and that the Office of the Privacy Commissioner of Canada be given the power to investigate breaches of the ethical guidelines defining those criteria.

CHAPTER 4: LEGISLATION ADAPTED TO THE DIGITAL AGE

Dr. Geist noted that the way data was aggregated and de-identified in the PHAC case was a textbook approach to how many organizations have addressed their privacy obligations—by de-identifying data and placing it outside the scope of the law. The potential use of the data in the midst of a global pandemic may well be beneficial. It does not appear that there was a violation of the law because the data was aggregated and de-identified. He believes the foundational problem that the PHAC case highlights is that our laws are no longer fit for purpose and are in dire need of reform. The Committee agrees with Mr. Geist: the laws need to be modernized.

Need for Reform

The *Privacy Act* was passed in 1983 and has not been substantially reformed since. The PIPEDA was passed in 2000. It has also not been substantially reformed since.

In 2016, the Committee conducted a review of the *Privacy Act*.[32] In 2018, the Committee conducted a review of PIPEDA.[33] The Committee has also published other reports containing numerous recommendations to improve PIPEDA.[34]

In November 2020, the government introduced the former Bill C-11 (43-2), which sought to amend PIPEDA. It died on the *Order Paper*. In 2021, the Government of Canada released a discussion paper as part of a public consultation on modernizing the *Privacy Act*.[35] No legislation has been introduced to amend the *Privacy Act* yet.

Application of Laws to De-identified Data

Mr. Therrien explained the following with respect to implied consent and de-identified data:

> In the event of implied consent, the legal principle is that properly de-identified data, being something that is entirely possible to do, is simply not personal information under current public sector law. So the government can collect and use it as it sees fit, without having to protect privacy. This is entirely possible, even though we haven't yet reached a conclusion. Therefore, the rule that seems to apply in this case is that, if properly de-identified, data is not personal information and consent is not required.

Mr. Therrien questioned "whether it is good legislative policy that de-identified information falls outside the reach of privacy laws" considering that "removing de-identified information from the reach of these laws would bring very significant risks and is not good policy." He reiterated:

> What needs to be understood is that, even when data is properly de-identified, there is always a risk of re-identification through data matching, through all kinds of possibilities. That is why, given the risk of re-identification in every case, we are suggesting that it is not good policy under the current law to treat de-identified information outside the scope of the *Privacy Act*.

Dr. Scassa said that both PIPEDA and the *Privacy Act* must be modernized so they can provide appropriate rules and principles to govern the use of data in a transformed and

---

32 ETHI, *Protecting the Privacy of Canadians: Review of the Privacy Act*, December 2016.

33 ETHI, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*, February 2018.

34 ETHI, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process*, June 2018; ETHI, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, December 2018; ETHI, *Privacy of Digital Government Services*, June 2019.

35 Department of Justice, *Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act* (Department of Justice consultation paper on the *Privacy Act*).

transforming digital environment. She believes that the fact that these two laws apply only to data about identifiable individuals creates a grey zone for de-identified data. She thinks the Privacy Commissioner must have some capacity to oversee the use of de-identified data, or at the very least to ensure that re-identification does not take place.[36]

Dr. El Emam noted the lack of clear, pan-Canadian regulatory guidance or codes of practice for creating non-identifiable information. He believes such codes, and more clarity in law, would reduce uncertainty, provide clear direction for what reasonable, acceptable approaches are, and enable organizations to be assessed to demonstrate compliance. He believes codes of practice, de-identification standards, and enforceable guidelines would ensure good practices are adopted each time.[37]

Dr. Scassa said if legislation is going to extented to de-identified data, then the legislation should extend to addressing or identifying what de-identification standards should apply. Dr. Cavoukian also agreed that federal privacy laws should apply to de-identified data.

Mr. Therrien stated that he supports proposals put forward by the government in Bill C-11 (43-2) and the Department of Justice consultation paper on *Privacy Act* modernization. Both proposed to "include a definition of de-identification in the law, add flexibility to the law to allow its use and disclosure in certain circumstances, and introduce an offence for re-identifying de-identified information."[38]

Mr. Therrien noted that Quebec updated its personal information protection laws to included definitions for the terms "de-identified" and "anonymized" and put in place penalties for identifying or attempting to identify a natural person using de-identified or anonymized information. Quebec allows the use of de-identified information without obtaining consent, as long as the use is necessary for study or research purposes, or for the production of statistics.[39]

---

36 David Young sent the Committee a compliance bulletin he wrote in May 2021. Mr. Young suggests that Bill C-11 (43-2) needs a comprehensive model for non-personal information. He suggests that the bill should make provision for a limited category of non-personal information that would also be subject to the new private sector privacy law, given that it is derived from personal information, i.e., de-identified data.

