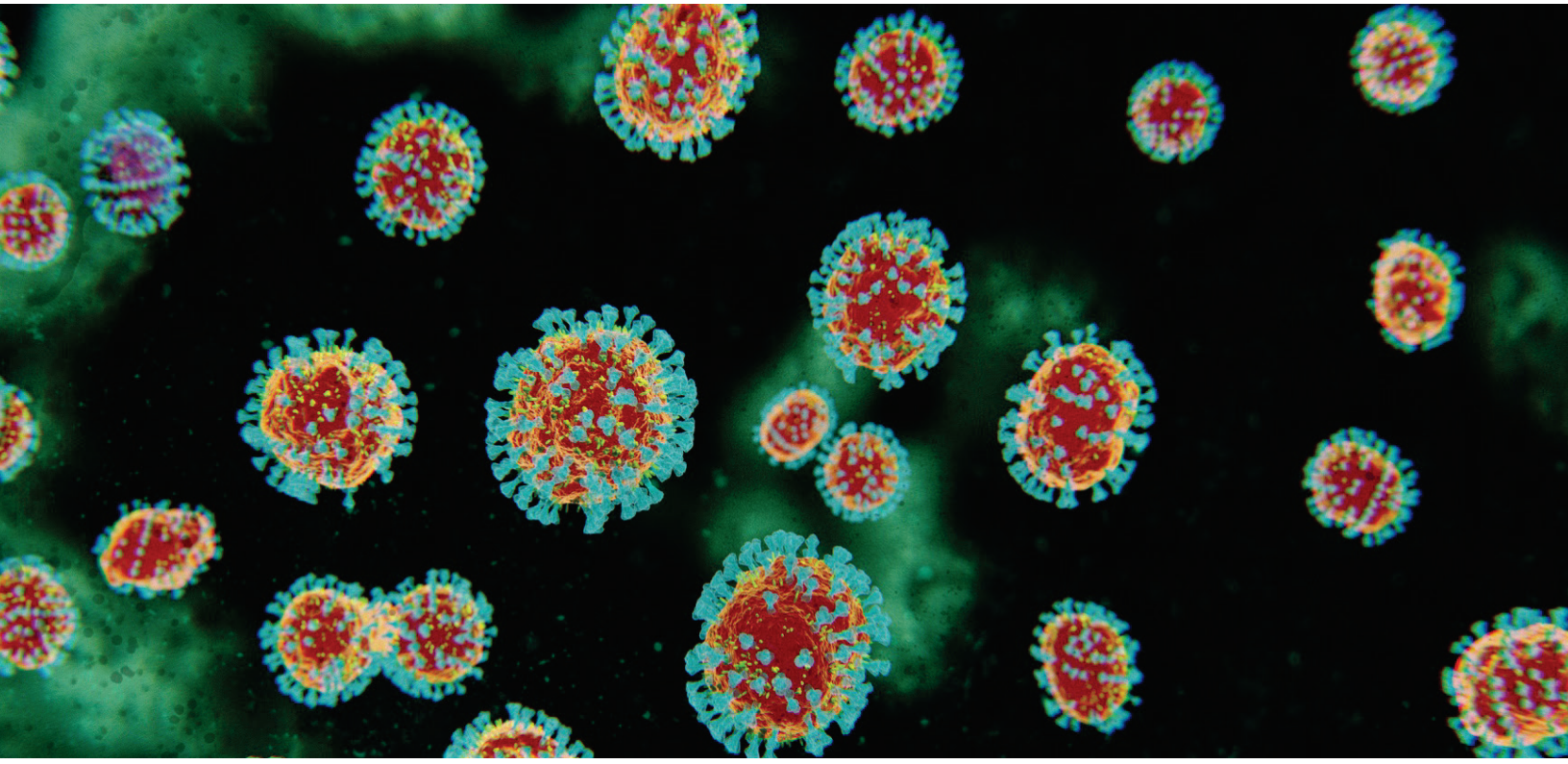
Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Protecting privacy in a pandemic



Special Report to Parliament

May 30, 2023

This document is available on the Web at www.priv.gc.ca. The html version of this report takes precedence over this document in case of a discrepancy.

Aussi disponible en français sous le titre : Protéger la vie privée pendant une pandémie

For more information, contact:

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Toll-free: 1-800-282-1376
Phone: 819-994-5444
TTY: 819-994-6591

IP54-113/2023E-PDF

978-0-660-47986-6

Table of contents

Commissioner's message

As Privacy Commissioner of Canada, I am pleased to table this Special Report to Parliament presenting the results of several investigations and advisory initiatives that examined the federal government's privacy practices in relation to measures adopted during the COVID-19 pandemic.

The pandemic was a rapidly evolving and unprecedented public health crisis that has had a profound effect on our world and our lives. It also raised important issues about the protection of personal information. Technology played a key role in helping the government and public health authorities to take swift action to predict, adapt and respond to an extraordinary public health crisis. The increased reliance on technology and the digitization of many aspects of our lives comes with undeniable benefits, but also has important privacy impacts that must be addressed.

Privacy matters to Canadians. In our most recent survey, 40% of respondents said that they were more concerned about privacy now than they were at the start of the pandemic. This is troubling. Canadians should feel confident that their privacy rights are being properly considered and protected, and organizations should make this a priority because when individuals are assured that their privacy is protected, it builds necessary trust in our institutions and the initiatives that they undertake.

Throughout the pandemic, my Office has continued to give key advice to public and private sector organizations to help ensure that privacy practices are appropriate, and that the measures implemented in response to the pandemic comply with privacy laws. We released a framework to assess privacy-impactful initiatives in response to the pandemic, and published guidance to help organizations understand their privacy-related obligations. We took the position that even during a public health crisis, privacy laws and other protections still apply and should not be seen as a barrier to the appropriate collection, use and sharing of personal information, but that a flexible and contextual approach to applying the law ought to be adopted.

We also called for public institutions to continue operating under lawful authority and to act responsibly, particularly with respect to the handling of information that may be considered sensitive, such as information about individuals' health. Public institutions should also ensure that privacy-impactful initiatives are time-limited; necessary and proportional to achieve a specific objective; that appropriate measures are taken to safeguard personal information; and that there are clear measures for transparency and accountability built in so that individuals can know and trust how their personal information is being collected, used, and disclosed.

My Office received approximately 100 formal complaints related to the COVID-19 crisis, and other privacy-related concerns were raised through media reports and before parliamentary committees. The results of our investigations, which we are making public by tabling this Special Report, found that the collection, use, disclosure and retention of personal information by federal institutions complied with the *Privacy Act*, with a few exceptions. We also identified areas for improvement where there are gaps or shortcomings, and some important lessons to be learned from the pandemic, the most significant being the need to modernize our privacy laws to make it a legal requirement for government institutions to demonstrate that their collection of individuals' personal information is necessary and proportional, and to provide a framework to address the use of de-identified information about individuals.

The COVID-19 pandemic has impacted almost every aspect of our lives over the last few years in ways that will continue to be felt for a long time. As we move forward, it is important to remember that privacy is fundamental to our individual dignity and our ability to enjoy other rights and freedoms. It is essential that the government protect our fundamental right to privacy – even during times of crisis or emergency – because doing so builds necessary trust in our institutions and supports the achievement of important public interest goals.

Philippe Dufresne
Privacy Commissioner of Canada

Introduction

In March 2020, the World Health Organization (WHO) declared a global pandemic. Efforts to contain the COVID-19 virus and to cope with its social and economic fallout prompted abrupt and colossal change worldwide. In response to the urgent public health crisis, the Government of Canada instituted public health measures, some of which involved the collection, use and disclosure of personal information, and which were intended to: (i) track virus transmission, (ii) enforce the *Quarantine Act* and other measures at Canada's borders, (iii) provide benefits and economic stimulus, and (iv) manage public servants' remote work practices and their eventual return to federal workspaces.

The mandate of the Office of the Privacy Commissioner of Canada (OPC) is to protect privacy rights and oversee compliance with Canada's public- and private-sector privacy laws. Throughout the COVID-19 pandemic, the OPC has played an important role protecting privacy rights by investigating complaints from individuals with respect to the personal information-handling practices of the federal public sector; consulting and providing advice to government and the private sector on a wide range of potentially privacy-intrusive proposals and initiatives related to health and safety; developing policy and collaborating with our domestic and international counterparts; and sharing information and best practices.

In the early days of the crisis, the OPC produced guidance on Privacy and the COVID-19 outbreak to address the questions being raised about privacy during a pandemic, and to provide a general overview of the applicable federal privacy laws. Soon thereafter, the OPC published a framework for assessing COVID-related initiatives as various government authorities began to describe more specifically the programs and initiatives that they intended to pursue in response to the pandemic.

"Privacy protection isn't just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental human rights and democratic values, even in exceptional circumstances," the OPC said in introducing its framework.

The framework set out the key privacy principles that government institutions should factor into any assessment of the measures proposed to combat COVID-19, including:

- Legal Authority: the proposed measures must have a clear legal basis.
- Necessity and Proportionality: the measures must be necessary and proportionate, and, therefore, be science-based and necessary to achieve a specific, identified purpose.
- Purpose Limitation: personal information must be used to protect public health and for no other purpose.
- De-Identification and Other Safeguarding Measures: use de-identified or aggregate data whenever possible.

- Vulnerable Populations: exceptional measures should be time-limited and the data collected during this period should be destroyed when the crisis ends given the likelihood that the information is sensitive and may disproportionately impact vulnerable populations.
- Transparency and Accountability: the government should provide clear and detailed information to Canadians about the basis for exceptional measures, as well as the applicable terms for such measures, and be accountable for them.

Privacy laws and other protections still apply during a public health crisis, but they are not a barrier to the appropriate collection, use and sharing of information. Rather, when privacy is properly considered and protected – even and especially in exceptional circumstances – it promotes continued trust in our institutions and ensures that fundamental rights are respected.

This Special Report will present the results of investigations into COVID-related complaints received in late 2021 and 2022. It will also highlight the consultations that we carried out with government agencies over the last 3 years, and provide key observations and lessons learned from the pandemic.

Overall, with a few exceptions, we found that the government's response to the pandemic complied with the requirements of the *Privacy Act* and was also necessary and proportional considering the unprecedented public health crisis. However, to further improve the protection of privacy should a similar situation arise in the future, we have identified some lessons learned and made forward-looking recommendations with respect to purpose identification and the assessment and documentation of potentially less privacy-intrusive measures.

In one instance dealing with the ArriveCAN app, we found a breach of the *Privacy Act* when insufficient measures were taken to ensure the app's accuracy, and fully vaccinated individuals were erroneously notified to quarantine as a result.

Further reading on the OPC website

Commissioner issues guidance on privacy and the COVID-19 outbreak

Commissioner publishes framework to assess privacy-impactful initiatives in response to COVID-19

Supporting public health, building public trust: Privacy principles for contact tracing and similar apps

Investigations

The OPC investigated more than 100 complaints from Canadians about having to provide their COVID-19 vaccination status as a condition of entering Canada, of travelling domestically by plane or train, or of being employed by the federal government. While the core issue for most was the vaccine mandates themselves, complainants also raised concerns about how personal information that was collected for the purpose of managing the pandemic would be protected from oversharing or secondary uses, and how long that information would be kept.

We also investigated complaints about the data collected by the Public Health Agency of Canada (PHAC) on patterns of movement, in response to different public health measures, that was gathered from de-identified and aggregated cellphone location data.

Finally, this report includes our investigation of an error in the ArriveCAN app that caused thousands of individuals to be incorrectly identified as needing to quarantine, as well as the details of an investigation carried out under PIPEDA that found a breach of the private sector privacy law.

In conducting these investigations, we were guided by the key principles set out in our COVID-19 guidance and framework, and the need to consider the relevant context – namely, the urgent and pressing need to take measures to protect the health of Canadians during the COVID-19 crisis, while at the same time ensuring the protection of fundamental privacy rights.

1. Vaccine mandates for domestic travel

From November of 2021 to June of 2022, Transport Canada issued a series of orders requiring air and rail passengers travelling within Canada to provide

Necessity and Proportionality

Though not a requirement of the *Privacy Act*, necessity and proportionality is a privacy principle that our Office strongly endorses and one that is embedded in the privacy laws of many other jurisdictions, including several Canadian provinces. Limiting the collection of personal information to what is demonstrably necessary is also a requirement of the Treasury Board Secretariat (TBS) Directive on Privacy Practices.

This principle is all the more important when institutions must respond quickly in times of crisis to implement measures that are intended to promote and protect public health, given the elevated potential for the measures to infringe on individuals' privacy rights.

To guide institutions in considering necessity and proportionality, our Office promotes a 4-part test that calls for institutions to ask themselves the following questions when establishing potentially privacy-intrusive programs and services:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is there a less privacy-intrusive way of achieving the same end?
- Is the loss of privacy proportional to the need?

The *Privacy Act* currently sets a lower legal threshold for the collection of personal information than necessity and proportionality; it permits federal government institutions to collect personal information where it "relates directly" to an operating program or activity of the government institution. Even though it is not a requirement of the *Act*, our investigations also assessed whether the government institutions met the threshold of necessity and proportionality.

proof of being fully vaccinated. The OPC received 18 complaints under the *Privacy Act* alleging that the collection of this personal information – specifically, the individual's COVID-19 vaccination status – was unlawful, and an unreasonable and unjustified limitation of their freedom of mobility. Some complaints also alleged that COVID-19 vaccines were ineffective and argued that testing or natural immunity were reasonable alternatives.

We did not assess whether the vaccination requirements were an unjustified limitation on individuals' freedom of mobility guaranteed by the *Canadian Charter of Rights and Freedoms* because this issue fell outside of our privacy mandate.

We found that the collection of personal information by VIA Rail, the Canadian Air Transport Security Authority (CATSA) and Transport Canada pursuant to these orders complied with the *Privacy Act* because it was directly related to the organizations' programs for ensuring health and safety on planes and trains.

We also assessed the collection of vaccination status against the principle of necessity and proportionality. Though not a requirement of the *Privacy Act*, necessity and proportionality is a privacy principle that our Office strongly endorses and one that is embedded in the privacy laws of many other jurisdictions, including several Canadian provinces. Limiting the collection of personal information to what is demonstrably necessary is also a requirement of the Treasury Board Secretariat (TBS) Directive on Privacy Practices.

We found that in the fall of 2021, prior to instituting the domestic travel COVID-19 vaccine mandate, the federal government had evidence that COVID-19 presented a serious health risk, and that COVID-19 vaccines were effective both in reducing the risk of spreading the virus and in reducing the risk of serious illness if infected. Apart from certain weaknesses that we elaborate on below, on balance we found that the collection of personal information by VIA Rail, CATSA and Transport Canada under the orders was necessary and proportional, as the requirement to provide proof of vaccination effectively contributed to achieving the objectives of transportation safety by reducing travellers' risk of severe illness, and the benefits to travellers were proportional to the loss of privacy in disclosing their vaccination status.

Weaknesses identified in assessment of necessity and proportionality

While we found that, overall, the collection of personal information under the mandates was necessary and proportional, we identified 2 weaknesses with Transport Canada's assessment of necessity and proportionality.

First, we found that the orders' primary objective of transportation safety was broad, which could give rise to a risk that inappropriate or irrelevant factors may be considered when evaluating the necessity and proportionality of the orders. Transport Canada initially told the OPC that in considering any adjustments to the orders, it took into account factors including "vaccine coverage to support broader societal protection." Transport Canada later clarified that this was a factor considered by PHAC in its advice to government departments, and that increasing Canada's vaccination coverage was not an objective of the orders. However, a Government of Canada news release announcing the domestic travel and federal workplace vaccine mandates on August 13, 2021, stated: "These measures will contribute to reaching the

overall levels of vaccination Canada needs to sustain a resilient economic recovery in the face of more transmissible and dangerous COVID-19 variants of concern."

Further, the broad scope of transportation safety did not differentiate between what may be appropriate for the purposes of protecting individuals from the risks imposed on them by others, and the risks that individuals may accept for themselves. This became material in the spring of 2022, as the effectiveness of COVID-19 vaccines in preventing transmission to others declined over time, while the vaccines remained effective in reducing the risk of severe illness for individuals themselves. Therefore, we recommended that if Transport Canada considers the mandatory collection of personal information for the purpose of transportation safety in the future, that it more clearly define both the intended objectives and the scope of such measures.

Second, Transport Canada indicated it had considered potentially less privacy-invasive alternatives but provided limited documentation of this assessment to our Office. Transport Canada did not, for example, provide evidence to the OPC demonstrating that it considered COVID-19 testing as an alternative to providing proof of vaccination beyond the initial one-month grace period, despite having access to data on this issue, such as PHAC's COVID-19 border testing figures.

While testing as an alternative can reduce the risk of infecting other travellers or transportation workers (i.e., the risk that an individual poses to others), it does not reduce the risk of suffering severe illness (i.e., the risk posed to the individual), which we accept was one of Transport Canada's goals under the broad objective of transportation safety. Therefore, we found that testing would not have been as effective as providing proof of vaccination to achieve this objective.

Nonetheless, we recommended that if Transport Canada considers similar measures in the future, it should more clearly define the scope of the goal and the intended objectives/consequences of such measures, and that it specifically examine and document its assessment of potentially less privacy-invasive alternatives. Transport Canada accepted our recommendations.

Handling of personal information collected was reasonable

Our investigations also examined the government's handling of the personal information collected under the vaccine mandate for domestic travel. We found the personal information handling practices of Transport Canada, CATSA and VIA Rail to be sufficient.

Specifically, we found no indications that the institutions were oversharing the personal information collected, or using it for inappropriate secondary purposes. We found that Transport Canada took appropriate steps to ensure that information-sharing requirements under the orders were clearly set out and minimized the amount of information retained by instructing rail and air carriers to verify – but not retain proof of – individuals' vaccination credentials.

Further reading on the OPC website

Vaccine mandates for domestic travel

2. Vaccine mandate for travellers entering Canada

From July 5, 2021 to September 30, 2022, the Emergency Orders issued by the federal government under the *Quarantine Act* required travellers to provide proof of being fully vaccinated to enter Canada without quarantine, with certain exceptions. We received complaints from 12 individuals with respect to this requirement, similar to those received about the domestic travel vaccine mandates. Some complainants also requested that their information be disposed of and claimed that the Canada Border Service Agency's (CBSA) and PHAC's retention of personal information was unnecessary.

We found that the CBSA and PHAC complied with the *Privacy Act*, as the collection of personal information was directly related to the administration and enforcement of the Quarantine Orders; the personal information was used and disclosed for legally authorized purposes; and the retention measures met the disposal requirement in the *Privacy Act,* the *Privacy Regulations* and the TBS *Directive on Privacy Practices*.

We also assessed whether the collection of this personal information was necessary and proportional. Apart from certain weaknesses that are discussed below, on balance we found that the collections were necessary and proportional in the circumstances. Specifically, the Emergency Orders were issued in response to the urgent public health crisis in order to decrease the risk of introducing and spreading COVID-19 in Canada. This also served the broader goal of protecting the health of Canadians by mitigating the potential burden on the health care system. We found that the collection of travellers' vaccination status was effective in meeting this need and that, on the whole, the loss of privacy experienced by travellers was proportional to the specific need being addressed.

Weaknesses identified in the assessment of necessity and proportionality

Our investigation identified gaps in PHAC's assessment of potentially less privacy-intrusive alternatives, and related issues with respect to the clarity of the objectives, in the final 6 months of the orders. During this period, pre-arrival tests were no longer required for fully vaccinated international travellers while the requirement remained in place for non-fully vaccinated travellers. For this period, PHAC told the OPC that COVID-19 test positivity rates at land ports of entry were relatively similar as between non-fully vaccinated travellers with a negative test result and fully vaccinated travellers. For travellers entering Canada by air, COVID-19 test positivity was consistently higher among fully vaccinated travellers than among pre-arrival tested non-fully vaccinated travellers with a negative test result. PHAC noted that this suggests the effectiveness of pre-arrival testing in reducing the importation of COVID-19 into Canada.

It is a positive step that PHAC collected and reflected on this evidence about the effectiveness of pre-arrival testing. However, as in our investigation of domestic travel vaccine mandates, PHAC did not demonstrate that it considered less privacy-intrusive alternatives, such as

permitting travellers to choose whether to provide a pre-arrival negative test result or proof of vaccination in order to enter Canada without quarantining after April 1, 2022.

PHAC took the position that the purpose clause in the *Quarantine Act*, which states that the objective of the order is "…to protect public health by taking comprehensive measures to prevent the introduction and spread of communicable diseases", necessarily includes not only reducing the importation of a disease into Canada, but also taking steps to reduce the seriousness or impact of an illness that is introduced or spread in Canada when it is not possible to completely stop its introduction or spread.

We recommended that if PHAC considers the mandatory collection of personal information in the future, it should examine and document its assessment of potentially less privacy-intrusive alternatives against objectives that have been clearly defined. PHAC accepted our recommendation. Further, should the *Quarantine Act* be reviewed in the aftermath of the pandemic, we would encourage Parliament to consider explicitly clarifying the scope of the purpose clause in the *Quarantine Act*.

Further reading on the OPC website

Vaccine mandates for entry into Canada

3. Investigations related to the federal government's vaccination attestation requirement

The OPC received many complaints about the vaccination attestation requirements announced by the Government of Canada for federal employees in October 2021. We examined this issue in 3 related investigations. The main allegations were that the collection of employees' vaccination status, and in some cases religious or medical information in support of an accommodation request to be exempted from the requirement, was unreasonable.

We found that the collection of vaccination status complied with the *Privacy Act* as it related directly to institutions' health and safety responsibilities as employers during a national emergency as a result of the COVID-19 pandemic.