37 Bill C-11 (43-2) provided for the possibility of codes of practice, approved by the Privacy Commissioner (sections 76 to 81 of the Consumer Protection Privacy Act). Mr. El Emam gave the example of the work of the *Canadian Anonymization Network* (of which Telus is a founding member) and the standards published by the Office of the Information and Privacy Commissioner of Ontario in 2016: De-Identification Guidelines for Structured Data.

38 OPC Letter of 14 March 2022.

39 Ibid.

Mr. Therrien also mentioned that Ontario amended its 2004 *Personal Health Information Protection Act* to generally prohibit any person from using or attempting to use de-identified information, either alone or with other information, to identify an individual, with certain exceptions.[40] Dr. Scassa noted that Ontario amended its *Freedom of Information and Protection of Privacy Act*, which applies to the public sector, to define de-identified information for the purposes of use by government, to require the development of standards for de-identified data, and to provide specific penalties for re-identification.[41]

At the international level, Mr. Therrien noted that the GDPR clearly distinguishes between "pseudonymized" data and "anonymized" data; the regulation continues to apply to the former and no longer applies to the latter. Japan's protection of personal information act sets out specific rules for "pseudonymously processed information" and "anonymously processed information." In Australia, specific rules about de-identified information and a definition similar to that in the Quebec and Ontario legislation are found in the 1988 *Privacy Act*. South Korea's legislation contains greater latitude for the processing of pseudonymous information, which can be processed without consent for statistical, scientific research, and archiving purposes in the public interest. It also contains penalties for re-identification.[42]

In a brief submitted to the Committee, Bell Canada said that the appropriate use of de-identified data can serve the public interest in protecting public health. It stated that data analytics offers an enormous opportunity to derive economic and social value from data and many existing de-identification techniques prevent re-identification. Consequently, Bell believes that de-identified data should not fall within the scope of privacy laws.[43]

---

40 Ibid.

41 See also the comments of the Privacy Commissioner regarding the Ontario law: OPC Letter of 14 March 2022.

42 Ibid.

43 Bell Canada declined an invitation to appear before the Committee. SaskTel declined an invitation to appear before the Committee. In a letter to the Committee dated 10 February 2022, SaskTel said that it was not in a position to answer questions regarding Telus' and BlueDot's practices and had no intention of participating in the PHAC tender. Rogers Communications declined an invitation to appear before the Committee. In a letter to the Committee dated 4 February 2022, Rogers said that it had not provided any information to PHAC, that it would not be a participant in the PHAC tender, and that it does not disclose customer information, de-identified or otherwise, unless ordered to do so by a court or other lawful authority.

Committee Observations and Recommendations

The Committee believes that, because the risk of re-identification is never zero, federal privacy laws should apply to de-identified data. It recommends:

Recommendation 8

That the Government of Canada amend federal privacy legislation to render these laws applicable to the collection, use, and disclosure of de-identified and aggregated data.

Recommendation 9

That the Government of Canada include in federal privacy legislation a standard for de-identification of data or the ability for the Privacy Commissioner to certify a code of practice in this regard.

Data Flows Between the Private and Public Sectors

Mr. Therrien said there is increasing interaction between the public and private sectors in terms of data management – which is not a bad thing – but it needs to be properly regulated according to known criteria and be the subject of investigation when the case arises.

Dr. Scassa said the PHAC situation illustrates how easily data flows from the private sector to the public sector in Canada. The current legal framework governs public and private sector uses of personal data separately. In her opinion, our laws need to be better adapted to address the flow of data across sectors. She thinks that flows between public and private haven't really been well considered in legislation.

However, Dr. Scassa attempted to reassure the Committee by noting that the Commissioner has already said that a government institution cannot use data that was collected illegitimately for a legitimate use, giving the Clearview AI case as an example.[44]

Dr. Geist said there is need to think about the interaction that the federal government may have with private sector participants in accessing data. Legislation needs to establish effective precautions and safeguards in that regard.

44 Office of the Privacy Commissioner of Canada, *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology*, 10 June 2021.

The International Gold Standard

Many witnesses acknowledged that the GDPR is a model for data protection.[45] For example, Mrs. Snively mentioned that the GDPR embraces the principle of privacy by design. However, Dr. Scassa cautioned against simply copying what has been done in Europe and transplanting it to the Canadian context.

Dr. Geist said:

> We also have, as I mentioned off the top, the European GDPR, which is effectively the model that many are comfortable with and are already seeking to comply with. It seeks to address some of these kinds of issues in terms of algorithmic transparency, in terms of greater penalties, and in terms of identifying some of the newer sorts of issues such as the right to be forgotten, and others, which form a part of what I think is widely viewed as a modernized privacy law, something that Canada no longer has.

However, Dr. Geist noted that was not to suggest that Canadian-specific rules couldn't be made.

Modernizing Laws

Amending the *Privacy Act*

As previously indicated, Mr. Therrien stated that "in the new law our office should have greater powers to proactively audit the practices of governments and the private sector", while noting that "unfortunately it is just not realistic to expect that we will pre-approve every use or disclosure of data in this country."

Mr. Therrien clarified that proactive verifications are not meant to be a thorn in the side of governments or companies that want to innovate responsibly. However, given the complexity of data flows and business models. He is of the opinion that the OPC is better placed to go under the hood in a number of places where it thinks there might be risks, so that it can either reassure Canadians that the law has been respected or intervene and sanction companies that have not complied with the law.

Mr. Therrien said that the principle of transparency should definitely be included in the *Privacy Act*. He said the GDPR contains explicit and extensive transparency-related requirements that apply not only at the time of collection but also when there is a

45 See, for example: ETHI, *Evidence*, 7 February 2022, Khaled El Emam; ETHI, *Evidence*, 10 February 2022, Ann Cavoukian and Theresa Scassa; ETHI, *Evidence*, 14 February 2022, David Murakami Wood; ETHI, *Evidence*, 28 February 2022, Michael Geist.

material change in the purpose of processing. The GDPR requires that "any information and communication relating to the processing of […] personal data be easily accessible and easy to understand, and that clear plain language be used."[46]

Dr. Parsons proposed a series of *Privacy Act* reforms. First, organizations that provide information to government should be mandated to prove that they have obtained meaningful consent from individuals to whom the information relates before it is disclosed. Second, he proposed that the *Privacy Act* be extended to aggregated or anonymous information and that the government include equity assessments as part of any privacy analysis of how government agencies might use aggregated or anonymous information that they obtain. Third, he proposed that the government must receive approval from the Privacy Commissioner before launching a program associated with such information.[47]

Dr. Parsons recommended including necessity and proportionality requirements, which would compel federal institutions to demonstrate that identifiable or anonymized information is required to fulfill a specific activity and ensure that the sensitivity of the data is proportional to the activity in question. He also believes the *Privacy Act* should prohibit the use of data for purposes other than those for which it was collected or received, without again obtaining the individual's meaningful consent.[48] Dr. Geist also suggested that a necessity criterion be included in the *Privacy Act*.

Dr. Parsons also recommended including retention limits on aggregated or anonymized data (commensurate with their level of de-identification and the sensitivity of the underlying data) and a prohibition on data re-identification.[49]

Dr. Parsons recommended that the *Privacy Act* empower the Commissioner to assess the proportionality of any anonymized dataset programs. He also recommended establishing a centralized location whereby Canadians can see whether their personal information has been collected or received by federal institutions.[50]

Dr. Geist recommended that the *Privacy Act* include a mandate for public education and research, as is the case under PIPEDA. He also recommend including security measures

46 OPC Letter of 14 March 2022.

47 Brief submitted by Dr. Christopher Parsons.

48 Ibid. Dr. Parsons says in his brief that section 4 of the *Privacy Act* currently justifies almost any data handling by the federal government as long as it is related to a government agency's program or activity.

49 Ibid.

50 Ibid.

for data breaches, like the one under PIPEDA, and requiring in the legislation that privacy impact assessments be conducted when new programs are launched. With respect to retaining data such as that accessed by PHAC, Dr. Geist noted that all modern laws provide a limit, namely that data is retained only as long as necessary.