After careful review, we determined that while institutions' responses to some of our questions could and should have been more fulsome and forthcoming, the measures were necessary and proportional given the emergency situation that existed and the central role that the TBS and federal public servants played in supporting the federal government's response to the pandemic, including the protection of the health and safety of Canadians and the provision of important and often vital public services during this unprecedented health crisis.

We recommended to TBS that it assess any future contemplated vaccination measures against the 4-part test for necessity and proportionality detailed earlier in this report. The TBS has not agreed to implement this recommendation.

Our investigations also found that overall, the handling of personal information, once collected, complied with the requirements of the *Privacy Act*, with a few notable exceptions. For example, our examination of the system used to collect vaccine attestations for Canadian Armed Forces (CAF) members, Monitor-MASS, found that this system had inadequate oversight to prevent unauthorized access to this personal information. While we did not find any instances of inappropriate access, we recommended measures to periodically ascertain that units properly review and revoke permissions that provide access to CAF members' sensitive information in Monitor-MASS where there is no longer, or never was, a need for access. The Department of National Defence (DND) has not agreed to implement this recommendation.

We also investigated allegations of specific incidents of inappropriate disclosure of personal information. We found that 2 cases of mail processing errors, which Canada Post subsequently investigated and addressed, led to the disclosure of personal information related to individuals' vaccination status. One mailing error led to approximately 3,500 Canada Post employees who had not complied with the institution's vaccine attestation requirements, or had attested to being partially vaccinated, receiving mail intended for a different employee in a similar situation. We also found that in 2 cases, DND/CAF personnel inappropriately disclosed to unauthorized recipients the identity and other details relating to the COVID-19 vaccination status of several individuals who had not attested to being fully vaccinated, or who had requested an accommodation. We also investigated situations where an employee at the CBSA and another at Global Affairs Canada inappropriately shared with the employee's work unit that they were on leave because they were unvaccinated. We did not find any indication of systemic concerns in our investigation of these incidents.

Finally, as described in the attached report Core Public Administration vaccination report, we found that the TBS contravened section 11 of the *Privacy Act* by not adding a Personal Information Bank (PIB) description for the COVID-19 vaccination attestation information to its published index within the required 12-month timeframe, though it has now done so. The PIB Index is a transparency and accountability tool that describes the personal information being held by the institution, as well as how it is collected, used, disclosed and retained or disposed of. While the attestation notification provided to employees at the time clearly described the purpose for which the personal information was being collected, we remind the TBS of its obligations under section 11 of the *Act*.

Further reading on the OPC website

Investigation into COVID-19 vaccination attestation requirements established by the Treasury Board of Canada for employees of the core public administration

Investigation into COVID-19 vaccination attestation requirements established by Department of National Defence for members of the Canadian Armed Forces

Investigation into COVID-19 vaccination attestation requirements established by certain separate employers of the federal public service

4. ArriveCAN application error inaccurately identified certain travellers as needing to quarantine

To determine a given traveller's applicable entry requirements under the Quarantine Orders in place from February 3, 2020 to September 30, 2022, and to ensure that these requirements were being respected, the CBSA and PHAC collected personal information from individuals entering Canada, primarily through the ArriveCAN mobile app.

Given the Emergency Orders' important consequences on the rights and mobility of incoming travellers, it is our view that a high degree of due diligence was required under the section 6 accuracy provisions of the Act to ensure the accuracy of the personal information contained in ArriveCAN and that was used in administrative decisions about those individuals. We therefore expected to see: (i) rigorous pre-release testing for issues that could lead to high negative impacts on individual users; (ii) effective human intervention with respect to high-impact decisions on individuals and (iii) effective and timely correction and recourse for individuals.

An error in version 3.0 of ArriveCAN, which was released on June 28, 2022, had the disruptive and distressing effect of causing approximately 10,000 fully vaccinated Apple device users to receive erroneous messages advising that they were required to quarantine even though they had met the conditions for quarantine exemption. Travellers using version 3.0 of ArriveCAN for Apple mobile devices, and who had saved their submission form after selecting the travellers for the trip and then later returned to the form to complete the submission, incorrectly had their "quarantine exempted" value set as "false" by ArriveCAN. Unfortunately, the error was not caught by the CBSA's pre-release testing of the app, and due to the system's design, it was not caught by screening officers when the affected travellers crossed the border. It took more than 3 weeks for the CBSA to stop the error from affecting new travellers, and nearly a month until a correction was sent to all affected individuals. We acknowledge that the pandemic caused significant challenges for government and public health authorities, but also note that the incident in question occurred more than 2 and a half years after the ArriveCAN app was introduced. Ultimately, our investigation found that the CBSA did not meet the requirements of the *Privacy Act* because it did not take all reasonable steps to ensure the accuracy of the information about individuals that it used for administrative decision-making processes that affected them.

The OPC recommended that the CBSA correct the inaccurate information in its data holding that was generated by the error. To date, the CBSA has refused to do so, and we hope that it will reconsider its position, correct and/or dispose of the inaccurate information in its possession, and put in place all necessary measures to mitigate the risk that such errors occur in the future.

Further reading on the OPC website

Erroneous quarantine notifications from ArriveCAN

5. Investigation into the collection and use of de-identified mobility data in the course of the COVID-19 pandemic

The OPC received 12 complaints under the *Privacy Act* against PHAC and Health Canada regarding the collection and use of Canadians' mobility data, which is comprised of geolocation data collected over time and other associated information.

The complainants alleged that PHAC secretly collected data on 33 million mobile devices during the COVID-19 pandemic, and that according to a request for proposal published in December 2021 to procure continued access to operator-based location data, it planned to continue to collect Canadians' mobility data over the ensuing 5 years.

In response to the complaints, PHAC stated that it relied on de-identified and aggregated data and did not collect or use any personal identifiable information, and that as a result, the *Privacy Act* did not apply.

Our investigation assessed whether there was a serious possibility that an individual could be identified using the mobility data procured by PHAC alone, or in combination with other available information.

We concluded that the combination of the de-identification measures and the safeguards against re-identification implemented by PHAC and its data providers reduced the risk that individuals could be re-identified below the "serious possibility" threshold. Therefore, we found that PHAC did not collect personal information and the *Privacy Act* does not apply. As we have done previously, we recommended that the government propose amendments to the *Privacy Act* to include a clear legal framework that defines the different types of de-identified data and specifies the rules that should govern the production, retention, use, disclosure, and collection of each type.

Canadians also raised concerns regarding the lack of transparency about PHAC's collection and use of mobility data. In this instance, the *Privacy Act* does not impose transparency obligations on PHAC because it did not collect personal information as defined under the *Act*. However, as noted in our framework released in the early days of the pandemic, we recommend that the government provide clear and detailed information to Canadians about the basis for any exceptional measures it implements, as well as the applicable terms for such measures, and be accountable for them.

As a final note, our investigation did not assess whether the private-sector third parties that provided the mobility data to PHAC collected and used the information in compliance with their privacy obligations, including whether they obtained informed consent. We would emphasize that organizations procuring de-identified data are also accountable and should take the necessary steps to ensure that the third parties they work with are complying with privacy laws.

Further reading on the OPC website

Investigation into the collection and use of de-identified mobility data in the course of the COVID-19 pandemic

6. Investigation under PIPEDA

Earlier in the pandemic, we investigated a complaint that Biron Health Group used a traveller's email address to send him marketing and promotional material without his consent after he underwent COVID-19 testing upon his arrival at an airport. Biron Health Group believed that it could rely on the complainant's implied consent to use his information in that way.

The OPC found that Biron Health Group could not imply consent of travellers arriving in Canada to use the information that it had collected for one purpose – mandatory COVID testing – for another purpose, such as marketing. Sensitive personal information generated in a crisis may have high-value applications to public and private sector organizations, but must be used within the limitations of the law. Even and especially in emergency situations, organizations must continue to operate under lawful authority and act responsibly, particularly with respect to handling personal health information, which is generally considered sensitive.

As Biron Health Group agreed to cease this practice in this case, the complainant agreed to treat the matter as settled. A full case summary is on our website.

Public-private partnerships

The COVID-19 crisis required government and private-sector organizations to collaborate to achieve public policy goals. This work highlighted gaps in our current legal framework and exposed the pressing need to examine issues related to public-private partnerships.

For example, we noted that in cases where the legal authority for an initiative was based on consent obtained by a private-sector organization, there was often no policy requirement for government institutions to ensure that this consent was meaningfully obtained.

TBS asserted that it could not add such a requirement because it was limited to the existing legal framework. According to the TBS, compelling departments to ensure that the government's private-sector partners had obtained meaningful consent would require legislative amendments.

As a result, under the current privacy laws, a public sector institution could deploy a technological solution to the pandemic that allows its private-sector partner to use the personal information collected for commercial purposes unrelated to public health. This raises issues with respect to the meaningfulness of consent in public-private relationships. In particular, there is a risk that where information is collected by a private-sector organization on behalf of the government, the organization's own commercial uses of that information may not always be well-understood.

We recommend that privacy laws be modernized to enshrine common privacy principles for the public and private sectors, and to set explicit limits on the permissible uses of data.

Engagement under the *Emergencies Act*

Illegal protests linked to the vaccine mandates occurred in several locations in early 2022, leading to the invocation of the *Emergencies Act*. The temporary powers granted as a result of the *Emergency Economic Measures Order* allowed law enforcement agencies to work more closely with banks and other financial service providers, and provided additional measures to monitor and disrupt financial activity associated with illegal blockades. While the activities of federal institutions must be limited to those that fall within their legal authority and comply with applicable laws, including the *Privacy Act*, the Order granted a temporary authority to share certain personal information, such as a requirement for financial service providers to disclose information to the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS). After concerns were raised by Member of Parliament Michelle Rempel Garner about the privacy implications of the use of the *Emergencies Act*, our Office engaged with the RCMP, CSIS and the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

As we noted in our submission to the Special Joint Committee on the Declaration of Emergency, we assessed against the *Privacy Act* how these 3 institutions collected, used and disclosed personal information under the provisions of the order, and our observations are included in this report.

We found that reasonable steps were taken to identify relevant, accurate and necessary information to assist financial institutions in meeting their obligations under the order, and that the sharing of personal information was proportionate to the needs arising from the unprecedented situation and the legal obligations imposed on the institutions under the *Emergencies Act*.

However, we found that there was a lack of clear direction on the limits to information sharing under the order. For example, we found that the order did not specify the conditions or requirements for information sharing, including the specific types and scope of personal information that could be shared, or how the information was to be shared; nor did it contain any explicit safeguard requirements to ensure that appropriate procedures were established and implemented to protect personal information. The need for organizations to act in a timely and efficient manner during a crisis makes it important to have clear and specific processes and guidance for information sharing so that government institutions and financial entities are aware of their obligations, and to ensure transparency and accountability to Canadians for the protection of their personal information.

Conclusion

Overall, our investigations found, with some exceptions, that the measures implemented by the government during the pandemic complied with relevant privacy laws and were necessary and proportional in response to the unprecedented public health crisis. We also observed that government initiatives generally adhered to the privacy principles set out in our guidance and

framework, as well as other statements and resolutions that we issued jointly with our provincial and territorial colleagues during the pandemic.

However, in some cases, there were weaknesses in how the government assessed and documented potentially less privacy-intrusive alternatives. The government could also have taken steps to enhance transparency with respect to the measures it implemented, such as PHAC's use of mobility data, and to clarify the scope of the objectives of vaccine mandates. As we noted at the outset of the pandemic, greater flexibility to use personal information for the public good should be accompanied by greater transparency and accountability.

Our investigations also highlighted the importance and usefulness of including the criteria of necessity and proportionality in assessing proposed measures under privacy principles.

In our consultations with the government, we found that while federal institutions had a genuine desire to identify and mitigate privacy risks in pandemic-related initiatives, there were obstacles, including the lack of privacy expertise, resources, and reliable processes in some institutions.

The impact of the pandemic continues to reverberate throughout our society, including in relation to privacy. There is important work to be done to ensure that personal information that is no longer needed is properly deleted, where appropriate, and that any new collections initiated during the pandemic (for example, the information collected via the ArriveCAN app) be carefully reviewed for ongoing necessity and proportionality.

During the pandemic, certain privacy protective processes, such as TBS requirements to conduct Privacy Impact Assessments of new collections and new uses of personal information, were not enforced, and certain tools, like ArriveCAN, were put into place quickly to meet pressing demands. It is a privacy lesson from the pandemic that where action is taken quickly to respond to an emergency, it is even more important to ensure that the policies and tools are carefully reviewed once in place and then regularly reassessed to ensure that they remain proportional and necessary, and as privacy protective as possible.

Some technologies and programs that were developed for urgent and special purposes during the pandemic were retained and used for ordinary activities after the initial emergency waned. Changes introduced as a result of the pandemic will be leveraged for continuing programs, expanding the use of digitization and advanced data analytics. It is essential that the privacy impacts of these and any other new initiatives be considered and addressed in consultation with the OPC.

The COVID crisis underlined the importance of developing a culture of privacy – building privacy principles such as necessity and proportionality into the DNA of new initiatives that deal with sensitive personal information. Government institutions and organizations need to engage with our Office early – whether in a crisis or not – so that the OPC can help them to accomplish their goals in a privacy-protective manner. While the OPC appreciates that a crisis requires expedient action, and a flexible and contextual approach to applying the law, the privacy rights of Canadians must always be protected. And finally, understanding that restrictions and impositions on privacy rights may be taken to combat a crisis, once the crisis ends, those restrictions must be promptly lifted.

Appendix 1: Engagement under the *Emergencies Act*

Table of contents

Overview

After concerns were raised by Member of Parliament ("MP") Michelle Rempel Garner about the privacy implications of the use of the *Emergencies Act*[1], our Office committed to engaging with three federal institutions regarding the implementation of the temporary emergency measures in relation to the collection and disclosure of Canadians' personal financial information.

The scope of the engagement was focused on pursuing lines of enquiry based on the *Privacy Act*, and specifically, to understand how the Royal Canadian Mounted Police (the "RCMP"), the Canadian Security Intelligence Service ("CSIS") and the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") handled personal information within the context of the *Emergencies Act* and related Emergency Economic Measures Order (the "Order").[2] Specifically, we reviewed how these institutions operationalized the provisions of the Order in relation to the collection and disclosure of personal information, including: (i) the steps taken to ensure the accuracy of personal information; (ii) whether personal information was used or disclosed for other purposes than the original purpose of collection; and (iii) what consideration had been given by the institutions to the publication of a new or modified Personal Information Bank ("PIB") to describe any personal information that was used, is being used, or is available for an administrative purpose as a result of the invocation of the *Emergencies Act.* We communicated the objectives of the engagement to the three institutions, in writing, in March 2022.

The Order was issued pursuant to the *Emergencies Act* and empowered law enforcement agencies to work more closely with banks and other financial service providers ("financial entities") and provided additional measures to monitor and disrupt financial activity associated with the illegal blockades. These measures included, among other things: (i) a requirement for certain financial entities to determine whether they have in their possession or control, property that is owned, held or controlled by or on behalf of a designated person[3] and to disclose this information to the RCMP or CSIS; (ii) a temporary authority for federal, provincial and territorial government institutions (including the RCMP, FINTRAC and CSIS) to share relevant information with financial entities if the disclosing institution was satisfied that the disclosure would contribute to the application of the Order; and (iii) a requirement for certain entities (e.g., crowdfunding organizations) to register and report certain financial transactions to FINTRAC.

Based on our fact finding and consideration of the roles of these three institutions with respect to the temporary powers granted as a result of the invocation of the *Emergencies Act*, we have assessed, against the *Privacy Act*, how personal information was collected and disclosed by these institutions under the provisions of the Order.

[1] *Emergencies Act* (R.S.C., 1985, c. 22 (4th Supp.))
[2] Emergency Economic Measures Order: SOR/2022-22
[3] Designated person means any individual or entity that is engaged, directly or indirectly, in an activity prohibited by sections 2 to 5 of the Emergency Measures Regulations.

Overall, we found that the disclosures of personal information made by the RCMP to financial entities were limited in scope and nature, and for the express purpose of allowing financial entities to meet their obligations under the Order (i.e., to determine whether they are in possession or control of property that is owned, held or controlled by or on behalf of a designated person). We found that the RCMP took reasonable steps to: (i) validate information before sharing it with financial entities, and (ii) assess and identify those entities to which disclosures should be made. There was no evidence to suggest that the disclosures of personal information made by the RCMP exceeded the parameters of what was necessary for financial entities to meet their obligations under the Order. All disclosures made by the RCMP were accompanied by a letter which provided the rationale and legislative authority for sharing the information, and a caveat for the use and safeguarding of the information. We found no indication that personal information was used or disclosed for other purposes beyond the purpose of collection – that is, to fulfil the obligations under the Order.

With respect to our engagement with FINTRAC, we found that the information exchanges that occurred during the time the Order was in place were based on the authorities set out in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the "PCMLTFA").[4] As such, any reporting FINTRAC received from existing entities and any financial disclosures it made were based on the existing thresholds under the PCMLTFA. FINTRAC did not track information about "designated persons" as defined in the Order, nor did it confirm or take into account whether an individual or entity named in a financial intelligence disclosure was a "designated person".

We confirmed during our engagement with CSIS that it did not request any specific measures under the *Emergencies Act*, nor did it benefit from any new authorities under the *Emergencies Act.* We also confirmed that CSIS did not receive any information from any of the financial entities set out in section 3 of the Order.

We note that FINTRAC and CSIS may have collected and disclosed personal information pursuant to their own legislative authorities during the period the *Emergencies Act* was invoked, however, we did not pursue lines of enquiry beyond the scope of the engagement objectives (i.e., how these institutions operationalized the temporary powers granted in the Order for the collection and disclosure of personal information).

These were extraordinary circumstances[5] and institutions were compelled to act quickly to respond to the requirements of the Order. Given the privacy implications and the potential for these temporary measures to infringe on Canadians' privacy rights, we also considered the use of these powers in light of the general principles of necessity and proportionality. While not

[4] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17)

[5] Protest blockades had effectively shut down numerous governmental operations and border crossings in Ottawa, Windsor, and Coutts, Alberta. Similar protests experienced in other jurisdictions - including the US, France, and most recently, Brazil - had become both destructive and violent. Policing attempts at de-escalation were faltering.

legal requirements under the Act, government institutions should ensure that measures taken are necessary and proportionate, even in exceptional circumstances. Our Office encourages organizations to apply a four part test to weigh the appropriateness of potentially privacy-invasive measures. Adapted from the 1986 Supreme Court of Canada decision in *R. v. Oakes*[6], the test weighs privacy implications in light of four questions relating to the necessity, effectiveness and proportionality of the measure, and whether less privacy-invasive methods could have achieved the same goal. Based on this, our engagement examined whether information exchanges pursuant to the Order were necessary and proportionate to the needs and legal obligations arising as a result of the temporary measures. We did not examine whether the specific temporary measures selected by the Government to deal with the situation that led to the declaration of the public order emergency were necessary and proportionate (and/or met the four part test). This issue is being considered by the Public Order Emergency Commission ("POEC")[7] and by the Special Joint Committee on the Declaration of Emergency ("DEDC").[8]

In light of the above, we considered whether only necessary information was shared, that the information was shared with the appropriate entities, and whether the information shared was proportionate to the need and level of risk. Based on the information we received during the engagement, we found that reasonable steps were taken to identify relevant, accurate and necessary information to assist financial entities in meeting their obligations under the Order. We also found that steps were taken to limit the sharing of that information, and that there was consideration for the safeguarding of the information disclosed. Information sharing was also time-limited and ceased when the temporary powers were revoked. Overall, we found that the sharing of personal information was proportionate to the needs arising from the unprecedented situation and the legal obligations deriving from the declaration of a public order emergency under the *Emergencies Act*.

Notwithstanding the above, we found that there was a lack of clear direction and/or guidance in relation to the specific requirements for information sharing under the Order. In particular, we noted that the Order did not include provisions for the precise types and scope of personal information that should be shared by financial entities with the RCMP, or how information should be shared by federal, provincial and territorial government institutions with financial entities. These were unique circumstances that allowed for the sharing of sensitive personal information. The mere fact that these individuals were identified as "designated persons" elevates the sensitivity of the information being disclosed and requires processes to ensure that information sharing practices are understood and effectively implemented. Further, given

[6] *R. v. Oakes* [1986] 1 S.C.R. 103
[7] The Public Order Emergency Commission was established to inquire into the circumstances that led to the declaration of emergency and the measures for dealing with the emergency
[8] Under subsection 62(1) of the *Emergencies Act*, a parliamentary review committee must review the "exercise of powers and the performance of duties and functions pursuant to a declaration of emergency." Accordingly, the DEDC was established by motion of the Senate and House of Commons on March 3, 2022.

the urgent circumstances, the RCMP and financial entities had to act in a timely and efficient manner to fulfil their obligations under the Order. This underscores the importance of having clear and specific processes and guidance for information sharing so that both government institutions and financial entities are aware of their obligations, and to ensure transparency and accountability to Canadians for the protection of personal information. This will assist institutions to effectively meet their obligations under the temporary measures, and also under relevant privacy laws, including the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

At the conclusion of our engagement, the RCMP, FINTRAC and CSIS were provided with an opportunity to review and comment on the findings and observations noted by our Office. We would like to express our appreciation to each of these institutions for their open and collaborative engagement with our Office on this important matter.

Our engagement findings and observations are detailed in the report that follows.

Background

1. On February 14, 2022, the federal government declared a public order emergency under the *Emergencies Act* to end border disruptions, blockades and the occupation of the city of Ottawa. As a result of the invocation of the *Emergencies Act*, the federal government made special temporary measures for dealing with the emergency which were detailed in the Emergency Measures Regulations (the "Regulations").[9] In addition, a series of financial measures to limit funding of illegal blockades and restore public order were announced. The details of those measures were outlined in the Order. The declaration of the public order emergency was revoked by the federal government on February 23, 2022.

2. On February 17, 2022, the OPC received correspondence from MP Rempel Garner expressing concerns about the privacy implications of the use of the *Emergencies Act*, including the disclosure of financial information to the RCMP, CSIS and FINTRAC. MP Rempel Garner requested that we "investigate the use of these temporary powers in light of existing privacy laws and the concept of proportionality".

3. While MP Rempel Garner's correspondence did not raise a complaint with respect to a specific contravention of the *Privacy Act*, we felt that due diligence was required given the privacy implications and concerns raised following the invocation of the *Emergencies Act*. As such, we opted to pursue an informal engagement with these three institutions to better understand how they operationalized the temporary powers granted under the *Emergencies Act* in relation to the collection and disclosure of personal information.

4. We also note that during our engagement with these institutions, various parliamentary committees were concurrently studying the Government's actions in relation to the invocation of the *Emergencies Act* and related measures. We have followed with interest

[9] Emergency Measures Regulations: SOR/2022-21 (Canada Gazette, Part II, Volume 156, Extra Number 1).

the testimony presented by the RCMP, CSIS and FINTRAC to those committees, as well as the POEC which was established to inquire into the circumstances that led to the declaration of emergency and the measures for dealing with the emergency.

Scope

5. The scope of the engagement was limited at the outset to the three government institutions identified in MP Rempel Garner's correspondence, namely the RCMP, CSIS and FINTRAC, and was focused on pursuing lines of enquiry based on the *Privacy Act*.

6. The objectives of the OPC's engagement were to:

    (i) understand the role of these three institutions with respect to the execution of the temporary powers and authorities deriving from the *Emergencies Act* as they relate to the collection and disclosure of personal financial information, and how these institutions operationalized the provisions of the Order with respect to the collection and disclosure of personal financial information; and

    (ii) within the context of the *Emergencies Act*, to understand and assess how these three institutions handled personal information pursuant to the *Privacy Act*, including:

    (a) what steps were taken, as required by Section 6 of the *Privacy Act* to ensure accuracy of personal information used for administrative purposes;

    (b) with respect to sections 7 (use) and 8 (disclosure) of the *Privacy Act*, whether these institutions used or disclosed personal information collected for other purposes than the original purpose of collection and if so for what purposes; and

    (c) what consideration has or will be given by the institutions to the publication of a new or modified PIB description, as required by sections 10 and 11 of the *Privacy Act*, to describe any personal information that has been used, is being used, or is available for an administrative purpose as a result of the invocation of the *Emergencies Act*.

7. The findings of the OPC's engagement with each of the three institutions are outlined below.

The Order

8. The Order was issued pursuant to the *Emergencies Act* to allow law enforcement agencies to work more closely with financial entities and provided additional measures to monitor and disrupt financial activity associated with the illegal blockades. These measures included:

- A requirement for financial entities[10] listed under section 3 of the Order to determine whether they have in their possession or control property that is owned, held or controlled by or on behalf of a designated person and to disclose this information, without delay, to the RCMP or CSIS. "Designated person" means any individual or entity that was engaged, directly or indirectly, in an activity prohibited by sections 2 to 5 of the Regulations.

- The authorization for federal, provincial, and territorial government institutions to disclose information to any entity set out in section 3 of the Order if satisfied that the disclosure would contribute to the application of the Order. This allowed law enforcement agencies to share the identity of designated persons with financial entities, enabling them to cease their dealings with those designated persons at their discretion.

- A requirement for certain entities (crowdfunding platforms and some payment service providers not previously subject to registration and reporting requirements to FINTRAC) to register with FINTRAC if they were in possession or control of a designated person's property. The Order also required that these entities report certain suspicious and large value transactions to FINTRAC.

9. The Order was automatically revoked when the *Emergencies Act* was revoked on February 23, 2022.

Engagement with the RCMP

Temporary powers granted under the Order

10. Section 5 of the Order required financial entities set out in section 3 to disclose information to the RCMP or CSIS, including the existence of property in their possession or control that was owned, held or controlled by or on behalf of a designated person, and any information about a transaction or proposed transaction in respect of that property.

11. The Order also authorized the RCMP to disclose information to financial entities when it was satisfied that the disclosure would contribute to the application of the Order, as per section 6. This allowed the RCMP to share the identity of individuals involved in the illegal protest, and that of owners and/or drivers of vehicles who did not want to leave the areas impacted by the protest, with financial entities, thereby enabling them to cease their dealings with those designated persons at their discretion.

12. The financial entities had a duty to determine on a continuing basis whether they were in possession or control of property that was owned, held or controlled by or on behalf of a designated person, and to cease dealings with that designated person (i.e., freeze assets), as per sections 2 and 3 of the Order.

[10] "Entity" includes a corporation, trust, partnership, fund, unincorporated association or organization or foreign state.

Scope of personal information received by the RCMP

13. The RCMP confirmed that it received information from 20 different financial entities, as required by section 5 of the Order. The information related to financial products held by 69 individuals who were subject to account freezing under the Order. In certain cases, linked corporate accounts were also frozen. Of these 69 individuals, the RCMP confirmed that it received information in relation to approximately 20 individuals that did not appear to be resulting from information disclosed by the RCMP to financial entities. The information of these 20 individuals was disclosed pursuant to the financial entities ongoing duty noted in paragraph 12 above.

14. However, the RCMP noted that the Order did not describe the types of information that financial entities were required to report; therefore, the information received by the RCMP varied in scope and detail. For example, in certain cases, the information reported may have included account holder names, account numbers, account balances, and rationales for the account freezes. In other cases, very little detail was reported by financial entities – i.e., the entity reported that "action had been taken in relation to X number of individuals", unaccompanied by any identifying particulars such as name or account number.

15. The RCMP confirmed that it did not request additional information from those financial entities that did not provide any identifying particulars in relation to individuals against whom they took action. The RCMP reported that, pursuant to sections 2 and 3 of the Order, the onus was on financial entities to determine whether they were in possession or control of a designated person's property and to cease dealings with those individuals (i.e., to freeze the assets of those individuals). Further, the RCMP stated that it had no oversight or authority over the actions taken by financial entities under the Order.

16. The RCMP confirmed that the information it received pursuant to section 5 of the Order is being managed in the Police Reporting and Occurrence System ("PROS") – the RCMP's occurrence records management system. The personal information will be retained for five years in accordance with the RCMP's information retention policies.[11]

17. The PIB that describes the collection, use, retention and disclosure of personal information for the administration or enforcement of the law is listed in InfoSource[12] as RCMP PPU 005 entitled "Operational Case Records".[13] The RCMP indicated that it has

---

[11] Institutions are required under subsection 6(1) of the *Privacy Act* to retain personal information that has been used for an administrative purpose for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information. Subsection 4(1) of the Privacy Regulations requires the personal information to be retained for at least two years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal.

[12] *InfoSource: Sources of Federal Government and Employee Information* provides information about the functions, programs, activities and related information holdings of government institutions subject to the *Access to Information Act* and the *Privacy Act*. It provides individuals and employees of the government (current and former) with relevant information to access personal information about themselves held by government institutions subject to the *Privacy Act* and to exercise their rights under the *Privacy Act*.

[13] RCMP PPU 005

not yet identified a consistent use[14] for the information that it received pursuant to section 5 of the Order.

Scope of personal information disclosed by the RCMP

18. The RCMP submitted that its efforts were focused on identifying individuals and entities who were actively involved in illegal action, either by organizing or influencing the illegal activities or by being present at the illegal protests.

19. The RCMP reported that there were two streams of disclosures made pursuant to the Order. In the first stream, the RCMP acted as a channel of communication between the Ottawa Police Service ("OPS") and the Ontario Provincial Police ("OPP") and financial entities,[15] and disclosed information on behalf of those police services relating to individuals who were identified as implicated in the illegal protest. The personal information included the names of individuals, dates of birth, residential addresses, relevant open source information[16], and related police information regarding their subjects of investigation. Given that the RCMP acted as a conduit between the police services and financial entities, the RCMP confirmed that it did not assess or supplement the information it shared on behalf of the police services.

20. In the second stream, the RCMP received information from the OPP in relation to vehicles observed in the assembly area. The RCMP corroborated the vehicle information and presence of individuals involved in the illegal protest and disclosed information in relation to individuals who were identified as owners and/or drivers of vehicles who did not want to leave the assembly area. The personal information disclosed included the name of the registered owner of the vehicle, the registered address on file, and information that would have contributed to the application of the Order, including open source information such as social media posts (i.e., Facebook, Twitter, LinkedIn, etc.) that supported the positive identification and potential last known location of an individual connected to a vehicle.

21. With respect to the nature and limits of personal information disclosed from open sources, the RCMP confirmed that the open source information included the names, addresses, and photographs of individuals and information on related businesses, including the names of businesses, the phone number, address and web address associated to the businesses where applicable, and the names of lawyers representing the businesses. The RCMP submitted that the sharing of open source information was limited in scope and only disclosed to assist financial entities to confirm and/or verify the identity of the individual in question. This also assisted entities to avoid targeting individuals that may share the same or similar name to the individuals participating in the illegal blockades.

---

[14] Under the *Privacy Act*, a government institution is permitted to use and disclose personal information for new purposes when those new purposes are consistent with the purposes for which personal information was collected – in other words, for a "consistent use".

[15] The RCMP reported that the Order did not prescribe how information was to be shared with financial entities; therefore, in an effort to be efficient and reduce redundancy, the RCMP acted as a conduit for provincial and territorial institutions to streamline communications and the sharing of information with financial entities.

[16] Open source information generally refers to information collected from the internet that is publicly available, such as information from websites, blogs, social networks, etc.

22. The RCMP confirmed that it did not share information relating to individual donors or those who purchased merchandise linked to the convoy/illegal protests.

23. According to the RCMP, it conducted extensive research to validate and ensure the accuracy of information before making disclosures to financial entities.[17] This included contacting individuals to confirm their ongoing participation in prohibited activities before sharing information with financial entities. For example, a number of individuals contacted by the RCMP confirmed that they were participating in the blockade in Ottawa and refused to leave. These individuals were advised by the RCMP of the risk that their bank accounts could be frozen pursuant to the Order. In other cases, there were individuals who wanted to leave but were not able to do so because the streets were not cleared. The RCMP reported that these individuals were instructed to ensure their truck was ready to leave when the streets were cleared, and information related to these individuals was not provided to financial entities.

24. The RCMP also indicated that, in a number of instances, its investigation resulted in a decision to not disclose information to financial entities if there was insufficient information to believe the person or entity was involved (i.e., the licence plate was invalid in the police database system, the person was attempting to leave but were unable to, or it was no longer believed the person or entity was involved). In some cases, the individual either left on their own accord or were removed by local police services.

25. According to the RCMP, it made a total of 57 disclosures to financial entities pursuant to section 6 of the Order. These disclosures included the identity of 62 individuals and 17 businesses.[18]

26. The RCMP confirmed that the disclosures to financial entities were framed as being "relevant to individuals or entities that are engaged, directly or indirectly, in an activity prohibited by sections 2 to 5 of the Emergency Measures Regulations". The RCMP also advised the financial entities that they would need to supplement the law enforcement information provided with their internal holdings in order to meet their own obligations under the Order.

27. During our engagement, we asked the RCMP to confirm how it determined which financial entities to share information with. The RCMP indicated that it made best efforts to identify entities to whom disclosure should be provided pursuant to section 6 of the Order, and to provide those entities with timely and relevant information. Therefore, the RCMP submitted that it assessed that certain organizations, such as banks, the Canadian Bankers Association, the Investment Industry Regulatory Organization of Canada, the Canadian Securities Administration, Credit Unions, and the Mutual Fund

[17] As noted at paragraph 19, the RCMP did not validate the information it shared on behalf of the police services – in those cases, the RCMP confirmed that it only acted as a conduit to streamline communications and the sharing of information with financial entities.
[18] The RCMP also disclosed 170 bitcoin wallet addresses to virtual asset service providers. Source: RCMP Institutional Report to the Public Order Emergency Commission

Dealers Association, were entities as defined by section 3 of the Order, and that disclosure to these entities would contribute to the application of the Order (as required by section 6).

28. The RCMP provided our Office with a list of all financial entities to which the information was disclosed pursuant to the Order, along with the RCMP's justification for sharing with those entities. As the disclosing institution, the RCMP submitted that it was satisfied that the information was relevant to individuals or entities that were engaged, directly or indirectly, in an activity prohibited by sections 2 to 5 of the Regulations, and that disclosure would contribute to the application of the Order.

29. We also asked the RCMP to confirm the steps taken to ensure the safeguarding of the information disclosed, including any provisions regarding the sensitivity of the information, or any instructions for the safeguarding, sharing or dissemination of the information by receiving entities. The RCMP confirmed that it identified points of contact within the financial entities to send the information to in order to minimize the broad circulation of the information. In addition, the RCMP provided financial entities with a "disclosure letter" which outlined the rationale and legislative authority for sharing the information and the classification level of the information being provided by the RCMP. The disclosure letters included a caveat that the document was the property of the RCMP, that it was provided on loan with the understanding that it was not to be further disseminated, reclassified or used for other purposes without the consent of the RCMP, and that distribution was to be done on a need-to-know basis. The caveat also stated that the document was to be protected in accordance with normal safeguards for law enforcement information.

30. According to the RCMP, once the information was received by the financial entities, it was understood that it was the responsibility of each entity to safeguard the information in line with their own regulations and policies, as well as their obligations under PIPEDA, and that the information was only to be used to fulfil the entities' obligations pursuant to the Order.

31. The RCMP provided our Office with a redacted copy of a sample disclosure made pursuant to the Order. As noted previously, the disclosure document included categories of information such as tombstone data (name, home address, date of birth), vehicle information, RCMP database checks[19] and relevant open source information.

32. We also requested information from the RCMP regarding the classification of the information disclosed to financial entities and the method of transmission. The RCMP confirmed that the information it disclosed was sent via unencrypted email to the points of contact identified within the financial entities. According to the RCMP, the information it disclosed is classified as "Protected A"[20], therefore, in accordance with the RCMP's

[19] Canadian Police Information Centre (CPIC), Police Reporting and Occurrence System (PROS), and Police Information Portal (PIP).

[20] "Protected A" applies to information when unauthorized disclosure could reasonably be expected to cause limited or moderate injury outside the national interest, for example, disclosure of an exact salary figure. Source: Treasury Board Secretariat "Directive on Security Management – Appendix J: Standard on Security Categorization

Departmental Security Policy, the RCMP stated that it was authorized to transmit the information via unencrypted email.

33. The RCMP confirmed that any personal information collected and disclosed pursuant to the requirements of the Order is retained in PROS.

Engagement Findings – RCMP

34. Overall, we found that the disclosures of personal information made by the RCMP to financial entities were limited in scope and nature (i.e., the disclosures included the identity of 62 individuals and 17 businesses), and for the express purpose of allowing financial entities to meet their obligations under the Order (i.e., to determine whether they are in possession or control of property that is owned, held or controlled by or on behalf of a designated person).

35. We found that the RCMP conducted due diligence by assessing and validating the information before sharing it with financial entities, which included validating licence plate information, the use of open source information[21] to support the positive identification and potential last known location of an individual connected to a vehicle, and contacting individuals to confirm their presence and/or participation in the illegal blockades. The RCMP also advised individuals of the consequences of their participation in prohibited activities in light of the requirements of the Order and did not disclose information related to individuals who were attempting to leave but were not able to do so because the streets were not cleared.

36. In our view, the RCMP took reasonable steps to ensure the accuracy and completeness of the information it disclosed to financial entities and that the information was relevant to individuals or entities engaged in an activity prohibited by sections 2 to 5 of the Regulations. This is in line with the RCMP's obligations under subsection 6(2) of the *Privacy Act* which requires government institutions to take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

37. With regards to the RCMP's use and disclosure of personal information collected under the authority of the Order, we found no indication that personal information was used or disclosed by the RCMP for purposes other than the purpose of collection. In particular, the RCMP received information from 20 different financial entities which related to financial products subject to freezing under the Order, and which was required by section 5 of the Order. The RCMP confirmed that it shared information received from a financial entity with another police service during the time the Order was in force for law enforcement purposes; but otherwise noted that it has not identified a consistent use for the information it received pursuant to section 5 of the Order that would warrant its sharing with a third party.

[21] We did not examine the tools used by the RCMP to collect open source information as part of this engagement. Our Office is investigating the RCMP's use of social media monitoring technology as a separate matter. See Investigations.

38. In addition, the RCMP collected information in relation to individuals who were identified as owners and/or drivers of vehicles who did not want to leave the assembly area, then disclosed the relevant information to financial entities pursuant to the Order. We found no indication that personal information collected for this purpose was used or disclosed for any other purpose.

39. Based on the information we received from the RCMP, it took steps to share relevant and timely information with financial entities and to ensure that the information shared did not exceed the parameters of what was necessary for financial entities to meet their obligations under the Order (i.e., to determine whether individuals were designated persons). The "disclosure letter" the RCMP provided to financial entities was precise, clear, and supported the steps taken by the RCMP to disclose relevant and consistent categories of information to assist financial entities in making a determination.

40. Further, the RCMP took steps to assess and identify those financial entities to which disclosures should be made, and as noted above, accompanied those disclosures with a letter which provided the rationale and legislative authority for sharing the information, and a caveat for the use and safeguarding of the information. Based on our engagement with the RCMP, the RCMP's actions in fulfilling its legal obligations under the Order were compliant with sections 7 and 8 of the *Privacy Act*, which place limits on the use and disclosure of personal information without an individual's consent.

41. With respect to the RCMP's transmission of information to financial entities, we noted that the RCMP disclosed information by unencrypted email, which was, according to the RCMP, in line with its Departmental Security Policy requirements for "Protected A" information. While Government of Canada institutions are responsible for stipulating and applying the required level of security for their information and assets, we question whether the information disclosures made to financial entities may not have been classified to reflect the sensitivity of the information and degree of injury that could reasonably be expected if compromised.

42. We accept that tombstone data (e.g., address, date of birth) may generally be classified as Protected A; however, when this information is combined with other categories of personal information (in this case, information gleaned from RCMP database checks and open source information), along with the fact that the disclosures identified individuals determined to be "designated persons" pursuant to the Order, we would expect that consideration be given to ensuring that the information is appropriately classified to the degree of injury caused by unauthorized disclosure.[22] In our view, compromise of the information could have resulted in financial impacts and reputational harm to the individuals in question.

43. While it is not the role of our Office to review the classification of an institution's information or assets, we note that it is the classification of the information that determines, in part, the security requirements and safeguards for that information,

[22] For example, "Protected B" applies to information when unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation. Source: Treasury Board Secretariat Directive on Security Management – Appendix J: Standard on Security Categorization

including the appropriate transmission requirements. In this case, the RCMP transmitted inherently sensitive information to financial entities by unencrypted email.

44. While federal departments and agencies have the capability to send and receive emails through encrypted channels, we acknowledge that information sharing between public and private sector entities does not, in most cases, benefit from the same level of information security[23]. Nevertheless, given the nature of the personal information disclosed, we would expect that consideration be given to the manner in which the information is shared and to ensure that institutions can implement the appropriate technological safeguards to protect the information.

45. Our engagement found that the RCMP retained the personal information collected during the time the *Emergencies Act* was in force in accordance with its retention policies, thus meeting its obligations under subsection 6(1) of the *Privacy Act*, which requires government institutions to retain personal information that has been used for an administrative purpose for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

46. As required by sections 10 and 11 of the *Privacy Act*, the personal information collected by the RCMP as a result of the invocation of the *Emergencies Act* is described in the PIB entitled RCMP PPU 005. According to the RCMP, it has not yet identified a consistent use for the information it received pursuant to section 5 of the Order; therefore, in line with the requirements of the *Privacy Act*, we expect that the RCMP will modify the PIB description to include a statement of any of the uses and purposes of that personal information before the information is used or disclosed.

47. At the conclusion of our engagement, we provided the RCMP with an opportunity to review the observations noted by our Office. The RCMP indicated that it accepts the recommendations we made, which included to: (i) ensure that information is protected according to its sensitivities; and (ii) update the relevant RCMP PIB descriptions to ensure that all consistent uses are listed.

Engagement with FINTRAC

Temporary powers granted under the Order

48. FINTRAC's mandate is to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control. FINTRAC reported that its mandate was not expanded as a result of the temporary emergency measures granted under the Order. The emergency measures created registration and reporting obligations for certain entities not subject to the PCMLTFA[24] prior to the Order being made, including those referred to in paragraphs 3(k) and 3(l) of the Order (i.e., crowd funding platforms,

[23] According to the RCMP, certain financial entities provided secure portals to allow the RCMP to upload information securely; however this was not the case for all entities.

[24] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17)

payment service providers and certain cryptocurrency platforms). These entities were required to register with FINTRAC if they determined that they were in possession of property owned, held or controlled by a designated person, and to report certain financial transactions to FINTRAC.

49. The Order also authorized FINTRAC to disclose information to any financial entity set out in section 3 of the Order when it was satisfied that the disclosure would contribute to the application of the Order (section 6).

Scope of personal information received by FINTRAC

50. FINTRAC reported that it did not have an opportunity to formally register any new entities as required by section 4 of the Order; therefore, no new entities reported suspicious or other financial transactions by designated persons to FINTRAC during the time the Order was in place. FINTRAC confirmed that any financial transaction reports it received during that time were received under the authority and thresholds of the PCMLTFA from existing entities.