Amending the *Personal Information Protection and Electronic Documents Act*

Mr. Therrien explained the following with respect to what should be found in privacy legislation:

> I don't think the ultimate solution is simply greater transparency and explicit consent, given that data is used in an extremely wide range of ways, sometimes for good reasons, sometimes for bad.
>
> Therefore, you need objective criteria, covering things like legitimate commercial use and using data to serve the public good, that a regulatory agency would enforce. Consent is important, but a regulatory agency also needs to play a role in properly protecting Canadians, given the complexity of how their data is being used.

According to Mr. Therrien, the framework needs to allow for flexibility and innovation in the use of data for legitimate commercial interests and the public good. However, it must protect privacy as a human right and be enforced by a regulator who can audit or investigate to ensure that, in these circumstances, the data indeed was used correctly and, when not, there should be consequential penalties for players and corporations that have violated the law.

Dr. Parsons indicated that the *Guidelines for Obtaining Meaningful Consent* should be built into PIPEDA. He suggested that:

> [T]he Government of Canada, whenever it is receiving either identifiable or aggregated and anonymized information derived from individuals from private organizations, should be required to demonstrate that such information was collected by those organizations after the individuals meaningfully consented to the collection and disclosure.

Dr. Parsons recommended mandating organizations to specify whether they or their partners collect information as opposed to simply raising the possibility that they might. He also recommends mandating organizations to specify the other organizations with

whom information is disclosed and their intended uses. Lastly, he recommends PIPEDA include a requirement to develop transparency reports.[51]

Mrs. Snively said there are some great aspects of the GDPR, including embracing privacy by design. She said there are also some great aspects of the current PIPEDA, for example that it is principle-based and allowed Telus to be nimble and agile in the way it assessed privacy.

In response to a question relating to the creation of a privacy protection tribunal, Dr. Geist said that a tribunal was proposed in Bill C-11 (43-2). However, he said there was some opposition to the tribunal, including from the Privacy Commissioner. He said he did not have a problem with it, as long as it was an expert tribunal, which was not the case in the former bill. In terms of enforcement, Dr. Geist said that the law must have strong penalties and give the Commissioner order-making power.

Committee Observations and Recommendations

The Committee believes that federal privacy laws must be improved as quickly as possible to adapt to the current reality where the data of millions of users is collected, used, and disclosed every day for a variety of purposes, some of which are commendable, as in this case, some of which are more problematic.

The Committee therefore makes the following recommendations:

Recommendation 10

That the Government of Canada include in federal privacy legislation a prohibition on re-identification of de-identified data and a corresponding penalty.

Recommendation 11

That the Privacy Commissioner of Canada be given the authority to proactively audit the practices of all third-party mobile data providers to ensure compliance with the *Personal Information Protection and Electronic Documents Act* when the data collected is used by any federal institution.

51 Ibid.

Recommendation 12

That the Government of Canada amend the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to regulate the activities of private companies in the collection, use, sharing, storage, and destruction of Canadian mobility data and that the government ensure private companies have obtained meaningful consent from their customers for the collection of such data.

Recommendation 13

That the Government of Canada strengthen the powers of the Office of the Privacy Commissioner of Canada to oversee the privacy rights of Canadians, with the power to investigate and enforce a strengthened *Privacy Act* and *Personal Information Protection and Electronic Documents Act*, including order-making powers and the ability to impose penalties.

Recommendation 14

That the Government of Canada amend the *Personal Information Protection and Electronic Documents Act* to require service providers that collect data to display a message offering the user the option to opt-out of the data collection, to continue using the service without accepting the terms and conditions, or to decline all terms and conditions and cookies.

Recommendation 15

That the Government of Canada require companies that generate, manage, sell or use data to comply with a framework additional to self-regulation.

Recommendation 16

That the Government of Canada be required to conduct its own audits of the source of the data as well as the meaningful consent, collection, transmission, and use of data.

Recommendation 17

That the Government of Canada include a public education and research mandate in the *Privacy Act* similar to the one found in the *Personal Information Protection and Electronic Documents Act*.

Recommendation 18

That the Government of Canada amend the *Privacy Act* to include necessity and proportionality criteria for the use, collection, and disclosure of personal information.

Recommendation 19

That the Government of Canada include the privacy by design standard in federal privacy legislation.