51. In addition, FINTRAC reported that, as no new entities registered with FINTRAC as a result of the Order, no amendments or modifications were required or made to its existing PIBs to describe any collection, uses or disclosures of personal information by these entities.

Scope of personal information disclosed by FINTRAC

52. FINTRAC reported that all disclosures of tactical financial intelligence which were made by FINTRAC to police, law enforcement and national security agencies during the time the Order was in place were made solely under the authorities set out in the PCMLTFA. This means that FINTRAC met one of the legal thresholds for disclosure, which requires FINTRAC to determine that its intelligence would be relevant to investigating or prosecuting a money laundering offence, or a terrorist activity financing offence, or would be relevant to threats to the security of Canada.

53. FINTRAC reported to our Office that it did not track information about “designated persons” as defined in the Order, nor did it confirm or take into account whether an individual or entity named in a tactical financial intelligence disclosure was a “designated person”. We note that FINTRAC also confirmed in its testimony to the DEDC that it did not receive a list of "designated persons.[25]

Engagement Findings - FINTRAC

54. Based on our engagement with FINTRAC, the information exchanges that occurred during the time the Order was in place were based on the authorities set out in the PCMLTFA. As such, any reporting FINTRAC received from existing entities and any financial disclosures it made were based on the existing thresholds under the PCMLTFA.

[25] See evidence provided by Mr. Barry MacKillop, Deputy Director, Intelligence, FINTRAC (May 3, 2022). Source: DEDC Committee Meeting: Evidence Tuesday, May 3, 2022.

55. Given that this was an informal engagement, our Office did not pursue lines of enquiry beyond the stated objectives for the engagement, and specifically, we did not review the activities of FINTRAC in relation to any collection and/or disclosure of personal information pursuant to its legislative mandate and authorities under the PCMLTFA.

56. FINTRAC was provided with an opportunity to review and comment on our engagement findings and indicated that it had no additional comments with respect to our understanding of its role as a result of the invocation of the *Emergencies Act*.

Other

57. We noted that amendments to the PCMLTFA Regulations and PCMLTFA Administrative Monetary Penalties Regulations came into force in April 2022.[26] The changes mean that crowdfunding platforms and certain payment providers are now covered as money services businesses ("MSBs") or foreign money services business ("FMSBs") under the PCMLTFA and have the following obligations: (i) to register with FINTRAC; (ii) to develop and maintain a compliance program; (iii) to carry out "know your client" requirements, including verifying the identity of persons and entities for certain activities and transactions; (iv) to keep certain records, including records related to transactions and client identification; and (v) to report certain transactions to FINTRAC.

Engagement with CSIS

Temporary Powers Granted under the Order

58. Section 5 of the Order required those financial entities set out in section 3 of the Order to disclose, without delay, certain information to CSIS or the RCMP, including: (a) the existence of property in their possession or control that they have reason to believe is owned, held or controlled by or on behalf of a designated person; and (b) any information about a transaction or proposed transaction in respect of property referred to in paragraph (a).

59. The Order also authorized CSIS to disclose information to any financial entity listed in section 3 of the Order if satisfied that the disclosure would contribute to the application of the Order.

Engagement Findings - CSIS

60. We confirmed that CSIS did not request any specific measures under the *Emergencies Act*, nor did it benefit from any new authorities under the *Emergencies Act*. We also confirmed that CSIS did not receive any information from any of the financial entities set out in section 3 of the Order pursuant to the Regulations or the Order itself. We have no

[26] Regulations Amending the PCMLTFA Regulations and PCMLTFA Administrative Monetary Penalties Regulations (SOR/2022-76)

concerns with respect to CSIS' activities from a privacy standpoint in the context of this engagement.

61. We note that CSIS' authority to collect information and intelligence on threats to the security of Canada rests primarily in section 12 of the *Canadian Security Intelligence Service Act* ("CSIS Act").[27] CSIS confirmed in its Institutional Report prepared for the POEC that it has information sharing protocols in place with the RCMP and other law enforcement agencies. Throughout the period of blockades and protests, CSIS and the RCMP worked under these protocols to share relevant intelligence on potential threats to the security of Canada.[28]

62. Given that this was an informal engagement, our Office did not pursue lines of enquiry beyond the stated objectives for this engagement, and specifically, we did not review the activities of CSIS in relation to any collection and/or disclosure of personal pursuant to its legislative mandate and authorities under the CSIS Act, or other information sharing protocols.

Observations

63. This was an informal engagement to better understand how the RCMP, CSIS and FINTRAC operationalized the temporary powers and authorities granted as a result of the invocation of the *Emergencies Act*. Our general objective was to assess against the *Privacy Act* these temporary powers – and specifically the authority to share information – against the requirements of the *Privacy Act*.

64. We note that there is a concurrent and ongoing study by the DEDC to review the exercise of powers and the performance of duties and functions pursuant to the declaration of emergency. Our Office was invited to submit a brief for the DEDC's consideration by January 23, 2023.[29] The DEDC is to present its final report in the House of Commons and the Senate no later than March 31, 2023.

65. In addition, the POEC examined and assessed the basis for the Government's decision to declare a public order emergency, the circumstances that led to the declaration, and the appropriateness and effectiveness of the measures selected by the Government to deal with the then-existing situation. The POEC also conducted a policy review of the legislative and regulatory framework involved, including whether any amendments to the *Emergencies Act* are necessary. The POEC's Commissioner, the Honourable Paul Rouleau, released the *Report of the Public Inquiry into the 2022 Public Order Emergency* on February 17, 2023.[30]

66. In light of these concurrent studies, we note that there may be potential for overlap with the observations from our engagement. Nevertheless, given the importance of this

[27] *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23)
[28] CSIS and Integrated Terrorism Assessment Centre (ITAC) Institutional Report Prepared for the Public Order Emergency Commission
[29] Submission of the Office of the Privacy Commissioner of Canada on Privacy during an Emergency
[30] Report of the Public Inquiry into the 2022 Public Order Emergency

matter, we take this opportunity to share certain observations we made during our engagement with these three institutions.

67. Overall, we found that information exchanges were limited in scope and nature, and reasonable steps were taken to identify relevant, accurate and necessary information to assist financial entities in meeting their obligations under the Order (i.e., to determine whether individuals were designated persons). We also found that reasonable steps were taken to ensure that disclosures made pursuant to the Order did not exceed the parameters of what was necessary for financial entities to meet their obligations under the Order, that there was consideration given to ensure that information was shared with the appropriate entities, and that there were caveats placed on the information disclosed. Information sharing was also time-limited and ceased when the temporary powers were revoked.

68. Given the privacy implications and the potential for these temporary measures to impact on Canadians' privacy rights, we considered the use of these powers in light of the general principles of necessity and proportionality.[31] Overall, we found that the sharing of personal information was proportionate to the needs arising from the unprecedented situation and the legal obligations deriving from the declaration of a public order emergency under the *Emergencies Act*.

69. Nevertheless, the privacy impacts of temporary measures such as those granted pursuant to the *Emergencies Act* need to have formal consideration within the framework of the emergency measures in order to ensure accountability in the protection of Canadians' privacy. On this point, we share the following observations.

70. First, the Order provided the authority to share inherently sensitive personal information. The mere fact that the information disclosures related to individuals identified as "designated persons" and potentially subject to financial measures, combined with other personal identifying information and financial information (which is often reputationally sensitive), requires clear and appropriate processes and procedures to handle information privacy and security risks. This is particularly important where the personal information, if compromised, could cause significant reputational or other harms to the individuals affected.

71. We noted that the Order did not specify the conditions or requirements for information sharing, including the specific types and scope of personal information that should be shared. As such, the information received by the RCMP pursuant to section 5 of the Order varied in scope and detail. This can be problematic from an accountability and transparency perspective. Limitations on information sharing need to be defined to ensure that: (i) only the minimum amount of personal information is disclosed for the stated purpose, (ii) recordkeeping practices are consistent and as complete as possible, and (iii) the integrity and reliability of the information to be used for authorized purposes.

72. We also noted that the Order did not prescribe how information was to be shared with financial entities. According to the RCMP, it acted as a conduit for provincial and

[31] While not legal requirements under the *Privacy Act*, government institutions should ensure that measures taken are necessary and proportionate, even in exceptional circumstances.

territorial institutions in order to streamline communications and the sharing of information with financial entities. While this approach may have increased efficiencies and reduced redundancy during the crisis (as noted by the RCMP), it also meant that information was transmitted and handled by a third party, which increases the privacy and security risks to the information. Information sharing practices need to be defined with clear controls and limits, and the expectations for information sharing must be understood by institutions so that they can ensure that the information-sharing activity is compliant with privacy laws, and that measures are implemented to mitigate potential privacy risks.

73. In addition, the Order did not contain any explicit safeguard requirements to ensure that appropriate procedures were established and implemented to protect the personal information, particularly given that the Order authorized information sharing between the Government and private sector entities. Security safeguards protect information against loss or theft, as well as unauthorized access, use, disclosure, copying or modification, and include: (i) physical measures (e.g., locked filing cabinets); (ii) organizational measures (e.g., limiting access on a "need-to-know" basis); and (iii) technological measures (e.g., the use of passwords and encryption).

74. Lastly, the RCMP indicated that it did not have authority to provide oversight over the actions that the entities took in relation to designated persons and the freezing of assets. In this light, we noted that the Order did not prescribe any formal oversight or reporting structure to capture the exchanges of information. This also makes it difficult to hold institutions accountable for the information they are sharing, or for the Government of Canada to assess the effectiveness of the measures and demonstrate transparency to Canadians.

Conclusions

75. Our Office has previously noted that privacy protection is more than just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental human rights and democratic values, even in exceptional circumstances. During any crisis, privacy laws still apply, but they should not pose a barrier to appropriate information sharing.[32]

76. For example, during the COVID-19 health crisis, our Office released a "Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19".[33] This framework highlights that new laws and measures implemented relating to the crisis should also provide specific provisions for oversight and accountability, as institutional safeguards become more, not less, important during times of crisis.

77. The authority to share sensitive personal information – particularly in the midst of a crisis when extraordinary measures are being implemented – needs to be supported by clear processes and guidance such that government institutions and financial entities

[32] The OPC's Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 (April 2020)
[33] Ibid.

are aware of their obligations at the outset, and to ensure transparency and accountability to Canadians for the protection of personal information.

78. In our view, this includes provisions and/or guidance to govern the implementation of the temporary measures, and specifically, the sharing of personal information, that at a minimum: (i) define the specific elements of personal information to be shared, (ii) define the specific purposes for the sharing, (iii) limit secondary uses and onward disclosures, and (iv) include provisions for a commensurately high level of safeguards to protect the information. Provisions framed in this manner will provide clarity and guidance to institutions and assist institutions in meeting their obligations under the temporary measures and privacy laws.

79. As noted above, new laws and measures specific to the crisis – and in particular those that authorize the sharing of personal information – require provisions for oversight and/or a reporting mechanism to track the exchanges of information. This will ensure that there are clear and reliable records of what is being disclosed, to whom, and for what purposes. Further, it will aid institutions in ensuring that they are meeting their legal obligations as required by the temporary measures, but also ensuring compliance with the *Privacy Act* and PIPEDA.

80. The invocation of the *Emergencies Act* in early 2022 was the first time powers under that legislation had ever been utilized. This was in reaction to extraordinary events, both in Ottawa, elsewhere in Canada and similar events abroad. We were pleased to engage on this important matter with the RCMP, FINTRAC and CSIS, and we would like to express our appreciation for their open and collaborative engagement with our Office. We hope that the observations we made as a result of this engagement provide helpful insight to the Government of Canada regarding the sharing of information, and also the provisions we would expect to see in the law for privacy oversight and accountability, in times of crises.

Vaccine mandates for domestic travel

Complaints under the *Privacy Act*

May 29, 2023

Description

From November 2021 to June 2022, air and rail passengers in Canada were required, by Ministerial Orders issued by the Minister of Transport, to be fully vaccinated against COVID-19. We investigated whether the related collection, use and disclosure of personal information by Transport Canada, VIA Rail and CATSA was compliant with the Privacy Act (the Act). Additionally, we examined the necessity and proportionality of the measures considering the circumstances under which they were established.

Takeaways

- Transport Canada, VIA Rail and CATSA had the authority to collect personal information, including vaccination status, to administer the Ministerial orders, as this collection was directly related to their programs or activities with respect to transportation safety.
- Though the principle of necessity and proportionality is not currently a requirement of the Privacy Act, limiting the collection of personal information to what is demonstrably necessary is a requirement of the TBS Directive on Privacy Practices. We identified weaknesses in Transport Canada's assessment and documentation, but found that the collections were necessary, effective, and proportional in the circumstances.
- To determine if a collection is necessary and proportional, the objective should be clearly and narrowly defined, to avoid overbroad interpretation.
- Institutions should clearly assess and document their consideration of potentially less privacy invasive alternatives, such as, in this case, COVID-19 testing as an alternative to vaccination status.

Report of findings

Table of contents

Overview

From November 30th, 2021 to June 20th, 2022, all air and rail passengers traveling within or outbound from Canada were required to be fully vaccinated, per a series of Orders issued under the authority of the Minister of Transport. As a result, airlines, passenger rail services, the Canadian Air Transport Security Authority ("CATSA"), and Transport Canada collected information related to travellers' vaccination status during this period.

We received 18 complaints under the *Privacy Act* (the "Act") which alleged, to varying degrees of specificity, that the mandatory collection of medical information prior to boarding a train or plane was: (i) an unlawful violation of the complainants' privacy and (ii) an unreasonable, unnecessary and unjustified limitation of their freedom of mobility. Some complainants specifically cited the diminishing efficacy of COVID-19 vaccines and the availability of alternatives, such as testing and natural immunity. In response, our Office investigated the federal institutions responsible for implementing and overseeing the passenger vaccine mandates (i.e., CATSA, VIA Rail and Transport Canada) for their compliance with the *Privacy Act* and with key privacy principles. Our investigation did not assess whether the vaccination requirements were an unjustified limitation on individuals' freedom of mobility guaranteed by the *Canadian Charter of Rights and Freedoms*.

Ultimately, we found that the personal information was collected, used and disclosed to administer the Orders issued pursuant to the *Aeronautics Act* and the *Railway Safety Act*. We therefore determined the complaints to be **not well-founded** as: (i) the collections by CATSA, VIA Rail and Transport Canada were directly related to institutional operating programs or activities, (ii) the subsequent uses of the information were for the purposes for which the information was collected or a consistent use with that purpose, and (iii) related disclosures were authorized under Acts of Parliament.

Our Office also considered whether the collection of personal information under the Orders was necessary and proportional. 'Necessity' is not a legal requirement under the Act, which requires a lesser threshold of "relates directly to", but it is a key privacy principle embedded in the privacy laws of many jurisdictions, including several Canadian provinces. In April of 2020, our Office issued a *Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19* and shared it with government institutions in an effort to outline key privacy principles, including necessity and proportionality, that should be considered when imposing COVID-19 response measures that have an impact on the privacy of Canadians. In May of 2021, Federal, Provincial and Territorial Privacy Commissioners recommended in a Joint Statement that governments and businesses consider the principle of necessity, effectiveness and proportionality in relation to the establishment of vaccine mandates. Several complainants specifically requested that our Office examine Transport Canada's consideration of this principle in the issuance of the Orders.

We found that overall, the collections of personal information by VIA Rail, CATSA and Transport Canada under the Orders were necessary and proportional. However, we identified concerns

with the broad scope of the Orders' stated objective of transportation safety, and with the related risk that inappropriate or irrelevant factors could be considered when evaluating the Orders. We also identified gaps in Transport Canada's assessment of potentially less-privacy invasive alternatives.

As a result, we recommended that if Transport Canada considers similar mandatory collections for the purpose of transportation safety in the future, it: (i) more clearly define the objectives of the measures and the scope of those objectives, and (ii) examine and document its assessment of potentially less privacy invasive alternatives. Transport Canada accepted our recommendations.

Background

1. On August 13th, 2021, the Government of Canada announced its intent to introduce COVID-19 vaccination requirements for air and rail passengers. Subsequently, on October 6th, 2021, the Government of Canada announced that, effective October 30th, 2021, travellers departing from Canadian airports and travellers on VIA Rail and Rocky Mountaineer trains would be required to either (i) be fully vaccinated or (ii) to show a valid COVID-19 molecular test from the past 72 hours in order to travel. They also stated that individuals who had not begun the vaccination process would risk not qualifying for travel as of November 30th, 2021.
2. On October 29th, 2021, Transport Canada issued two related Orders[1] under the *Aeronautics Act* and the *Railway Safety Act*. According to their preambles, the Order issued under the *Aeronautics Act* was "required to deal with a significant risk, direct or indirect, to aviation safety or the safety of the public", while the Order issued under the *Railway Safety Act* was considered to be "necessary in the interest of safe railway operations", with "safe railway operations" encompassing the safety of persons and property transported by railways as well as the safety of others persons and other property.[2]
3. These Orders, effective October 30th, 2021, prohibited individuals over the age of 12 years and 4 months from:
    - (i) entering a restricted area at an airport if they could not provide a proof of vaccination credential ("PVC") or an acceptable COVID-19 molecular test result to the screening authority, i.e., CATSA; and
    - (ii) boarding an aircraft or railway equipment if they could not provide a PVC or COVID-19 test result to their air or rail carrier, e.g., Air Canada or VIA Rail.

---

[1] The Minister of Transport issued *Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 43*; The Director General of Rail Safety, with the authorization of the Minister of Transport, issued *Order pursuant to Section 32.01 of the Railway Safety Act (MO 21-08) Vaccination Mandate for Passengers*.
[2] Definition of *'safe railway operations'*, *Railway Safety Act*, R.S.C. 1985, c. 32, subsection 4(4).

4. A valid PVC must have included or indicated:

    - the name of the person who received the vaccine;
    - the name of the government or the name of the non-governmental entity that issued the PVC;
    - the brand name or any other information that identifies the vaccine that was administered; and
    - the dates on which the vaccine was administered.

5. A month later, two additional Orders[3] were issued, which, effective November 30th, 2021, removed the option for travellers to present the results of a COVID-19 molecular test to enter a restricted area or to board a plane/train, subject to the exceptions set out in the Orders. Exceptions were notably available for individuals who were not vaccinated due to a medical contraindication or a sincerely held religious belief, individuals who were traveling to receive an essential medical service or treatment, individuals accompanying someone who was under the age of 18 years or who had a disability, and individuals travelling to remote communities only accessible by train.

6. 18 additional orders[4] under the *Aeronautics Act* and 2 additional orders[5] under the *Railway Safety Act* had been issued since November of 2021, with each repealing and replacing the last. The core vaccination requirements of those orders, which will be referred to as the "Air Orders" and the "Rail Orders" respectively, had largely remained unchanged, with air carriers and rail operators being prohibited from allowing a person to board if they could not provide a PVC (exceptions continued to apply).

7. Since December 21st, 2021, the Air Orders no longer required CATSA to verify PVCs prior to allowing entry into a restricted area (e.g., the terminals at an airport).[6]

8. On June 14th, 2022, the Government of Canada had announced that the vaccination requirements for domestic and outbound air and rail travel would be rescinded on June 20th, 2022.

---

[3] The Minister of Transport issued *Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 47*; The Director General of Rail Safety, with the authorization of the Minister of Transport, issued *Order pursuant to Section 32.01 of the Railway Safety Act (MO 21-09) Vaccination Mandate for Passengers – Phase 2.*

[4] The last Order under the *Aeronautics Act* was *Interim Order for Civil Aviation Respecting Requirements Related to Vaccination Due to COVID-19, No. 3*, which was issued on June 14th, 2022.

[5] The last Order under the *Railway Safety Act* was *Order pursuant to Section 32.01 of the Railway Safety Act (MO 21-09.2) Vaccination Mandate for Passengers*, which was issued on February 28th, 2022.

[6] *Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 49*, sections 17.8 and 17.16.

9. The last Air Order vaccination requirement ceased to have effect on June 20th, 2022, and, through an order[7] issued on June 17th, 2022, the Rail Order's vaccination requirement was repealed effective June 20th, 2022 as well.

Jurisdiction

10. Most complainants asserted that restricting domestic air and rail travel to vaccinated individuals was a contravention of their mobility rights guaranteed by section 6 of the *Canadian Charter of Rights and Freedoms* ("the Charter"), and that therefore the Air and Rail Orders were unlawful. However, mobility rights are outside of the scope of our Office's jurisdiction under the *Privacy Act* and thus outside the scope of this report's analysis.[8]

11. Concerns were also raised with respect to:

    - the PVC verification applications developed and issued by the provinces and territories;
    - the vaccine mandates imposed by provinces and territories;
    - inconsistencies between vaccine mandates for federally regulated sectors, such as air and rail transportation, and provincially regulated sectors, such as certain forms of road transportation (e.g., coach bus services).

    Given that our Office does not have jurisdiction over the practices of provincial and territorial governments, our analysis is limited to assessing the compliance of federal institutions with the *Privacy Act*.

Analysis

Issue 1: Was the vaccination information collected by CATSA and VIA Rail directly related to their operating programs or activities, as required by the Act?

12. The complainants allege that CATSA, VIA Rail and other transportation providers lacked the authority to collect sensitive medical information, such as the immunization status of passengers.

13. Section 4 of the Act states that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution. Programs or activities of an institution are typically established or otherwise authorized by an Act of Parliament. Section 4 does not require a collection to be

---

[7] *Order pursuant to Section 32.01 of the Railway Safety Act (MO 22-02) Order Ending Vaccination Mandates for Passengers and Employees*, Transport Canada, last modified June 17th, 2022.
[8] Note: The constitutionality of these orders was recently confirmed in *Syndicat des métallos, section locale 2008 c. Procureur général du Canada*, 2022 QCCS 2455.

"necessary", just that there be "a direct, immediate relationship with no intermediary between the information collected and the operating programs or activities of the government."[9]

14. As described in further detail below, we determined that both VIA Rail and CATSA's collections of travellers' vaccination information were directly related to their operating programs given that both were required to collect the information for safety purposes under the Rail Orders and Air Orders. The Minister of Transport, in turn, was authorized under the *Railway Safety Act* and the *Aeronautics Act* to issue such Orders for the safety of the public, which includes the safety of passengers.

15. The Air Orders were issued pursuant to section 6.41 of the *Aeronautics Act*, which allows the Minister of Transport to make an interim order to deal with a significant risk or an immediate threat to aviation safety, aviation security or the safety of the public. Such an order may only contain provisions that may be made in a regulation of the *Aeronautics Act*, and according to sections 4.71 and 4.9 of that Act, regulations may be made respecting:

    - the safety of the public, passengers, crew members, aircraft and aerodromes and other aviation facilities;
    - restricted areas in aircraft or at aerodromes or other aviation facilities, including regulations respecting access to them;
    - the screening of persons entering or inside an aircraft or an aerodrome or other aviation facility; and
    - the conditions under which persons may be transported by aircraft.

16. The Rail Orders were issued pursuant to section 32.01 of the *Railway Safety Act*, which allows the Minister of Transport, should they consider it necessary in the interests of safe railway operations, to order a company to stop an activity that might constitute a threat to safe railway operations. Subsection 4(4) of the *Railway Safety Act* stipulates that, "in determining […] whether railway operations are safe railway operations, or whether an act or thing constitutes a threat to safe railway operations or enhances the safety of railway operations, regard shall be had not only to the safety of persons and property transported by railways, but also to the safety of other persons and other property."

17. In support of the Orders' measures, Transport Canada submitted evidence from the Public Health Agency of Canada ("PHAC"), demonstrating that in the fall of 2021, when the mandate was put in place:

    - COVID was known to be more transmissible in indoor crowded spaces;

[9] Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) v. Canada (Attorney General), 2016 FC 1289 at para. 141, affirmed 2019 FCA 212.

- The Delta variant of COVID-19, which at the time was becoming the dominant variant, was more transmissible than previous variants and risked leading to more hospitalizations and deaths in the midst of what was then Canada's fourth wave of the pandemic;
- The approved COVID-19 vaccines were very effective at preventing severe illness, hospitalization and death; and
- The approved COVID-19 vaccines appeared to be somewhat effective at preventing outbreaks and the transmission of the virus, though further research was required to determine their level of effectiveness against the Delta variant.

Transport Canada also provided evidence, from PHAC's COVID-19 testing of travellers entering Canada between July and October of 2021, demonstrating that unvaccinated travellers were at least five times more likely than vaccinated travellers to test positive for COVID-19.

18. CATSA and VIA Rail were subject to the Air Orders and the Rail Orders respectively. As screening authorities under the Air Orders, CATSA officers were required to request that individuals provide a PVC at screening checkpoints.[10] As a company listed in Appendix A of the Rail Orders, VIA Rail was required to follow the procedures, including the information collection procedures, set out in the Rail Orders.[11] Accordingly, we consider CATSA and VIA Rail's compliance with the Orders to be valid institutional operating programs/activities.

19. Additionally, part of CATSA's primary operating program/activity is to screen persons who access aircraft or the restricted areas of airports to ensure transportation security,[12] while VIA Rail, as a railway company, is required under paragraph 3(c) of the *Railway Safety Act* "…to demonstrate, by using safety management systems and other means at their disposal, that they continuously manage risks related to safety matters".[13] The Air Orders and the Rail Orders state their objective as being aviation safety[14] and safe railway operations[15] respectively, and thus are related to CATSA's and VIA Rail's other, core operating programs/activities as well.

---

[10] *Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 43*, last modified October 29th, 2021, section 17.6.
[11] *Order pursuant to Section 32.01 of the Railway Safety Act (MO 21-08) Vaccination Mandate for Passengers*, last modified October 29th, 2021, Preamble.
[12] *Canadian Air Transport Security Authority Act*, S.C. 2002, c. 9, s. 2, section 6.
[13] *Railway Safety Act*, R.S.C. 1985, c. 32, subsection 3(c).
[14] *Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 43*, last modified October 29th, 2021, Preamble: "Whereas the annexed Interim Order Respecting Certain Requirements for Civil Aviation Due to COVID-19, No. 43 is required to deal with a significant risk, direct or indirect, to aviation safety or the safety of the public;".
[15] *Order pursuant to Section 32.01 of the Railway Safety Act (MO 21-08) Vaccination Mandate for Passengers*, last modified October 29th, 2021, Preamble: "…I, Michael DeJong, Director General, Rail Safety, considers it necessary in the interest of safe railway operations to make this order under sections

All personal information collected was 'directly related'

20. We also considered whether all the information collected by CATSA and VIA Rail was directly related to the administration of the Orders and its measures.

CATSA

21. Overall, CATSA's collection of personal information was limited to that which was required to enforce the Air Orders. Information would only be recorded and retained in instances where a passenger failed to provide a valid PVC.

22. CATSA employees conducted a visual inspection of passengers' PVCs prior to their entry into the restricted area of an airport. CATSA was required to verify the PVC of at least 8% of passengers, or to verify PVCs on a "continuously busy basis" of all eligible passengers when passenger volumes allowed, as prescribed by the Minister of Transport in a supplementary bulletin and in accordance with section 17.8 of the Air Orders. PVCs, which are referred to as "evidence of COVID-19 vaccination" in the Air Orders, contained the vaccinated individual's name, the PVC's issuer, the vaccine that was administered and the date it was administered.

23. CATSA never employed the use of verification applications to scan or authenticate PVCs with QR codes. Officers instead performed a visual verification of the PVC to ensure that it appeared legitimate, that it contained the necessary information, and that the name on the PVC matched the name on the passenger's boarding pass. The information contained within a valid PVC was never recorded or retained by CATSA.

24. If the passenger did not provide a valid PVC, they were denied entry into the restricted area. In such instances, CATSA screening officers notified a supervisor, who would then fill out a 'Vaccination Check Failure Form' recording the traveller's name and flight number, the date and time, the airport and screening checkpoint, and the fact that they were denied entry for failing to provide a valid PVC. As we will discuss in the following subsection, this information was collected so that CATSA could notify both the traveller's air carrier and the Minister of Transport of the denied entry, as prescribed by the Air Orders.

25. Based on the facts outlined above, we find that the information collected by CATSA was directly related to the administration of the Air Orders, a valid operating program/activity of the institution.

VIA Rail

26. For their part, VIA Rail collected a limited amount of personal information, and only retained or recorded information where a request for an exception was made or in

---

32.01 and 36 of the *Railway Safety Act* requiring the companies listed in Appendix A to follow the procedures set out below."

response to specific incidents of passenger non-compliance (e.g., failure to provide a valid PVC).

27. VIA Rail station agents, senior service attendants and service managers were responsible for verifying that passengers (i) above the age of 12 years and 4 months, (ii) who had not been granted an exception and (iii) who were accessing a VIA Rail lounge or boarding a VIA Rail train, provided a PVC.[16] The PVC could have been paper or digital, and for passengers originating outside of Canada, it could have taken the form of an ArriveCAN receipt with the individual's immunization status denoted.

28. According to VIA Rail's '*Mandatory COVID-19 Vaccination for Passengers*' Policy, VIA Rail employees verified the identification of the passenger and confirmed that the name on the train ticket matched the name on the PVC. The employee was also required to visually confirm on the PVC that the passenger was fully vaccinated and that this status was obtained at least 14 days prior to the departure date. PVCs with a QR code were verified using the applicable PVC verification application.[17] VIA Rail confirmed that no additional personal information was collected from PVCs with a QR code as compared to PVCs without a QR code.

29. While the passenger's PVC, identification and ticket were visually inspected and verified by VIA Rail employees, no personal information was retained during this process, except when the passenger had made an exception request or failed to provide a valid PVC. The Rail Orders required such events to be documented, and that the number/frequency of documented events be reported to the Minister of Transport. This information would also occasionally be used by VIA Rail to respond to complaints or claims arising from passengers who were denied boarding.

30. In light of these facts, we consider the information collected by VIA Rail to be directly related to the administration of the Rail Orders, which we consider to be a valid institutional operating program/activity.

31. VIA Rail and CATSA's collection of travellers' vaccination status and other prescribed information was therefore compliant with section 4 of the Act, and this element of the complaints is **not well-founded**.

32. The Air Orders expired and Rail Orders were repealed on June 20th, 2022. In their news release announcing the end of the vaccine mandates, the government stated that "As the COVID-19 pandemic has evolved, so too have public health measures and advice, which includes vaccination requirements that were always meant to be a temporary measure." The government concluded by stating that it "will not hesitate to make adjustments based on the latest public health advice and science to keep Canadians safe", which "could include […] the reimposition of public service and transport vaccination mandates." In this context, we note that should similar requirements be

[16] See paragraph 4 for information that must be included in a PVC.
[17] These applications are issued and operated by Provincial authorities. Examples of such applications include VaxiCode Verif (Québec) and Verify Ontario. All Provincial verifier applications were developed using the SMART Health Card Framework, and rely on public key infrastructure.

reintroduced, continuous or periodic reviews are critical to ensuring that any future collections of personal information meet the threshold of being related directly to operating programs or activities – in this case, railway and aviation safety.

Issue 2: Were uses or disclosures of personal information, and the centralized collection by Transport Canada, compliant with sections 4, 7 and 8 of the Act?

33. Several complainants expressed concern that personal information collected pursuant to the vaccine mandates could be used for surveillance, location tracking and other secondary purposes. As detailed below, we found no indications that personal information was used or disclosed by CATSA or VIA Rail, or collected and used by Transport Canada, for purposes other than enforcing and supervising the enforcement of the Orders, in compliance with sections 4, 7 and 8 of the Act.

Use and Disclosure by VIA Rail and CATSA

34. With respect to the use of information by CATSA and VIA Rail, section 7 of the Act states that personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

35. The two institutions confirmed that they did not use any of the personal information collected for any purpose other than to (i) determine eligibility for exceptions in accordance with the Orders (e.g., on the basis of religious grounds or for urgent travel), (ii) to allow or deny entry/boarding, or (iii) to respond to related complaints about these decisions. The first two uses are directly provided for in the relevant Orders, while the third, in our view, constitutes a 'consistent use' with the original purpose of collection as it is so directly connected that an individual would reasonably expect it.[18] Therefore, the uses described above are all compliant with section 7 of the Act.

36. We also examined disclosures by VIA Rail and CATSA. Section 8 of the Act sets limits on permissible disclosures of personal information without consent of the individual. One of the permissible disclosures, under paragraph 8(2)(b) of the Act, is a disclosure made for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure.

[18] The jurisprudence on "consistent use" identifies its threshold requirement as "a sufficiently direct connection between the purpose and proposed use, such that an [individual] would reasonably expect that the information could be used in the manner proposed." (Emphasis added). See *Bernard v. Canada (Attorney General)*, 2014 SCC 13, at paragraph 31.

37. VIA Rail disclosed information to Transport Canada on a weekly basis as required by Section G (formerly Section E) of the Rail Orders, which required the following figures to be submitted:

    - total passenger volumes;
    - the number of exception requests received and accepted for each category of exception;
    - the number of persons denied boarding due to failing to provide an acceptable PVC or due to rejected exception requests; and
    - the number of acceptable and unacceptable COVID-19 test results received.

38. During the investigation, our Office confirmed that VIA Rail's weekly reports did not contain any personal identifiers and that there was no indication of a serious possibility of identification of individuals.

39. If CATSA denied entry to a traveller for failing to provide a valid PVC, CATSA disclosed the individual's personal information to Transport Canada and to the airline with which the traveller was scheduled to fly. These disclosures were expressly required under section 31 of the Air Orders (formerly sections 17.14 and 17.16). The Air Orders specified that the notifications to the Minister of Transport for each incident should include: (i) the person's name and contact information; (ii) the date and number of the person's flight; and (iii) the reason CATSA believed that the evidence was likely to be false or misleading, or the reason why the person was denied entry. The Air Orders also specified that the notifications to the traveller's air carrier should include the individual's name and flight number.

40. To comply with this requirement, CATSA disclosed the information it collected on its 'Vaccination Check Failure Form' (see paragraph 24) to: (i) the airline verbally, and (ii) Transport Canada, through both a phone call and an email notification.[19] From October 30th, 2021 to December 9th, 2021 (i.e., the period during which CATSA was required to verify the PVC of passengers), there were a total of 54 denials of entry related to PVC verifications at pre-board screening checkpoints. We found no indications that extraneous personal information had been included in these notifications by CATSA in the context of these disclosures. Given that the disclosures were authorized by the Air Orders issued under the *Aeronautics Act*, we therefore find that they were compliant with paragraph 8(2)(b) of the Act.[20]

---

[19] Note: The details of the incident, including the specific reason for the individual's denial of entry, were disclosed by CATSA's Security Operations Centre to Transport Canada's Situation Centre. An email notification of the incident was also sent to Transport Canada's Situation Centre, but without the passenger's name.

[20] Subsection 6.41(2) of the *Aeronautics Act* dictates that an interim order under s. 6.41 of the Act, "has effect … as if it were a regulation…". Along similar lines, non-compliance with an order under s. 32.01 of the *Railway Safety Act* is an offence under s. 41 of the Act. Furthermore, both orders are an example of 'delegated' or 'subordinate' legislation, as recently observed by the court in *Syndicat des métallos, section locale 2008 c. Procureur général du Canada*, *supra* note 8 at paragraphs 68-74.

Collection and Use by Transport Canada

41. In addition to collecting the information described above, Transport Canada also collected weekly aggregated reports from airlines subject to the Air Orders (similar to those it collected from VIA Rail), and individual personal information from airlines in cases where they denied a traveller boarding for failure to provide a valid PVC or had reason to believe the traveller had provided evidence that was likely to be false or misleading.

42. As noted above, section 4 of the Act requires that personal information collected be related directly to an operating program or activity of the institution. Given that for air travellers, Transport Canada did collect identifiable personal information, we examined whether this collection and subsequent use was compliant with sections 4 and 7 of the Act.

43. Transport Canada explained that it collected personal information to carry out its mandated activities of supervising and enforcing the requirements of the Air Orders. This activity is consistent with subsection 4.2(1) of the *Aeronautics Act*, which states that the Minister of Transport is responsible for the regulation of aeronautics, the supervision of all matters connected with aeronautics, and the investigation of matters relating to aviation safety.

44. Transport Canada indicated that, in addition to the incident reports from CATSA, it collected the following personal information from airlines (as set out in the Air Orders), in cases where airlines denied boarding for failure to provide a valid PVC or had reason to believe the evidence provided by the traveller was likely to be false or misleading:

    - the person's name and contact information;
    - the date and number of the person's flight;
    - the reason the air carrier believed that the evidence was likely to be false or misleading, or the reason why the person was denied permission to board the aircraft; and
    - whether the individual had been issued a document from the air carrier accepting their exception/accommodation request for that specific flight.

45. Transport Canada demonstrated that it used this information to enforce the Air Orders as per its mandate. Specifically, after being notified of an incident, it reviewed the notification to determine whether an investigation would be warranted. An investigation would normally involve: (i) contacting the air carrier/CATSA and the accused passenger to obtain more information about the alleged incident and (ii) determining the appropriate enforcement actions to be taken, if any. Investigations by Transport Canada have led to enforcement actions which have included, depending on the nature of the

offence, verbal counselling, written warnings and the issuance of fines to individuals.[21] Our investigation found no indications that the personal information collected by Transport Canada has been used for purposes other than supervising and enforcing the Air Orders.

46. In light of the Minister of Transport's statutory responsibilities and the Air Orders' reporting requirements, we find that the personal information collected by Transport Canada was directly related to an operating program/activity of the institution as required by section 4 of the Act: i.e., enforcing and supervising the Air Orders, and that its subsequent use for this purpose was compliant with section 7 of the Act.

47. Based on the above, VIA Rail and CATSA's use and disclosures of personal information, and Transport Canada's collection and use of personal information were thus compliant with sections 4, 7, and 8 of the Act, and we therefore find these elements of the complaints to be **not well-founded**.

Other: Was the information collected necessary and proportional?

48. Multiple complainants raised concerns over the necessity and the proportionality of the measures enacted by the Orders. Certain complainants expressed beliefs, based on a range of online sources, that COVID-19 vaccines were potentially dangerous or ineffective and/or that COVID-19 did not present a serious risk to health that would justify intrusions on their rights and freedoms.

49. Though not a requirement of the Act, necessity and proportionality is a privacy principle that our Office endorses and one that is embedded in the privacy laws of many jurisdictions, including several Canadian provinces. Limiting the collection of personal information to what is demonstrably necessary is also a requirement of Treasury Board Secretariat's *Directive on Privacy Practices.*[22]

50. This principle is all the more important when institutions must respond quickly in times of crisis to implement measures that are intended to promote and protect public health, given the elevated potential for the measures to infringe on individuals' privacy rights. Prior to the issuance of the Air and Rail Orders, our Office published a *Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19* in April of 2020 and the Federal, Provincial and Territorial Privacy Commissioners issued a joint statement in May of 2021 entitled, "*Privacy and COVID-19 Vaccine Passports*". Both of these publications highlighted the importance of considering necessity and

---

[21] As of February 24th, 2022, Transport Canada had indirectly collected the personal information of 2,360 individuals who had been identified as being non-compliant with one or more requirements of the Air Orders, and had issued 18 administrative penalties, averaging $1,444.

[22] *Directive on Privacy Practices*, Treasury Board Secretariat, last modified June 18th, 2020, section 4.2.9: "Heads of government institutions or their delegates are responsible for the following […] Limiting the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities."

proportionality in the development of measures to address COVID-19, and that doing so would not be a barrier to effective public health management. Several complainants specifically asked our Office to consider whether institutions had complied with the public guidance promoted by our Office. Consideration of necessity and proportionality was also a key element of the advice we provided to Transport Canada when it consulted the OPC on the implementation of the vaccine mandates from August to October of 2021. Given its importance, we thus examined the necessity and proportionality of the collection of personal information mandated by the Orders.

51. Transport Canada was cooperative and forthcoming when asked to justify the necessity and proportionality of the mandates. In addition to their detailed responses, Transport Canada provided our Office with the scientific evidence considered prior to the issuance of the Orders.

52. Overall, we found that the collection of information pursuant to the Orders was necessary and proportional. However, as described in greater detail below, we identified concerns with (i) the broad scope of the Orders' objectives, and (ii) the lack of evidence demonstrating that less privacy-invasive alternatives had been considered. Prior to the issuance of this final report, a preliminary report of findings was presented to Transport Canada, to which they responded with further comments and clarifications relating exclusively to our analysis of necessity and proportionality.

53. To guide institutions in considering necessity and proportionality, our Office advocates a four-part test[23] that calls for institutions to ask themselves the following questions when establishing particularly privacy-invasive programs and services:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?
    - Is there a less privacy-intrusive way of achieving the same end?
    - Is the loss of privacy proportional to the need?

Necessity

54. With respect to the first point of the four-part test, necessity, we expect institutions to be able to explain, in detail, how a privacy-intrusive initiative is rationally connected to a defined, pressing and substantial goal, and how the proposed collection or use of personal information will serve to meet the goal. This requires empirical evidence in support of the initiative and should preclude the collection of personal information for speculative or "just in case" scenarios.

---

[23] Expectations: OPC's Guide to the Privacy Impact Assessment Process - *Questions for high-risk programs: necessity, effectiveness, proportionality and minimal intrusiveness*, Office of the Privacy Commissioner of Canada, last modified March 3rd, 2020.

55. While our Office was able to identify a pressing and substantial goal based on Transport Canada's representations, for the reasons detailed below, we found that Transport Canada did not adequately define the scope of 'aviation safety' and 'safe railway operations' as objectives. Consequently, when determining whether to continue applying the vaccine mandate, factors were considered that, in our view, go beyond the reasonable scope of aviation safety and safe railway operations.

56. In its representations to our Office, Transport Canada provided, as noted in paragraph 17, evidence that COVID-19 presented a serious risk to the health of individuals, and stated the following:

    "The primary mission of Transport Canada's Rail and Air Orders is to ensure the safety and security of the transportation system and its operations. Recognizing that people travel for a range of essential and non-essential purposes and that transportation is an essential service, [Transport Canada]'s approach to the vaccination mandate was designed to meet multiple objectives, including but not limited to: safety for the transportation system as a whole; allowing for essential domestic and international travel; transportation of essential goods without disruption to supply chains; keeping exceptions to a minimum while allowing for accommodations for residents of remote communities and those travelling for specified essential or urgent reasons, such as to receive medical care or to respond to emergencies; being feasible for operators to implement while respecting privacy and other applicable legislation; and moving incrementally toward greater compatibility between the international and domestic travel regimes."

57. While the Ministerial Orders pursued multiple objectives, such as enabling essential travel and striving for operational feasibility, their primary goal of ensuring the safety and security of the transportation system was loosely defined.

58. Transport Canada initially told OPC that "In considering any adjustments to the Orders, various public health factors are considered, including, but not limited to:

    i. "Epidemiologic trajectory and modelling (i.e. caseloads, hospitalizations and severe illness trends);

    ii. Vaccine science (i.e. its effectiveness over time; if dosing regimen (e.g., booster doses) is still appropriate; and protection from infection and severity of illness);

    iii. Vaccine coverage to support broader societal protection; and

    iv. Impacts and prevalence of variants of concern or new variants."