CHAPTER 5: BIG DATA, MASS SURVEILLANCE, AND POTENTIAL SOCIAL IMPACTS

Big Data and User Understanding

Mr. Therrien said that, generally, people do not have an awareness of the many ways in which their data is used. He hoped that Telus users know their data is being collected by Telus and maybe a few companies around Telus – but they would not know generally that their data is being used for the Data for Good program. The premise of Canadians is that their data is used for the purposes for which they provided it to the company or the department in question, and maybe other related ones, but not for any and all purposes that we see nowadays.

Dr. Parsons said that few users realized that, by consenting to provide mobility data to an app developer, they are also permitting this information to be sold or made available to other companies. In this context, the user consents to the first use, but not the second. While individuals can read privacy policies, these documents are known to be incredibly challenging to assess and understand. For example, the Information and Privacy Commissioner of Alberta concluded in an investigation involving Telus and Babylon Health that Babylon Health's privacy policy was insufficient for informed consent.[52]

Dr. French made similar comments about the complexity of terms of service and privacy policies. He said:

> I think this is a general cultural practice that we have of clicking "I agree"… It's just our culture today. We don't tend to read the terms of service and privacy policies, so we're

52 Brief submitted by Dr. Christopher Parsons; Office of the Information and Privacy Commissioner of Alberta, *Investigation Report P2021-IR-02: Investigation into Babylon by Telus Health's compliance with Alberta's Personal Information Protection Act*, p. 67.

> not often aware. How could we be? They're often not written very clearly. They're not written to be read easily or understood.
>
> This is, I think, a big problem. Many organizations say they're using personal health information, mobility data and other kinds of information. Even after they aggregate it, for example, de-identify it, there's still this kind of issue of consent maybe looming in the background more generally.

Dr. Scassa said that the use of mobility data and the reaction to it highlights some of the particular challenges of our digital and data society. It confirms that people are concerned about how their data is used and shows that they struggle to keep abreast of the volume of collection, the multiple actors engaged in collection and processing, and the ways in which their data is shared with and used by others.

Dr. Scassa noted that data is often collected and curated for purposes that go well beyond maintaining consumer or customer relationships. Data is the fuel of analytics, profiling, and artificial intelligence. Some of these uses are desirable and socially beneficial while others are harmful or deeply exploitative. The challenge is to facilitate the positive uses and to stop the negative ones.

Dr. Scassa added that we often have to agree to all sorts of privacy policies, which we don't have the time or even the skills to understand.

Dr. Murakami Wood said that today, informed consent is virtually meaningless. It is impossible to understand or read the policies created by corporations and government. Particular kinds of operations, such as location tracking, are often hidden in the policy. The consent is not meaningful, because it is often needed to supply a service: if you do not get consent, you do not get the service.

Dr. Lyon also agreed that in the current data collection environment it is becoming increasingly difficult to obtain consent for data collection and data analysis. He said there needs to be much broader public education so that we understand what we are doing when we supposedly give consent and when we actually give consent.

Dr. Deneault said the following with respect to the ability of people to clearly give consent to their data being used or taken:

> The answer is no, quite simply. Studies have been done on how difficult it is to really understand the contracts we are made to sign when we become users of these software programs that collect our data the moment we use them. We all know the saying: when we are given something such as software, it is because we are the product. It takes a legal background, and then some, to make an informed judgment about what we are signing up for when we use this software.

Dr. Deneault went so far as to say that the production of big data by tech giants constitutes a legal impoverishment from a government's perspective because these companies, which hold a technical monopoly, end up making law through membership contracts.

Dr. Deneault suggested the production of big data is, in itself, a totalitarian mechanism that involves monitoring the behavioural reality of subjects and making it predictable, even controllable. He advocates that we prevent its production at source. In his view, ethical concerns about the use of data exist because the mechanism is inherently totalitarian. While he recognized that there may be risks in not using massive data, he suggested the risk is to trivialize surveillance.

Dr. Deneault, invoking ethicist Hans Jonas, raised the following points about big data. The data-generating techniques being implemented today act on human subjectivity. If we allow such techniques to be deployed on a societal scale, without ever being able to measure and control their impact, that is, to check what they generate on a social and political scale, we are not being ethical. We must be as creative in terms of ethics as the technicians who create these devices are inventive.

Dr. French raised concerns about the public sector's increasing reliance upon the private sector to execute their duties and responsibilities to the public at large. He noted that the fragility of the public health system matched with the incredible data collection capacity of a number of private sector organizations makes it seem quite reasonable that we would turn to them for data.

Asked about data exploitation and surveillance capitalism, Dr. Khan conceded that there are concerning uses of data in some forms that can have negative social impacts, but that he doesn't believe that the work BlueDot is doing, which he says is noble and for the social good, falls into that domain. Mrs. Snively made similar remarks with respect to Telus's work.

Surveillance and Limits on Data Collection

Definition of Surveillance

Dr. Lyon said that surveillance is often associated with police activities, such as keeping a suspect under observation or keeping watch on those suspected of terrorism. However, the definition of surveillance is much broader and includes public health surveillance. He believes surveillance should be defined as the "focused, routine and systematic

attention to personal details for specific purposes, such as management, protection or influence."

Mr. DeMarsh explained that in public health surveillance is used as a catch-all term for infectious disease case data or other disease case data. It is a general term well understood within public health collection of data.

Potential Social Impacts

Dr. Murakami Wood shed light on the risk of collecting large datasets: they hide existing forms of bias and prejudice. He said it is very important to be able to understand not just the data as facts but the data in its social context. He shared a hypothetical scenario with the Committee to illustrate that point:

> Say, in Telus's "data for good"—this is just made up, by the way—it was found that people in a particular suburb of Toronto were travelling further distances more often than other people in Toronto. You could easily assume from this data that these people were spreading the virus or were disobeying government instructions on travel. In fact, if you look into this particular suburb, you find it's a low-income place, largely Black and of ethnic minority. You have in this area people who have to travel to get to warehousing jobs or work in the gig economy, and the reason they're mobile and moving more often is precisely because they're under-privileged. Therefore, to stigmatize these people or to blame them for the virus spread would be to misread the social facts on the ground.

Christopher Parsons also noted that even aggregated and anonymized data can have population-level effects when that information is used to guide policy making, for example how services and resources are allocated. For instance, some communities may be less represented in mobility data if not all members in a household have a mobile phone. It is insufficient just to consider an individual's privacy violation; community impacts must also be considered.[53]

Dr. French made similar comments. He is not against public health surveillance but is interested in whether people might be advantaged or disadvantaged by it. Because mobility data can be used to make recommendations or identify problems like people not obeying lockdown regulations or curfew, Dr. French said that, if intensification of enforcement follows, it could fall on communities that are dealing with other issues. In a brief submitted to the Committee, he further explains how certain groups may be

53 Brief submitted by Dr. Christopher Parsons.

exposed to increased risks or harms as a result of public health mobility tracking, focusing on equity questions.[54]

Dr. Lyon also recognized that public health surveillance is an important task, but said that this doesn't reduce the fact that there are risks entailed in it at every stage: collection, analysis, interpretation, and use. Each stage presents difficulties and can cause harms at the individual level as well as the group level. Dr. Lyon said that surveillance can cause different kinds of harms but can also bring social benefits.

Dr. Murakami Wood emphasized that surveillance or data collection in itself is not a form of human rights violation or anything else. It can be good when used as the basis of evidence-based policy making. He gave the example of arguments about the long-form census, where, despite concerns about privacy, most academics argued in favour of it because it provided important data for effective policy-making.

Limits on Surveillance

Dr. Cavoukian said that, during a crisis or emergency, 9/11 for example, emergency measures can be introduced to put privacy laws on hold. The problem to her is that, after the emergency ends, the emergency measures often continue. Transparency goes out the door and surveillance grows and continues to grow. The measures taking place during emergencies must be suspended when the emergency is over.

Dr. Cavoukian also raised the fact that technologies are introduced without considering their impact on others, giving the example of cameras that capture photos of neighbours. She believes measures are needed to reduce the collection of data and surveillance and maximize the privacy choices that people can make.

Dr. Cavoukian noted that today she no longer needs to explain why privacy is important because people are already concerned about it. She notes a decline in public trust in institutions and widespread fear about the possibility of privacy breaches. This is the result:

54 Dr. Martin French, *Brief to ETHI Committee: Study on the Collection and Use of Mobility Data by the Government of Canada*, 25 March 2022. Dr. French makes three recommendations for the Public Health Agency of Canada: it should amplify its public awareness and education work surrounding mobility tracking and disease surveillance initiatives; it should protect access by law enforcement to mobility tracking data or surveillance data, to avoid, among other things, disease criminalization; and it should develop robust forms of community engagement, for example through independent surveillance-focused Community Advisory Boards whose mandate would be to support input from diverse community members regarding mobility tracking and disease surveillance initiatives.