    In our view the first and fourth factors above are linked to 'transportation safety' regardless of how broadly the objective is scoped, as they speak to whether COVID-19 remained a sufficient risk to the health of travellers and to the health of the transportation workers to warrant protective measures. The second factor above is also linked to transportation safety, as it references both protection against transmission (which reduces the risk a vaccinated individual poses to others), and protection against

severe disease (which reduces the risks posed to the vaccinated individual). Finally, the third factor is not clearly linked to transportation safety.

59. Based on these factors, we initially inferred that the scope of Transport Canada's goal of 'transportation safety' included:

    a) reduce the risk the vaccinated individual posed to other travellers and to transportation workers (e.g., reducing likelihood individual will transmit COVID-19 to others);

    b) reduce the **risks posed to the vaccinated individual** (e.g., reducing likelihood individual will contract COVID-19 or suffer severe illness as a result of COVID-19); and

    c) reduce the **risks to society as a whole** (e.g., increasing vaccination coverage across Canada).

60. Objective c) (i.e., reducing the risks to society as a whole by increasing vaccine coverage) lacked a direct connection to transportation safety, the primary and overarching goal of the Ministerial Orders. In response to our preliminary report, Transport Canada indicated that the public health factors in paragraph 58 above were those that PHAC considered in its advice to government departments, and which Transport Canada subsequently considered through a transportation safety and security lens. It indicated that reducing the risks to society as a whole "was a factor that PHAC provided for consideration" but that it should not be inferred that this specific factor was in the scope of Transport Canada's goal.

61. However, the news release in August 2021 which announced the government's intent to require vaccination for employees of the federal public service, federally regulated air, rail, and marine transportation sectors, and domestic travellers noted that increasing the vaccination coverage was an intended consequence:[24]

    "These measures will contribute to reaching the overall levels of vaccination Canada needs to sustain a resilient economic recovery in the face of more transmissible and dangerous COVID-19 variants of concern. More than 71% of eligible people in Canada are fully vaccinated, and more than 82% have had their first shot. However, more than 6 million eligible people in Canada are still unvaccinated. We are urging all of you to get out there and get vaccinated now. Doing so will help keep our communities safe."

62. That aside, we find that objectives a) and b) can reasonably be considered within the scope of transportation safety, and the pressing nature of these goals were demonstrated due to the health risks posed by COVID-19.[25] Accordingly, the test of

[24] Furthermore, the news release announcing the end of the measures implied that the suspension of the vaccination requirements was a result of "a successful vaccination campaign."

[25] We note that, while the risk of serious illness and death from COVID-19 has diminished since the beginning of the pandemic, it continued to present a significant health risk to individuals during the period of the domestic travel vaccine mandates, as evidenced by hospitalizations and deaths throughout 2022. See *COVID-19 epidemiology update*.

necessity was met, as the Orders were rationally connected to the pressing and substantial goal of protecting individuals from the risk that they might contract or transmit COVID-19 while traveling, or that they might suffer severe illness due to COVID-19.

63. The scope of transportation safety did not distinguish between what may be appropriate for the purposes of protecting individuals from the risks imposed on them by others, and the risks that they accept for themselves. For example, individuals were required to be vaccinated to protect other passengers (an objective which may justify greater restrictions), but also to protect themselves (an objective which may not warrant as significant restrictions, and which should leave greater deference for each individual's personal risk tolerance).

64. Additionally, the broad framing of the objective may have led to the consideration of irrelevant and inappropriate factors, such as Canada's vaccine coverage, in decisions which should have been limited to transportation safety. **We therefore recommended** that, in the future, if Transport Canada considers similar mandatory collections of personal information for the purpose of transportation safety, that it more clearly define: (i) the scope of the goal and (ii) the intended objectives/consequences of such measures.

Effectiveness

65. With respect to the second element of the four-part test, effectiveness, we considered whether the measures implemented under the Orders would be effective in meeting the specific needs identified above. Multiple complainants expressed beliefs that (i) COVID-19 vaccines were ineffective in protecting against COVID-19, particularly after Omicron variants became the dominant, and/or (ii) that vaccines were dangerous. Certain complainants based their views on various online sources. It is a reality of the COVID-19 pandemic that much information, but also misinformation, is publicly circulating. Individual reports and opinions, and preliminary, unverified, or misinterpreted data can create confusion. We therefore carefully reviewed the evidence Transport Canada considered to determine the effectiveness of collecting individuals' vaccination status to protect travellers and transportation workers.

66. Transport Canada demonstrated that, prior to the issuance of the Orders, it relied on information from PHAC which included documented, peer reviewed studies, and data specific to the Canadian context, accompanied by evidence-based analysis by PHAC to interpret the information. This evidence concluded that:

    - For the Delta COVID-19 variants of concern circulating at the time, preliminary data indicated that two doses of a COVID-19 vaccine provided meaningful protection against contracting COVID-19 (in the range of 39 to 88%, with

Canadian studies showing protection rates of 80% plus).[26] This was supported by evidence from PHAC's COVID-19 testing of travellers entering Canada between July and October of 2021, which showed that unvaccinated travellers were at least five times more likely than vaccinated travellers to be infected with COVID-19.

- For the Delta COVID-19 variant, vaccines provided even stronger protection (over 90%) against hospitalization and death from COVID-19.
- COVID-19 vaccines approved for use in Canada present a very low risk of serious adverse health risks.[27]

67. The effectiveness of a measure can change over time – particularly in a rapidly changing epidemiological context. Transport Canada provided evidence that it continued to receive data on vaccine effectiveness while the Orders were in effect. This data demonstrated that, as Omicron became the dominant COVID-19 variant, protection offered by vaccines against infection[28] waned over time after a second dose. The complainants pointed to similar evidence and argued that the vaccine mandates imposed by the Orders would thus fail to prevent travellers from contracting or transmitting the virus.

68. However, the evidence from multiple peer reviewed studies continued to show that vaccines provided meaningful protection against serious illness from the Omicron variant 6 months after vaccination (with most studies showing protection in the range of 70-90%). In other words, inoculation, despite providing a waning protection against infection over time, continued to protect travellers from the risks of serious illness if they became infected while aboard a plane or train.

---

[26] Studies conducted before Delta became the dominant strain indicated that COVID-19 vaccines prevented transmission in two ways – by decreasing infection and by decreasing transmission from vaccinated individuals who became infected. However, by August of 2021, PHAC observed that preliminary data from multiple sources indicated that vaccinated individuals who contracted the Delta variant may have been as likely to transmit the virus as infected, unvaccinated individuals.

[27] A PHAC report shared with Transport Canada dated August 2021 references numerous studies on the safety of the vaccines approved in Canada and describes the comprehensive safety monitoring system in place in Canada. For example, it noted that Canada's National Advisory Committee on Immunization (NACI) quickly adjusted the recommendations for the AstraZeneca vaccine when rare thrombotic events were detected. It further notes that as of August 6th, 2021, serious adverse health events were reported after vaccination in only in 0.006% of all doses administered in Canada. Importantly, these adverse events were not necessarily related to the vaccines, as in any large enough group of people adverse events, including deaths, will occur in any given period. Health Canada and PHAC reviewed the reports to determine whether the vaccine may have played a role.

[28] A PHAC analysis shared with our Office by Transport Canada indicated that, in March of 2022, most evidence available to PHAC suggested that for Omicron variants, fully vaccinated individuals without a booster dose were as likely to spread infection to household contacts as unvaccinated individuals. Additionally, studies showed diminishing protection against infection/symptomatic disease over time (20% or less after 6 months), though protection against severe disease was generally sustained over time.

69. We are therefore satisfied that there was evidence to suggest that collecting passengers' vaccination status effectively reduced the risks posed to those individuals, one of the two implicit goals under the broad objective of transportation safety.

Less Privacy Intrusive Measures

70. With respect to the third element, whether less privacy-intrusive measures could achieve the same end, we considered whether Transport Canada considered alternatives to the collection of travellers' vaccination status. This element required Transport Canada to demonstrate that less privacy-intrusive measures would not have been able to achieve its important objective of protecting railway and air transportation safety. In this respect, certain complainants questioned why demonstrating 'natural immunity' or a negative COVID test were not offered as alternatives to proof of vaccination.

71. Firstly, while Transport Canada shared reports which studied the shortcomings of natural immunity, they did not directly provide evidence that natural immunity was ever considered as an alternative to the collection of travellers' vaccination status.

72. For example, in December of 2021, PHAC reported data suggesting that the Omicron variant appeared to be more likely to cause reinfection than previous variants.

73. In March of 2022, Transport Canada received a report from PHAC analysing studies into the protective effects of a previous COVID-19 infection. These studies concluded that a previous infection provides substantial protection from re-infections, though the protective effect is variable and dependent on factors such as the extent of symptoms, the time since infection, and the variant (e.g., Omicron is more likely to cause re-infections than earlier variants). This report highlighted, however, that a number of studies have shown the importance of three exposures to the antigen, whether by infection and/or vaccination, with some studies noting the importance of spacing the exposures. Some studies found that Omicron infections in individuals who were unvaccinated resulted in an immune response to Omicron, but not an immune response to other variants. As a result, the report concluded that vaccination remained an important protective measure, even for individuals with a previous infection.

74. Based on these reports, it was therefore not apparent that natural immunity provided an equivalent or comparable level of protection as vaccines.

75. In their review of mandatory vaccination policies for transportation workers, the Québec Superior Court considered whether natural immunity could be an alternative to mandatory vaccination. It ultimately determined that, based on the expert testimony and relevant studies, natural immunity provided a weaker protection compared to vaccines, particularly against Omicron and against serious illness.[29] Transport Canada advised our Office that, despite making minimal representations on this subject in the

[29] *Syndicat des métallos, section locale 2008 c. Procureur général du Canada*, 2022 QCCS 2455 at paragraph 242.

course of our investigation, they had assisted in preparing more fulsome arguments before the Court in this case's proceedings.

76. Secondly, Transport Canada did not provide evidence that it considered retaining testing as an alternative to vaccination, beyond the initial one-month grace period following the issuance of the Orders, despite having access to data on this issue.

77. Transport Canada indicated to our Office that they considered the results of PHAC's COVID-19 border testing data,[30] which appeared to suggest that testing could be a viable alternative for the purpose of reducing the risk of transmitting COVID-19 to other travellers or to transportation workers. As of April 1st, 2022, vaccinated travellers entering Canada were no longer required to provide a negative pre-arrival COVID-19 test on entry, though this requirement continued to apply to unvaccinated travellers. Post-entry, all unvaccinated travellers continued to be tested for COVID-19, with some vaccinated travellers being randomly tested as well. From this date forward PHAC told OPC that test positivity rates at land ports of entry were relatively similar between the two traveller groups and for travellers entering Canada by air, COVID-19 test positivity was consistently *higher* among fully vaccinated travellers than among tested, non-fully vaccinated travellers.

78. We acknowledge that testing as an alternative can reduce the risk of infecting other travellers or transportation workers (i.e., the risk an individual poses to others). However, given that testing does not reduce the risk of suffering severe illness (i.e., the risk posed to the individual), which we accept was one of Transport Canada's implicit goals under the broad objective of transportation safety, we therefore acknowledge that this alternative would not have been as effective as the requirement to provide a proof of vaccination.

79. Nonetheless, **we recommended that** if Transport Canada considers similar mandatory collections for the purpose of ensuring transportation safety in the future, it specifically examine and document its assessment of potentially less privacy-invasive alternatives, such as testing.

80. In response to our preliminary findings, Transport Canada clarified that a number of less privacy invasive measures had been considered, though these deliberations were the subject of legal applications and actions challenging the Orders, and as a result, were not shared with our Office. Transport Canada had originally requested that our investigation be suspended pending the outcome of these court cases, though our Office denied this request.

Proportionality

81. With respect to the fourth part of the four-part test, whether the loss of privacy is proportional to the need, we had expected Transport Canada to demonstrate that they

---

[30] *COVID-19: Summary data about travellers, testing and compliance - Test Volumes and Positivity Rates*, Public Health Agency of Canada, viewed March 30, 2023.

had analyzed whether the potential privacy impacts to travellers resulting from the collection of information relating to their COVID vaccination status were proportional to the benefits that would result from the collection.

82. The Orders only required the collection of limited information about an individual's vaccination status, which in most cases, was not recorded or retained. Nevertheless, this still constituted medical information, which is inherently sensitive. This loss of privacy must be measured against the benefits of the Orders.

83. In this case, travel by train and plane requires close and prolonged indoor contact of all travellers, with the associated risks of contracting COVID-19 and potentially becoming seriously ill. In light of the benefits of the vaccine which were summarized in the 'Effectiveness' test, the requirement to provide a proof of vaccination credential thus brought meaningful benefits to the safety of travellers. Further, the Orders permitted individuals to travel without showing proof of vaccination in certain circumstances, including to accommodate religious beliefs and travel for medical/emergency purposes. Accordingly, we believe the benefits to travellers from the Orders' measures were proportional to the loss of privacy they suffered when disclosing their vaccination status.

Recommendations

84. We recommended that if Transport Canada considers similar mandatory collections for the purpose of transportation safety in the future, that it (i) more clearly define the scope of the goal, and (ii) specifically examine and document its assessment of potentially less privacy-invasive alternatives. Transport Canada accepted our recommendations.

Conclusion

85. We conclude that the collections, uses and disclosures of personal information by VIA Rail, CATSA and Transport Canada under the Orders were done in compliance with the legal requirements of the *Privacy Act*. The complaints are therefore **not well-founded**.

86. While not a requirement under the *Privacy Act*, we observed that the collection of personal information undertaken by VIA Rail, CATSA and Transport Canada pursuant to the Orders was necessary and proportional. However, we also identified issues with (i) the scope of the objectives under the broad goal of transportation safety, (ii) the consideration of factors unrelated to transportation safety, and (iii) the limited information provided by Transport Canada with regard to its assessment of less privacy invasive alternatives.

87. We believe that this investigation highlights the need to better reflect the principle of necessity and proportionality in public sector privacy law, as the government advances their plans to modernize the *Privacy Act* in the near future.

Vaccine mandates for entry into Canada

Complaints under the *Privacy Act*

May 29, 2023

Description

Under Emergency Orders issued under the *Quarantine Act* in 2021 and 2022 travellers entering Canada were required, with certain exceptions, to provide proof of vaccination status to enter Canada without quarantining (and providing pre and post arrival COVID-19 tests). We investigated whether the related collection, use, retention and disclosure of personal information by Public Health Agency of Canada (PHAC) and Canada Border Services Agency (CBSA) was compliant with the *Privacy Act* (the Act). Additionally, we examined the necessity and proportionality of the measures considering the circumstances under which they were established.

Takeaways

- PHAC and CBSA had the authority to collect personal information, including vaccination status, to administer the Emergency Orders, as this collection was directly related to activities, they were mandated to carry out under the *Quarantine Act*.
- Though the principle of necessity and proportionality is not currently a requirement of the *Privacy Act*, limiting the collection of personal information to what is demonstrably necessary is a requirement of the TBS Directive on Privacy Practices. We identified weaknesses in PHAC's assessment and documentation, but ultimately found that the collections were necessary, effective, and proportional in the circumstances.
- To determine if a collection is necessary and proportional, the objective should be clearly defined, so stakeholders and the public understand the scope of what the measures are trying to achieve.
- Institutions should clearly assess and document their consideration of potentially less privacy invasive alternatives, such as, in this case, COVID-19 testing as an alternative to vaccination status.

Report of findings

Table of Contents

Overview

In the wake of the COVID-19 pandemic, 80 Emergency Orders were issued from February 3rd, 2020 to June 24th, 2022 under the *Quarantine Act* to prevent the introduction and spread of COVID-19 in Canada. Until September 30, 2022 they imposed restrictions on travellers entering the country which varied depending on their age, residency status/citizenship, symptoms and vaccination status. To determine a given traveller's applicable entry requirements and to ensure that these requirements were being respected, the Canada Border Services Agency ("CBSA") and the Public Health Agency of Canada ("PHAC") collected personal information from individuals entering Canada.

The complainants argued that this collection, and the subsequent use and disclosure of their personal information, was unlawful, and believed that their vaccination status in particular should not have been used to limit their other rights (e.g., mobility rights, right to enter Canada, right to liberty, right to security of the person). Some complainants requested that their information be disposed of and claimed that the CBSA's and PHAC's retention of personal information is unnecessary. We note that numerous complaints raised issues which fall outside the scope of the *Privacy Act*, and therefore were not considered by our Office.

We found that the CBSA and PHAC acted in accordance with the *Privacy Act*. The personal information collected was directly related to an operating program or activity (i.e., the administration and enforcement of the Emergency Orders). The information was primarily used and disclosed for the purpose for which it was collected, and/or a purpose authorized by an Act of Parliament. The CBSA and PHAC's retention periods for the personal information collected are equally compliant with the *Privacy Act*.

We also examined the necessity and proportionality of the CBSA and PHAC's personal information processing activities. While not a requirement of the *Privacy Act*, necessity and proportionality is a key privacy principle that we and provincial and territorial Privacy Commissioners recommended be considered in relation to the establishment of vaccine mandates in a Joint Statement.

We found that overall, CBSA and PHAC's collection of personal information under the Emergency Orders was necessary and proportional. However, we identified gaps in PHAC's assessment of potentially less privacy intrusive alternatives, and related issues with respect to clarity of the objectives, in the final six months of the Orders.

In light of these issues, **we recommended** that if PHAC considers similar mandatory collections for the purpose of addressing a pandemic in the future, it specifically examine and document its assessment of potentially less privacy intrusive alternatives against clearly delineated objectives. Further, should the *Quarantine Act* be reviewed in the aftermath of the Pandemic, we would encourage Parliament to consider explicitly clarifying the scope of the purpose of the *Quarantine Act*. PHAC committed to implement the recommendation with respect to examining potentially less privacy intrusive alternatives and confirmed that should the Quarantine Act undergo review it will take the OPC's comments above into consideration.

Background

1. Pursuant to section 58 of the *Quarantine Act*, the Governor in Council may make an order prohibiting or subjecting to any condition the entry into Canada of any class of persons who have been in a foreign country if the Governor in Council is of the opinion that:

   (a) there is an outbreak of a communicable disease in the foreign country;

   (b) the introduction or spread of the disease would pose an imminent and severe risk to public health in Canada;

   (c) the entry of members of that class of persons into Canada may introduce or contribute to the spread of the communicable disease in Canada; and

   (d) no reasonable alternatives to prevent the introduction or spread of the disease are available.

   As orders are made under the authority of the Quarantine Act, the scope of such Emergency Orders are also contoured by the purpose of that Act, defined in section 4 as "to protect public health by taking comprehensive measures to prevent the introduction and spread of communicable diseases."

2. On February 3rd, 2020, the first[1] of 80 emergency orders ("Emergency Orders") was issued pursuant to section 58 of the *Quarantine Act* by the Governor in Council, on the recommendation of the Minister of Health, with the purpose of reducing the risk of importing and spreading the coronavirus disease 2019 ("COVID-19") into Canada. These Orders imposed conditions on individuals entering Canada, which evolved as the Orders were revised and reissued:

   - Prior to the availability of COVID-19 vaccines, earlier versions[2] of the Emergency Orders required most travellers to present an acceptable, pre-arrival COVID-19 test result[3], to test post-border and to quarantine for 14 days upon arrival.
   - Effective July 5th, 2021[4], fully vaccinated[5] travellers with a right of entry into Canada were no longer required to test post-border or to quarantine. We note that

---

[1] *Minimizing the Risk of Exposure to 2019-nCoV Acute Respiratory Disease in Canada Order*, Order in Council PC Number 2020-0059, issued February 3rd, 2020.

[2] *Minimizing the Risk of Exposure to COVID-19 in Canada Order (Quarantine, Isolation and Other Obligations)*, Order in Council PC Number 2021-0421, issued May 21st, 2021.

[3] An acceptable COVID-19 result is either a negative test result from the last 72 hours, or a positive test result that is between 10 and 180 days old.

[4] *Minimizing the Risk of Exposure to COVID-19 in Canada Order (Quarantine, Isolation and Other Obligations)*, Order in Council PC Number 2021-0615, issued June 21st, 2021.

[5] '*Fully vaccinated person*' means a person who completed, at least 14 days before the day on which they entered Canada, a COVID-19 vaccine regimen that uses a COVID-19 vaccine authorized for sale in Canada or in another jurisdiction, that has been determined by the Minister of Health, on the recommendation of the Chief Public Health Officer, to be suitable in preventing the introduction or spread of COVID-19 or any other factor relevant to preventing the introduction or spread of COVID-19.

travellers who did not qualify as fully vaccinated or who chose not to present a proof of vaccination were still required to quarantine for 14 days upon arrival.

- Effective April 1st, 2022[6], pre-arrival testing requirements (also referred to as pre-departure testing) and additional post-border requirements were removed for fully vaccinated travellers, with no changes to the requirements applicable to non-fully vaccinated travellers.

3. The last Emergency Order[7] expired on September 30th, 2022, with the Government of Canada announcing[8] its decision to end the COVID-19 entry restrictions, including testing and quarantine requirements. They attributed this decision to a number of factors, including "modelling that indicate[d] that Canada ha[d] largely passed the peak of the Omicron BA.4 and BA.5 fuelled wave, Canada's high vaccination rates, lower hospitalization and death rates, as well as the availability and use of vaccine boosters (including new bivalent formulation), rapid tests, and treatments for COVID-19."

Analysis

Issue 1: Was the personal information collected directly related to an operating program or activity of PHAC and CBSA?

4. The majority of the complainants argue that the collection of personal information by the CBSA and by PHAC pursuant to the Emergency Orders, and specifically the collection of an individual's vaccination status, was unlawful. We note that the measures under analysis will be limited to those which were in effect from January to September of 2022, as the first complaint related to the Emergency Orders was received by our Office in January of 2022.

5. Section 4 of the *Privacy Act* stipulates that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

6. To determine whether the CBSA and PHAC acted in compliance with the Act, we will first identify the personal information collected by the institutions, then state the operating program/activity for which the information was collected, and finally determine whether such an operating program/activity should be considered legitimate for the respective institutions.

---

[6] *Minimizing the Risk of Exposure to COVID-19 in Canada Order (Quarantine, Isolation and Other Obligations)*, Order in Council PC Number 2022-0321, issued March 31st, 2022.

[7] *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, Order in Council PC Number 2022-0836, issued June 25th, 2022.

[8] *Government of Canada to remove COVID-19 border and travel measures effective October 1*, News release from the Public Health Agency of Canada, issued September 26th, 2022.

Personal information collected

7. Individuals were obligated to provide to employees of the CBSA acting as screening officers[9], and to employees of PHAC acting as screening officers, quarantine officers[10] and as delegates of the Minister of Health[11], the following information/evidence:

    - their COVID-19 test results[12];
    - their quarantine plan[13], which notably included the civic address of their place of quarantine;
    - their contact information[14];
    - the countries where they had resided/visited during the previous 14 days[15];
    - information related to and evidence of their COVID-19 vaccination status[16];
    - responses to any relevant questions posed by the screening officer or quarantine officer[17];
    - for those who were required to quarantine, confirmation that they had arrived at their place of quarantine and daily updates on their health status while in quarantine[18]; and
    - notification that they had developed signs and symptoms of COVID-19 or that they had received a positive COVID-19 test result.[19]

8. Since November 21st, 2020, travellers were required[20] to use the ArriveCAN mobile and web applications ("ArriveCAN") to electronically submit the information[21] listed above. Approximately 200 data elements were collected and retained by the CBSA for each

---

[9] *Quarantine Act*, S.C. 2005, c. 20, section 2 '*screening officer*'.
[10] *Id.*, subsection 5(2).
[11] *Public Health Agency of Canada Act*, S.C. 2006, c. 5, section 5.
[12] *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, Order in Council PC Number 2022-0836, issued June 25th, 2022, paragraphs 12(1)(b), 13(1)(b) and 14(b).
[13] *Id.*, subsection 19(1).
[14] *Id.*, subsection 19(2).
[15] *Id.*, subsection 20(1).
[16] *Id.*, subsection 20(2).
[17] *Id.*, subsection 20(10).
[18] *Id.*, sections 23, 25, 36 and 38.
[19] *Id.*, sections 32 and 36.
[20] *Government of Canada announces new mandatory requirements for travellers to Canada*, News release from the Public Health Agency of Canada, issued November 2nd, 2020.
[21] *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, Order in Council PC Number 2022-0836, issued June 25th, 2022, subsections 19(4) [quarantine plan and contact information], 20(8) [travel history and vaccination information], and sections 23 and 36 [arrival at place of quarantine and daily health status updates].

ArriveCAN submission, such as the traveller's trip information, submission metadata, quarantine information, symptoms, and vaccination information. In some cases, the CBSA collected information from travellers at the port of entry and had inputted it directly into the 'Contact Trace Desktop App', an information management system which contained the same data fields as ArriveCAN. While most information was collected directly from the incoming traveller, some values were generated by ArriveCAN itself, such as the "ocr_result" and "qr_result".

9. The "ocr_result" was generated in response to an optical character recognition ("OCR") check of the traveller's uploaded proof of COVID-19 vaccination credential (also referred to as a 'proof of vaccination credential', 'proof of vaccination' or 'vaccination credential') completed within ArriveCAN to assist the CBSA in their review of each traveller's submission. This OCR check verified that the image or PDF file of the credential contained the requisite elements, based on a fixed set of criteria. If a traveller's credential did not meet the OCR check or if the check was pending, ArriveCAN would flag to the CBSA screening officer that the vaccination credential needed to be examined. Conversely, if the OCR check was successful, the vaccination credential would not typically be viewed or accessed by a screening officer. That said, a screening officer could override the outcome of the OCR check from ArriveCAN by updating the traveller's record in the Contact Trace Desktop App. Finally, we note that the OCR feature of ArriveCAN was the subject of an algorithmic impact assessment[22], as prescribed by the *Directive on Automated Decision Making*[23], conducted by PHAC with the collaboration of the CBSA.

10. If a proof of vaccination credential contained a quick response code ("QR code"), ArriveCAN could authenticate and validate this credential by decoding its contents and verifying its encrypted signatures using the SMART Health Cards Framework protocol[24], thus generating a "qr_result". To complete this process, ArriveCAN would have required the credential issuer's public key. Accordingly, any communication between ArriveCAN and entities which issued proof of vaccination credentials (e.g., provincial health authorities) would have been limited exclusively to the daily download of public encryption keys by ArriveCAN/the CBSA. The CBSA advised our Office that they did not disclose any personal information to issuing entities for the purposes of verifying and authenticating proof of vaccination credentials.

11. The information from ArriveCAN and the Contact Trace Desktop App would be consolidated and delivered to PHAC in a 'combined report'. This combined report contained 114 distinct data elements, which notably included the traveller's name, date

---

[22] *Algorithmic Impact Assessment - ArriveCAN Proof of Vaccination Recognition*, Open Government, Publisher: Public Health Agency of Canada, published October 15th, 2021, Record ID: afc17416-3781-422d-a4a9-cc55e3a053c8.
[23] *Directive on Automated Decision-Making*, Treasury Board Secretariat - Policies, directives standards and guidelines, last modified April 1st, 2021.
[24] *Protocol – SMART Health Cards Framework*, v. 1.2.2, copyright Computational Health Informatics Program, Boston Children's Hospital, Boston, MA.

of birth, passport/travel document number, contact information, address while in Canada, purpose of travel and vaccination information.

12. In addition to what was received from the CBSA, PHAC also collected quarantine compliance information, health / symptoms updates, and COVID-19 test results from:

    - travellers providing information directly to quarantine officers and other PHAC staff[25];
    - the Royal Canadian Mounted Police ("RCMP") and contracted security officers[26], who would conduct compliance verification visits post-border at the traveller's place of quarantine;
    - hotels designated as places of quarantine / government authorized accommodation[27];
    - Employment and Social Development Canada and their contracted service provider, Accenture, who: (i) received calls to report compliance with quarantine measures and health status / symptom updates and (ii) proactively made calls to verify quarantine compliance; and
    - COVID-19 test providers[28].

Operating program or activity

13. The personal information acquired by the CBSA and by PHAC was collected for, and thus directly related to, the administration and enforcement of the Emergency Orders, which themselves were issued pursuant to section 58 of the *Quarantine Act*.

---

[25] At some ports of entry, paper forms used by incoming travellers were scanned by a PHAC employee and sent by encrypted email to either Public Services and Procurement Canada or to a third party information management contractor, Iron Mountain, for manual data entry.

[26] PHAC had entered into contracts with Garda Canada Security Corporation, the Canadian Corps of Commissionaires, G4S Secure Solutions (Canada) Ltd and Paladin Security Group Ltd.

[27] Note: Previous versions of the Emergency Orders required travellers to stay at government authorized accommodation facilities until they had received the results of their COVID-19 post-arrival 'Day 1 Test', see *Minimizing the Risk of Exposure to COVID-19 in Canada Order (Quarantine, Isolation and Other Obligations)*, Order in Council PC Number 2021-0075, issued February 14th, 2021, paragraph 3(1.01)(a).

[28] COVID-19 testing providers have included LifeLabs, Alberta Health, Calian, Dynacare, Biron, Switch Health, BioTech Labs, AlphaLabs, the University of Calgary, Shopper's Drug Mart - DynaLIFE and the National Microbiology Laboratory.

14. The Emergency Orders assigned responsibilities to the CBSA, as screening officers[29], and to PHAC, as screening officers, quarantine officers[30] and as delegates of the Minister of Health[31], which included the collection of personal information.[32]

15. Previous versions of the Emergency Orders had withstood judicial scrutiny[33], primarily on *Charter* grounds, in *Spencer v. Canada (Health)*, 2021 FC 621, though we note that this case only assessed the obligation to quarantine, and not the requirements to submit personal information.

16. Accordingly, we consider the administration and enforcement of the Emergency Orders, which appear to have been issued by the competent authority and which had not otherwise been declared invalid, to be a legitimate operating program/activity of both the CBSA and PHAC.

17. Additionally, the *Quarantine Act* grants the CBSA, as screening officers, and PHAC, as screening officers, quarantine officers and delegates of the Minister of Health, the authority to request and receive a broad spectrum of information/records:

    "15 **(1)** Every traveller shall answer any relevant questions asked by a screening officer or quarantine officer and provide to the officer any information or record in their possession that the officer may reasonably require in the performance of a duty under this Act.

    […]

    55 The Minister [of Health] may collect relevant medical information in order to carry out the purposes of this Act."[34]

18. Furthermore, the collection of personal information, including travellers' vaccination status, was related to both the CBSA's and PHAC's core operating mandates, as outlined in their respective administrative statutes. For example, the CBSA is responsible[35] for providing integrated border services that support public safety by administering program legislation, such as the *Quarantine Act* and the *Customs Act*. PHAC, for its part,

---

[29] *Quarantine Act*, S.C. 2005, c. 20, section 2 '*screening officer*'; *Customs Act*, R.S.C. 1985, c. 1, subsection 2(1) '*officer*'; *Canada Border Services Agency Act*, S.C. 2005, c. 38, section 2 '*program legislation*' and paragraph 5(1)(a).
[30] *Quarantine Act*, S.C. 2005, c. 20, subsection 5(2).
[31] *Public Health Agency of Canada Act*, S.C. 2006, c. 5, section 5.
[32] See footnotes from paragraph 7.
[33] Other notable cases include *Kakuev v. Canada*, 2022 FC 1465, where the Federal Court struck a claim contesting the legality of the Emergency Orders' vaccination requirements given the mootness of the issue, and *Canadian Constitution Foundation v Attorney General of Canada*, 2021 ONSC 4744, which confirmed and adopted the conclusions from *Spencer* regarding the quarantine requirements.
[34] *Quarantine Act*, S.C. 2005, c. 20, subsection 15(1) and section 55.
[35] *Canada Border Services Agency Act*, S.C. 2005, c. 38, section 2 '*program legislation*', and subsection 5(1); *Quarantine Act*, S.C. 2005, c. 20, section 2 '*screening officer*': "screening officer means […] an officer within the meaning of subsection 2(1) of the *Customs Act*."; *Customs Act*, R.S.C. 1985, c. 1, subsection 2(1) '*officer*' and subsection 11(1).

may exercise[36] any of the powers, duties and functions that the Minister of Health is authorized to exercise or perform under any Act of Parliament, which notably include the protection of the people of Canada against risks to health and the spreading of diseases, the monitoring of diseases, and the collection of information relating to public health.

Finding I

19. For the reasons outlined above, we therefore consider the personal information collected by the CBSA and by PHAC to: (i) be directly related to the administration and enforcement of the *Quarantine Act* and the Emergency Orders, (ii) be explicitly authorized by the *Quarantine Act* and the Emergency Orders, and (iii) be rationally connected to the institutions' core, statutory mandates. As such, the CBSA and PHAC acted in compliance with section 4 of the Act, and we find the collection aspect of the complaints to be **not well-founded**.

Issue 2: Was the personal information used or disclosed for the purpose for which it was compiled/obtained, or in accordance with an Act of Parliament?

20. Several complainants have argued that the personal information collected by the CBSA and by PHAC should not have been used to deny travellers entry[37] into Canada, or for the imposition of fines. Others were concerned by the disclosure of their information to provincial and international health authorities, and some suspected that their information would be misused or accessed unlawfully.

21. Sections 7 and 8 of the Act allow institutions to use and disclose personal information, without the consent of the individual to whom the information relates for, among other reasons,

    - the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or
    - any purpose in accordance with any Act of Parliament or any regulation thereunder that authorizes its use/disclosure.

22. In the analysis that follows, we will first describe who could access the personal information held by the CBSA, the CBSA's uses and disclosures of that personal information, and how those activities may be interpreted under sections 7 and 8 of the Act. The same process will subsequently be repeated for the uses and disclosures by PHAC.

---

[36] *Public Health Agency of Canada Act*, S.C. 2006, c. 5, section 5, section 7 and section 11; *Department of Health Act*, S.C. 1996, c. 8, section 4.
[37] Under different iterations of the Emergency Orders, certain non-Canadians were denied entry, while Canadians were, in certain circumstances, required to delay their entry based on pre-departure test results.

CBSA

Uses and disclosures related to Emergency Orders

23. The personal information that the CBSA collected was stored on the Protected B CBSA Amazon Web Services cloud environment, which is aligned with Treasury Board of Canada Secretariat and Shared Services Canada security requirements. Access to the data was controlled via data access profiles monitored by the CBSA.

24. CBSA officers, as screening officers, accessed the personal information in the cloud environment through the Contact Trace Desktop App, and used it to determine whether travellers at a port of entry had satisfied the requirements of the Emergency Orders. Based on the information received and on the conditions/exceptions in force at the time, screening officers provided quarantine instructions to individuals entering Canada[38]. As previously mentioned, this assessment conducted by CBSA officers involved automated processes, such as the OCR scan and QR code verification of the vaccination credential. When warranted, the information received would be used by the CBSA to refer a traveller to PHAC's quarantine officers. CBSA officers, as screening officers, were required to notify quarantine officers of certain events, as prescribed by the *Quarantine Act*[39] (e.g., if a screening officer had reasonable grounds to suspect that a traveller might have a communicable disease).

25. As explained in paragraph 11, the CBSA disclosed a subset of the collected information to PHAC in a 'combined report' for every border crossing. This disclosure enabled PHAC to continue administering and enforcing the Emergency Orders, in their role as screening officers, quarantine officers and delegates of the Minister of Health, and was thus made to support the public health follow-up and compliance verification activities mandated by the Orders.

26. Lastly, the CBSA provided PHAC with data analytics. For example, ArriveCAN information would be presented in charts to illustrate the number of travellers that had arrived on a particular date, or in a map that showed the self-reported locations of symptomatic travellers.

27. In our view, the CBSA's uses and disclosures of personal information, described above, were for the purpose for which the information was obtained or compiled: to administer and enforce the *Quarantine Act* and the Emergency Orders. By using the personal information collected to screen travellers and by disclosing information to PHAC, the CBSA ensured that they fulfilled their role as screening officers, that PHAC fulfilled their

---

[38] *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, Order in Council PC Number 2022-0836, issued June 25th, 2022, section 22. See also: *Quarantine Act*, S.C. 2005, c. 20, subsection 15(3).
[39] *Quarantine Act*, S.C. 2005, c. 20, subsection 16(1). .

role as screening/quarantine officers, and that individuals adhered to the applicable quarantine regime/requirements.

Other uses and disclosures

28. In addition to the administration and enforcement of the Emergency Orders, the CBSA technical support team, the CBSA Cloud Operations team and the CBSA ArriveCAN development team used personal information to support travellers in resolving technical issues and to assist in ArriveCAN troubleshooting.

29. The CBSA also used depersonalized ArriveCAN information to inform operational planning. This included statistics related to traveller types (e.g., exempt vs. not exempt from quarantine and testing), traveller flows, and travel volumes. Staffing at certain ports of entry, for example, would be adjusted based on the amount of traffic they had received and expected to receive.

30. While the purposes of these activities were not entirely related to the purpose for which the information was originally obtained or compiled, we consider them to be consistent with the original purpose, as the uses are sufficiently connected to the purpose of collection that an individual would reasonably expect that the information could be used in such a manner[40]. For example, individuals requesting technical assistance would be aware, and thus reasonably expect, that their personal information could be accessed by the CBSA. Likewise, innocuously using travellers' data from ArriveCAN to adjust staffing and optimize screening efficiency would directly benefit those travellers and would not, in our view, fall outside travellers' reasonable expectations.

31. Lastly, the CBSA indicated that information collected for the purpose of administering the Emergency Orders was not used for any additional purposes, such as informing customs or immigration related matters.

PHAC

32. The information collected by PHAC was accessed, used and disclosed in accordance with the ArriveCAN privacy notice, which, during the period that the Emergency Orders were in effect, stated the following:

"The information required before, when, and after you enter Canada will be used and disclosed for the following purposes:

- for public health follow-up (including disclosure for this purpose to the province or territory where you will be in quarantine/isolation)

[40] Note: For a use to be considered a 'consistent use' for the purposes of the *Privacy Act*, there must exist "a sufficiently direct connection between the purpose and proposed use, such that an [individual] would reasonably expect that the information could be used in the manner proposed." See *Bernard v. Canada* (Attorney General), 2014 SCC 13, paragraph 31.

- for monitoring and verifying compliance with the Quarantine Act and the Emergency Orders made under it (including disclosure for this purpose to law enforcement including, in particular, peace officers)
- to help determine eligibility for new border measures and to support a public health response to COVID-19"

Access

33. Personal information collected from travellers entering into Canada, including the information submitted through ArriveCAN, is populated automatically[41] in PHAC's Quarantine Case Management System ("QCMS"). PHAC had conducted multiple security assessments of the QCMS, obtaining an Interim Authority to Operate in 2020. Security controls were implemented in a phased approach as part of each release, and notably included:
    - supervisor approval of all Dynamics QCMS license assignments to PHAC staff;
    - creation and assignation of a unique designation number for each PHAC officer with access to the QCMS;
    - mandatory completion of the Health Canada/PHAC online privacy training module and of QCMS training by all users prior to gaining access;
    - signing of the QCMS user agreement[42];
    - restricting access to clinical information to users with clinical designations and certifications (i.e., quarantine officers and nurses); and
    - multi-factor authentication for each QCMS login.
34. QCMS users within PHAC were assigned roles and permissions to access data relevant to their function, which were adjusted/removed as necessary. These roles did not typically restrict the number of accessible records, only the content of certain records (e.g., medical information was restricted to quarantine officers, nurses and other professional staff).
35. Besides contracted nurses working at designated quarantine facilities, no external parties could directly access the QCMS. That said, PHAC shared a minimum amount of

[41] Note: The QCMS contains three distinct and separate modules: the Quarantine Officer module, the Compliance & Enforcement module, and the Compassionate Exemptions module. A record is created automatically in the Compliance & Enforcement module for each border crossing, of which there have been more than 46 million since the beginning of the program. Given that each border crossing is captured separately and not linked or consolidated with previous crossings, PHAC has not ascertained the number of distinct individuals whose information is contained within the QCMS.
[42] The user agreement notably required that users only access personal information on a need-to-know basis, that they not export personal identifiers, and that they notify the QCMS administrative team if their QCMS credentials had been used by someone other than themselves.

personal information from the QCMS with other entities to enable them to fulfil their associated roles (as described below in further detail), without granting these parties access to the QCMS. For example, PHAC provided select personal information to the RCMP, contracted security agencies and to Service Canada to enable them to assist in compliance and enforcement. On August 1st, 2022, there were a total of 1,082 internal users and 145 external nursing contractors[43] with access to the QCMS.

Referral to quarantine officer and public health follow up

36. Referrals to a PHAC officer occurred for screening, public health follow-up, or cases of non-compliance.[44] Besides compliance related matters, the information collected was used by PHAC quarantine officers to assess and mitigate a given traveller's public health risk. For example, the personal information of individuals who tested positive on arrival or during their quarantine was shared with local public health authorities, as referenced in previous versions of the ArriveCAN Privacy Notice:

    "As part of Government of Canada's response to the COVID-19 pandemic, your medical information may also be shared with provincial, territorial, municipal governments or organizations as well as their institutions for contact tracing, public health management, following up on cases, and/or for situational awareness."

37. PHAC disclosed individuals' accommodation requirements, COVID-19 status, health evaluation and voluntarily provided special accommodation needs to contracted entities, such as nurses and other medical personnel, responsible for the traveller's stay at a designated quarantine facility. The purpose of this disclosure was to deliver services (e.g., provision of accommodations, food and transportation) and to enhance situational awareness at the facility.

Compliance verification – Applicable border measures (port of entry)

38. Like the CBSA, PHAC employees used the information collected to determine each traveller's applicable entry and quarantine requirements[45], based on the version of the Emergency Order in effect at the time, and verifying whether the traveller met their pre-arrival requirements (e.g., providing a pre-arrival COVID-19 test result or a proof of vaccination credential).

---

[43] Note: The nursing contractors / staff nurses only had access to the Quarantine Officer module of the QCMS, and did not have access to the Compliance and Evaluation module.
[44] Note: Referrals resulted in an 'Event' being created within the QCMS, with 'Traveller' and 'Associated Traveller' records created for each traveller in the Event. When a health assessment of a given traveller was conducted, this was also recorded as an 'Assessment'. By July 20th, 2022, there were 230,000 Events, 340,000 Travellers, 350,000 Associated Travellers and 285,000 Assessments in the QCMS module for quarantine officers.
[45] For example, travellers could consult the following site to identify their applicable entry/quarantine requirements.

Compliance verification – Quarantine and testing (post-border)

39. As indicated in the ArriveCAN Privacy Notice, the personal information held by PHAC was used to verify and enforce compliance with the Emergency Orders' post-border requirements:

    "After your entry to Canada, verification that you have arrived at your place of isolation or quarantine and/or your COVID-19 test results (if applicable) will be used to monitor and verify your compliance with the *Quarantine Act* and the Emergency Orders made under it, and this information may be further disclosed for this purpose to law enforcement. Symptom information, where required during your quarantine, will be used and/or disclosed to the Province or Territory where you will be in quarantine or isolation for public health follow-up.