> The growth of surveillance that follows that is massive. A lot of times people say to me, "Oh, you just have to give up on privacy; it's just not possible anymore." No, we don't give up on privacy. Privacy forms the foundation of our freedom. If you want to live in a free and open society, we have to have privacy, so I fight for this, even though trust is waning. Let's build it up. Let's get our governments to be honest with what they're doing with our information and at least notify us. Having it under the hood, not letting people know about it, just grows distrust, unfortunately.

The Committee agrees. It is not time to give up on privacy.

Committee Observations and Recommendations

Chapter 5 highlights the many challenges that living in a highly digital society can create. It confirms that many people do not comprehend how often their personal data is collected, used, and shared, nor the impact the various forms of surveillance may have. The Committee therefore makes the following recommendations:

Recommendation 20

That the Government of Canada increase its investment in digital literacy initiatives, including initiatives aimed at informing Canadians of the risks associated with the collection and use of big data.

Recommendation 21

That the government of Canada increase its public awareness and education work surrounding mobility tracking and disease surveillance initiatives.

Recommendation 22

That the Government of Canada develop clear guidelines regarding the use of mobility data by federal institutions and that it consult with the Office of the Privacy Commissioner, stakeholders and community groups that may be disproportionately affected by such initiative in that process.

CONCLUSION

The PHAC case highlighted the challenges of the digital society we live in. Because of this reality, the Committee suggests that, when government seeks to harness the potential of big data, such as mobility data, it should do so as transparently as possible by redoubling its efforts to explain to Canadians what kind of data is being collected, why it

is needed, how it will be used, and how they can opt out of the collection if they want to.

The evidence clearly illustrated that Canada's current regulatory framework does not adequately address the use of data, particularly de-identified or aggregated data. The Committee notes, as it has in several previous reports, that federal privacy laws are in dire need of modernization. The Committee is confident that, if implemented, the recommendations in this report will strengthen the privacy of Canadians.

The Committee invites the Government of Canada to consult the recommendations in its previous reports in addition to those in this report.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Departmnent of Health	2022/02/03	4
Hon. Jean-Yves Duclos, P.C, M.P., Minister of Health		
Public Health Agency of Canada	2022/02/03	4
Christopher Allison, Acting Vice-President Corporate Data and Surveillance Branch		
Dr. Theresa Tam, Chief Public Health Officer		
Kathy Thompson, Executive Vice-President		
As an individual	2022/02/07	5
Khaled El Emam, Canada Research Chair in Medical Artificial Intelligence		
Office of the Privacy Commissioner of Canada	2022/02/07	5
Daniel Therrien, Privacy Commissioner of Canada		
Martyn Turcotte, Director Technology Analysis Directorate		
As an individual	2022/02/10	6
Ann Cavoukian, Executive Director Global Privacy and Security by Design		
Martin French, Associate Professor Department of Sociology and Anthropology, Concordia University		
Teresa Scassa, Canada Research Chair in Information Law and Policy Faculty of Law, Common Law Section, University of Ottawa		
Daniel Weinstock, Full Professor Department of Philosophy, McGill University		

Organizations and Individuals	Date	Meeting
As an individual	2022/02/14	7
Alain Deneault, Professor of Philosophy		
David Lyon, Professor Emeritus Queen's University		
David Murakami Wood, Director Surveillance Studies Centre and Associate Professor, Department of Sociology, Queen's University		
Christopher Parsons, Senior Research Associate Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto		
BlueDot	2022/02/17	8
Alex Demarsh, Director Data Science		
Dr. Kamran Khan, Chief Executive Officer and Founder Professor of Medicine and Public Health, University of Toronto		
Telus Communications Inc.	2022/02/17	8
Pamela Snively, Vice-President Chief Data and Trust Officer		
As an individual	2022/02/28	9
Jean-Pierre Charbonneau, Former Quebec Parliamentarian and Professional Speaker on Ethics		
Michael Geist, Professor of Law Canada Research Chair in Internet and e-Commerce Law		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Bell Canada

French, Martin

Parsons, Christopher

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 3 to 10, 13, 14 and 16) is tabled.

Respectfully submitted,

Pat Kelly
Chair

Dissenting Opinion of the Liberal Party of Canada

On January 13th, 2022, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee") unanimously adopted a motion to study the issue of Collection and Use of Mobility Data by the Government of Canada. The motion reads as follows:

> *That, in light of recent media reports, the committee immediately undertake a study, pursuant to Standing Order 108(3)(h)(vi) and (vii), of the Public Health Agency of Canada collecting, using or possessing Canadians' private cellphone data, without their knowledge or consent, and: a) invite the Chief Public Health Officer of Canada to appear for one hour, including a five-minute opening statement; (b) invite the Minister of Health to appear for one hour, including a five-minute opening statement; and (c) request that the members of the committee provide to the clerk, one day following the adoption of this motion, their preliminary witness lists for this study.*

The Liberal members on the Committee recognize the importance of the privacy of Canadians and the government's responsibility to protect that privacy. While Liberal members applaud the efforts of the Committee to tackle the issue at hand, we note that:

- The motion is based on misleading reports on the scope of the collection and use of mobility data by the Public Health Agency of Canada. Witnesses confirmed that while mobility data was collected, it was not for 33 million people, as was reported and echoed by members of the Committee. Liberal members on the Committee also note that the text of the motion is based on a false premise – that Canadians were not informed of this collection of de-identified and aggregated data when in fact, the government announced in March 2020 of this collection. The work conducted with the collection of mobility data has been made publicly available on the COVIDTrends website as a means to provide Canadians with local information on COVID-19 in their communities with explanations of how this data is used, and the privacy protections currently in place.

- The report, while it highlights important issues relating to privacy concerns and the government's responsibility to be open and transparent, includes sweeping recommendations that go beyond the scope of the study as proposed by the motion outlined above. The study embarked upon by the Committee was in fact a case-study of a specific contract engaging contractors to collect, de-identify, and aggregate mobility data for the purpose of better informing public health policy decisions during the COVID-19 pandemic. The Request for Tender included provisions that mandated the protection of privacy of Canadians. Witnesses confirmed that, to further protect privacy, the Public Health Agency of Canada also used a multi-barrier approach from the source of the data, along the data pipeline and prior to it being received. In fact, witnesses confirmed that while the risk of data being re-identified is never zero, in this contract, there were no breaches in the privacy of Canadians and strong standards for the protection of privacy were followed.

- The report identifies over 20 recommendations that go beyond the scope of this case study. Liberal members on the Committee note that many recommendations call on the government

to do what it already is doing. For example, the Committee heard from witnesses that the Government already engages in substantial and ongoing consultation with the Privacy Commissioner and privacy experts when navigating the collection of data. Another example is that the Privacy Commissioner already has the power to investigate complaints and possible breaches in privacy.

- Liberal members on the Committee also note that several recommendations in this report demand that privacy legislation be amended in various ways. We agree that privacy legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) needs to be modernized. However, we are of the view that this modernization must be based on a fulsome review of federal privacy legislation that clearly defines and captures the scope, use, and disclosure of de-identified and aggregated data; such review should include establishing a standard for the de-identification of data. Without a fulsome review, the possible result could be a patchwork of amendments that do not solve the challenges at hand.

- Liberal members on the Committee note that the Minister of Innovation, Science and Industry has committed to digital privacy reform as a top priority, including the reform of the Personal Information Protection and Electronic Documents Act (PIPEDA), and will take these considerations into account.

- We also note that the Minister of Justice and Attorney General of Canada is also committed to reform of the Privacy Act (PA) and will similarly take these considerations into account. In particular, he has been mandated to build on previous public consultations and technical engagements amongst experts and to continue substantive review of the PA including engagement with Indigenous partners to develop specific proposals for amendments.

- Liberal members on the Committee believe that, when it comes to the protection of privacy of Canadians, better is always possible and the government should continue to review policy and legislation and identify gaps in the ever-evolving digital space and its implications on the privacy of Canadians.

The Liberal members of the Committee thank the House of Commons analysts and clerk for their hard work on this important case-study as well as the witnesses who appeared before us and helped inform the substance of this report.