    Personal information may be disclosed to contractors working for the Public Health Agency of Canada and Service Canada as well as to the following entities: other government institutions, as well as provincial, territorial, municipal governments or international health organizations[46] as well as their institutions for these purposes."

40. Service Canada, a program operated by Employment and Social Development Canada, managed a contract with a third-party call centre, Accenture, which was used by PHAC to verify that travellers were following quarantine/isolation requirements through automated calls (also referred to as 'robocalls'), live agent calls and compliance promotion emails. Based on their responses during these communications, a traveller's compliance with the Emergency Order's requirements was assessed against a risk matrix. Call centre employees were trained and designated as screening officers under section 5 of the *Quarantine Act*.

41. Local law enforcement officers and security contractors also physically visited quarantine locations, established contact with travellers, verified their identity and confirmed that they were in the place of quarantine/isolation that they had indicated in their pre-entry submission. As was the case for the call centre employees, contracted security workers were designated as screening officers under section 5 of the *Quarantine Act*.

42. A record was created in the QCMS every time that a compliance verification activity (e.g., robocall, live call, security visit, police visit, etc.) occurred. By July 14th, 2022, the QCMS contained over 18.2 million compliance monitoring and verification records, which pertained to:

    - 2.4 million automated promotional calls;
    - 4.6 million live compliance verification calls;

[46] Despite this reference in the ArriveCAN Privacy Notice, PHAC confirmed that they have not disclosed information derived from ArriveCAN to international health organizations.

- 8.1 million automated compliance verification calls;
- 2.4 million referrals to the RCMP and to security companies;
- 550,000 in-person compliance verification visits by security companies; and
- 150,000 in-person compliance verification visits by law enforcement.

Compliance enforcement

43. The information was also used for compliance enforcement. In cases of suspected non-compliance, an investigation would be triggered using the information collected. When non-compliance was confirmed, enforcement action could be taken by PHAC, such as issuing a warning or a fine. By July 14th, 2022, there had been over 16,000 recorded enforcement actions. The total number of fines issued in response to contraventions of the Emergency Orders[47], broken down by province and by contravention, has been published on the Government of Canada's *COVID-19: Summary data about travellers, testing and compliance* page[48]. We note that the most common fine was for the maximum amount of $5,000, which was issued 6,632 times.

44. In limited circumstances and at the discretion of PHAC officers or of law enforcement, non-compliant travellers could face summary conviction or arrest. By August 1st, 2022, there had been 17 summary convictions and 9 arrests.

Program evaluation

45. Finally, PHAC used the information under their control, in combination with other available evidence[49], to develop/adjust border policies, to evaluate the effectiveness of current measures, and to support a public health response to COVID-19. This use was explicitly mentioned in previous versions of the ArriveCAN privacy notice, though its description was somewhat vague:

    "The information required before, when, and after you enter Canada will be used and disclosed for the following purposes:

    […]

    - to help determine eligibility for new border measures and to support a public health response to COVID-19

---

[47] Ticket fine amounts could be found in Schedule XVI of the *Contraventions Regulations*. The most common offences were captured under section 58 of the *Quarantine Act* and the maximum penalty amount set in the Contraventions Regulations for that offence was a fine of $5,000. Additional provincial surcharges were applied to these fines, depending on the jurisdiction where the ticket was issued.
[48] *COVID-19: Summary data about travellers, testing and compliance* – Number of fines issued for non-compliance, Public Health Agency of Canada, last modified November 8th, 2022.
[49] COVID-19 data trends, Public Health Agency of Canada, last modified November 1st, 2022; COVID-19 Data Explorer (Source: Johns Hopkins University CSSE COVID-19 Data), Our World in Data.

[…]

Personal information may also be used for program evaluation."

46. When evaluating the Emergency Orders, PHAC considered testing data collected from incoming travellers, a summary of which has been shared on the *COVID-19: Summary data* page[50]. For example, when testing data showed a disproportionally higher number of cases among individuals travelling on flights originating from India and Pakistan, the Government of Canada suspended[51] all direct commercial and private passenger flights from those two countries for 30 days, effective April 22nd, 2021.

Purposes of uses and disclosures

47. For all the activities described above, PHAC used and disclosed the personal information under their control for the same purpose for which the information was originally obtained or compiled: to administer and enforce the Emergency Orders, which notably required incoming travellers to provide information pre-arrival, to quarantine, to undergo a COVID-19 test, and to report on their health status. Individuals were informed of the purposes for which their information would be used and disclosed through the ArriveCAN Privacy Notice, which was presented to them at the moment of collection. As a result, we find these uses and disclosures to have been compliant with paragraphs 7(a) and 8(2)(a) of the Act.

Finding II

48. As such, we find the use and disclosure aspect of the complaints, for both the CBSA and PHAC, to be **not well-founded**.

Issue 3: Was the personal information disposed of in accordance with the *Privacy Regulations* and the *Directive on Privacy Practices*?

49. Certain complainants have requested that the personal information collected by the CBSA and by PHAC, notably through ArriveCAN, be disposed of.

50. Subsection 6(3) of the Act requires government institutions to dispose of personal information under their control in accordance with the *Privacy Regulations* and with any directives or guidelines issued by the President of the Treasury Board.

51. In turn, paragraph 4(1)(a) of the *Privacy Regulations* requires government institutions to retain personal information for at least two years following its last use for an administrative purpose (i.e., a decision making process that directly affects an

---

[50] *COVID-19: Summary data about travellers, testing and compliance – Test volumes and positivity rates*, Public Health Agency of Canada, viewed November 8th, 2022.
[51] *Government of Canada suspends flights from India and Pakistan*, News release from Transport Canada, issued April 22nd, 2021.

individual[52]), unless the individual to whom the information concerns consents to its disposal.

52. While the Treasury Board Secretariat has issued the *Directive on Privacy Practices*, its disposal requirements are not particularly prescriptive, and simply require institutions to apply their respective disposition standards/practices[53].

CBSA

53. In their representations to our Office, the CBSA indicated that they had finalized their data retention and disposal standard operating procedures for information collected in ArriveCAN[54] in the fall of 2022, and are now disposing of all travel related health data that is more than two years old, with exceptions for: (i) data pertaining to active or upcoming investigation/litigation cases, and (ii) for data which may be removed/disposed of directly through ArriveCAN by the user, such as:

    - their ArriveCAN login information[55];
    - their ArriveCAN profile information;
    - their ArriveCAN 'Saved Traveller' profiles; and
    - their active, re-usable ArriveCAN submissions.

54. The CBSA has automated its disposition of travel related health data, with purges occurring once a month since September of 2022. The CBSA also stated that they would dispose of all travel related information collected via ArriveCAN upon receiving a formal, written disposal request by the concerned individual. Such a request may be sent to the CBSA's 'Information Sharing, Access to Information and Chief Privacy Office' or through the electronic form found on the CBSA's 'Compliments, comments and complaints' web page.

PHAC

55. Using Library and Archives Canada's *Generic Valuation Tools*[56] ("the Tools") and complying with the two year minimum retention period prescribed by the *Privacy Regulations*, PHAC had created a retention and disposition schedule for the information collected pursuant to the Emergency Orders. In short, based on the Tools' assessment,

---

[52] *Privacy Act*, R.S.C. 1985, c. P-21, section 3 '*administrative purpose*'.
[53] *Directive on Privacy Practices*, Treasury Board Secretariat, last modified June 18th, 2020, sections 4.2.30 to 4.2.33; *Directive on Security Management*, Treasury Board Secretariat, last modified July 1st, 2019, sections B.2.3.4 and C.2.3.2.4.
[54] Note: While we asked the CBSA to provide their retention and disposal policy for ALL information collected pursuant to the Emergency Orders, they only provided their policy for information collected in ArriveCAN.
[55] Note: This is done by deleting/disposing of the user's ArriveCAN account.
[56] *Generic Valuation Tools*, Library and Archives Canada, last modified August 31st, 2022.

PHAC decided to retain certain categories of information for two years, and other categories for five years. This retention and disposal schedule, as well as a disposition authorization held by PHAC, have been approved by Library and Archives Canada.

56. PHAC indicated to our Office that they are currently refining their processes and systems to ensure that the information collected is disposed of in a comprehensive and coordinated manner. PHAC indicated that it was unwilling to act on requests for disposal before the end of the applicable retention period, out of concern that the information could be needed to examine an individual's travel and/or compliance history, and to inform future compliance activities. There is currently no formal procedure for individuals to request that PHAC dispose of their personal information.

Finding III

57. Based on both the CBSA's and PHAC's actions and policies described above, there was nothing to suggest that either institution contravened the disposal requirements prescribed by the Act, the *Privacy Regulations* or the *Directive on Privacy Practices*. As such, we find the retention and disposal aspects of the complaints to be **not well-founded**.

58. Lastly, we would like to highlight that: (i) the Act **does not** provide a right for individuals to request that their personal information be disposed of, (ii) that institutions **may** dispose of personal information with the consent of the concerned individual prior to the expiry of the mandatory two-year retention period, though are not required to do so, and that (iii) the Act prescribes a considerable minimum retention period of two years, and no **maximum** retention period. Upon future review of the Act, we would recommend that these limitations be addressed by Parliament.[57]

Compliance related matters not explicitly raised by complainants

59. While not the subject of any specific complaints, the representations received during the course of this investigation demonstrated that the CBSA and PHAC were compliant with sections 5 and 10 of the Act, given that the personal information was collected directly from the incoming travellers and described in the 'Quarantine Program' Personal Information Bank (PHAC PPU 071)[58], and that the ArriveCAN privacy notice informed individuals of the purposes for which the information was being collected.

---

[57] Similar proposals have been put forward by Justice Canada, see *Respect, Accountability, Adaptability: A discussion paper on the modernization of the* Privacy Act, Justice Canada, last modified September 1st, 2021, 1.3 Proposed personal information protection principles for the *Privacy Act* – Limiting Retention, and 2.4 Introducing a principles-based approach to retaining personal information.

[58] *Info Source: Sources of Federal Government and Employee Information Public Health Agency of Canada*, PHAC Access to information and privacy, last modified June 30th, 2022, Quarantine Program PHAC PPU 071.

Other: Was the collection of personal information under the Emergency Orders necessary and proportional?

60. Multiple complainants raised concerns over the necessity and the proportionality of the measures enacted by the Emergency Orders. Some believed that COVID-19 vaccines were ineffective and that COVID-19 did not present a health risk that would justify intrusions on their rights and freedoms.

61. Though not a requirement of the Act, necessity and proportionality is a privacy principle that our Office strongly endorses and one that is embedded in the privacy laws of many jurisdictions, including several Canadian provinces. Limiting the collection of personal information to what is demonstrably necessary is also a requirement of Treasury Board Secretariat's *Directive on Privacy Practices*[59].

62. This principle is all the more important when institutions must respond quickly in times of crisis to implement measures that are intended to promote and protect public health, given the elevated potential for the measures to infringe on individuals' privacy rights. In April of 2020, our Office published a *Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19* and in May of 2021, the Federal, Provincial and Territorial Privacy Commissioners issued a joint statement entitled *Privacy and COVID-19 Vaccine Passports*. Both of these publications highlighted the importance of considering necessity and proportionality in the development of measures to address COVID-19, and that doing so would not be a barrier to effective public health management. Several complaints specifically asked us to consider whether institutions had complied with the public guidance promoted by our Office. Consideration of necessity and proportionality was also a key element of the advice we provided to PHAC when it consulted the OPC on the development and implementation of the Emergency Orders' border measures. Given its importance, we thus examined the necessity and proportionality of the collection of personal information mandated by the Emergency Orders.

63. To guide institutions in considering necessity and proportionality, our Office advocates a four-part test[60] that calls for institutions to ask themselves the following questions when establishing particularly privacy-invasive programs and services:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?

---

[59] *Directive on Privacy Practices*, Treasury Board Secretariat, last modified June 18th, 2020, section 4.2.9: "Heads of government institutions or their delegates are responsible for the following […] Limiting the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities."

[60] Expectations: OPC's Guide to the Privacy Impact Assessment Process - *Questions for high-risk programs: necessity, effectiveness, proportionality and minimal intrusiveness*, Office of the Privacy Commissioner of Canada, last modified March 3rd, 2020.

- Is there a less privacy-intrusive way of achieving the same end?
- Is the loss of privacy proportional to the need?

64. We found that CBSA and PHAC's collection of personal information under the Emergency Orders was necessary and proportional. However, as detailed in the section on less privacy intrusive measures below, we identified gaps in PHAC's assessment of potentially less privacy invasive alternatives, and related issues with respect to clarity of the objectives, in the final six months of the Orders.

Necessity

65. With respect to the first part of the four-part test, necessity, we expect institutions to be able to explain, in detail, how a privacy-intrusive initiative is rationally connected to a defined, pressing and substantial goal, and how the proposed collection or use of personal information will serve to meet the goal. This requires empirical evidence in support of the initiative and should preclude the collection of personal information for speculative or "just in case" scenarios.

66. We will first note that the Emergency Orders' enabling provision, section 58 of the *Quarantine Act*, outlines the pressing and substantial goal that the Orders must strive to address, which is to prevent the introduction or spread of a communicable disease that would pose an imminent and severe risk to public health in Canada:

> "The Governor in Council may make an order prohibiting or subjecting to any condition the entry into Canada of any class of persons who have been in a foreign country or a specified part of a foreign country if the Governor in Council is of the opinion that
>
> **(a)** there is an outbreak of a communicable disease in the foreign country;
>
> **(b)** the introduction or spread of the disease would pose an imminent and severe risk to public health in Canada;
>
> **(c)** the entry of members of that class of persons into Canada may introduce or contribute to the spread of the communicable disease in Canada; […]"

67. Similarly, the purpose of the *Quarantine Act* itself, as stated in section 4 of that Act, is to "protect public health by taking comprehensive measures to prevent the introduction and spread of communicable diseases."

68. According to the explanatory notes which accompanied each of the Emergency Orders in their Canada Gazette publications, the objective of the Orders was to "decrease the risk of introducing and spreading COVID-19 and its new variants into Canada, in order to

protect the health of Canadians and mitigate potential burden on the health care system."[61]

69. Based on these statements, we have determined that the Emergency Orders pursued two interrelated goals:

    - the specific goal of "decreasing the risk of introducing and spreading COVID-19 and its new variants into Canada", which in turn served
    - the broader or overarching goal of "protect[ing] the health of Canadians and mitigate potential burden on the health care system", i.e., an imminent and severe risk to public health in Canada.

70. PHAC declined to share the evidence considered prior to the issuance of the Emergency Orders on the basis that such material consisted of confidences of the Queen's Privy Council, which are explicitly exempt from our Office's production powers under subsection 34(2) of the Act. That said, PHAC did point our Office to the Orders' explanatory notes and other publicly available resources, which supported the Government's rationale for issuing the Orders.

71. The last Emergency Order's explanatory notes[62] reported facts which suggested that, with the passage of time, the risk posed by the introduction or spread of COVID-19 was reduced and that the need had therefore become less pressing and substantial:

    - Omicron, the dominant COVID-19 variant of concern circulating when the complaints were received, had with time proved to be less severe than previous variants, and vaccines continued to be effective, especially against severe outcomes;
    - By April of 2022, the domestic Omicron wave had peaked;
    - Domestic availability of COVID-19 vaccines and high levels of vaccination coverage among the people of Canada provided protection against infection and severe disease;
    - Therapeutics to treat circulating variants were effective and had become increasingly available; and
    - COVID-19 spread and severity indicators, including daily case counts, lab test positivity, and wastewater signals, were stabilizing with most areas continuing to decline.

---

[61] Canada Gazette, Part I, Volume 156, Number 28: ORDERS IN COUNCIL, QUARANTINE ACT *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, P.C. 2022-836, issued June 25th, 2022, Explanatory Note.
[62] *Id.*, Explanatory Note.

72. On the other hand, the same explanatory notes also included the following facts, which suggested the continuing need to "decrease the risk of introducing and spreading COVID-19 and its new variants into Canada, in order to protect the health of Canadians and mitigate potential burden on the health care system":

    - COVID-19 can be a severe, life-threatening respiratory disease, which can cause widespread illness if not controlled;
    - Many countries continued to experience COVID-19 transmission and had different levels of vaccination coverage, factors which could have led to the emergence of new and potentially unpredictable variants of concern;
    - With the emergence of the Omicron variant of concern in late November 2021, test positivity among both unvaccinated and fully vaccinated travellers entering Canada increased, peaking in early January 2022;
    - Omicron, being a more transmissible variant, seriously strained public health resources in Canada once introduced;
    - The unexpected emergence of new variants of concern remained a serious public health concern given the potential for a resurgence of travel-related and domestic cases in Canada in the fall of 2022; and
    - Some areas in Canada continued to experience relatively higher cases, severity and/or demands on the local health care system. Canada had also been seeing increased spread of several Omicron sub-lineages.

73. It was therefore reasonable for PHAC to be of the opinion that there was: (i) an imminent and severe risk to public health in Canada, as required by section 58 of the *Quarantine Act*, and (ii) a pressing and substantial need for the Emergency Orders, and thus for the collection of person information. Despite indicators which suggested that the impact of the virus had waned by the spring of 2022, the risks posed by COVID-19 and its variants continued to loom over Canada's public health, as recent historical trends have demonstrated.

Effectiveness

74. With respect to the second part of the four-part test, effectiveness, we considered whether the personal information collection implemented under the Emergency Orders were effective in meeting the specific need identified above.

75. To reiterate, the goal of the Emergency Orders was to decrease the risk of introducing and spreading COVID-19 and its new variants into Canada in order to protect the health of Canadians and mitigate the potential burden on the health care system.

76. In order to achieve this objective, the Emergency Orders imposed requirements (that changed over time) on some or all travellers entering Canada. These included pre-arrival COVID-19 tests as well as quarantine and post-arrival testing. These measures were

supported by evidence of efficacy[63] for decreasing the risk of introducing and spreading COVID-19: (i) by delaying entry of travellers testing positive, (ii) by allowing both the traveller and any notified public health authorities to become aware of and mitigate active COVID-19 cases detected on or after entry[64], and (iii) by limiting contact of recently arrived travellers, who could be incubating COVID-19, with others.

77. PHAC explained that when vaccines were introduced, they were shown to be effective at preventing infection. Therefore, non-fully vaccinated travellers presented a higher risk of importing COVID-19 into Canada compared to fully vaccinated travellers. PHAC highlighted that from July to November 2021 border test positivity was markedly lower among fully vaccinated international travellers compared with non-fully vaccinated travellers. With the emergence of the Omicron variant in late November 2021, the difference in COVID-19 test positivity between these two traveller groups narrowed but remained two to four times higher in the non-fully vaccinated traveller group. This trend persisted through to the end of March 2022.

78. The collection of individuals' vaccination status served to distinguish[65] between fully vaccinated travellers and non-fully vaccinated travellers, who were, in light of the above, each subject to different entry and post-entry requirements. From January of 2022, when our Office received the first complaint about the Emergency Orders, to September of 2022, when the last Emergency Order expired, travellers who did not qualify as fully vaccinated were required to undergo pre-arrival, on-arrival and post-arrival COVID-19 testing, and to quarantine for 14 days after entering Canada, whereas fully vaccinated travellers could enter into Canada largely uninhibited[66]. To effectively apply these disparate regimes, it was necessary to collect each traveller's vaccination status.

---

[63] *Priority strategies to optimize testing and quarantine at Canada's borders*, COVID-19 Testing and Screening Expert Advisory Panel, published May 2021, pages 15 to 16 of pdf: "Modelling shows that both pre-departure and arrival testing are likely to reduce importation of SARS-CoV-2 […] Modelling studies indicate that a 7-day quarantine with a test at the end of the quarantine period may be similarly effective to a 14-day quarantine without testing."

[64] Canada Gazette, Part I, Volume 156, Number 28: ORDERS IN COUNCIL, *QUARANTINE ACT Minimizing the Risk of Exposure to COVID-19 in Canada Order*, P.C. 2022-836, issued June 25th, 2022, *Explanatory Note – COVID-19 situation in Canada*: "The Canada Border Testing Program has detected over 100 000 cases of COVID-19 in arriving international travellers since it was implemented in February 2021. Both pre-arrival and post-arrival testing contribute to reduced secondary transmission in Canadian communities. There is some evidence in scientific literature that each infected international traveller passes the virus on to at least one or two other people. Interrupting these transmission chains through border testing continues to be an important contribution to reducing pressure on Canada's health care systems during successive waves of COVID-19 and to protecting Canada's vulnerable populations."

[65] Note: When the quarantine exemption for fully vaccinated individuals was first introduced, the available data and scientific literature demonstrated that COVID-19 vaccines were effective in preventing infection and reducing transmission. See *Priority strategies to optimize testing and quarantine at Canada's borders*, COVID-19 Testing and Screening Expert Advisory Panel, published May 2021, pages 19 to 21 of pdf; and *Recommendations on the use of COVID-19 vaccines*, National Advisory Committee on Immunization, published May 28th, 2021, Vaccines – Efficacy and effectiveness.

[66] As noted in paragraph 2 of this report, fully vaccinated travellers with a right of entry into Canada were granted an exemption from the requirement to quarantine effective July 5th, 2021, and pre-arrival testing requirements and additional post-border requirements were removed for fully vaccinated travellers effective April 1st, 2022.

79. In our view the collection of vaccination status was thus effective as it enabled quarantine to be imposed on this group of travellers who presented a higher risk of having COVID-19 on entry - and therefore a higher risk of spreading the disease into Canada. Given that unvaccinated travellers were also more likely to fall seriously ill and to be hospitalized, preventing unvaccinated foreigners from entering Canada, and incentivizing Canadians to become vaccinated to avoid quarantine requirements, was likely also effective in mitigating the burden on the health care system as a whole.

Less Privacy Intrusive Measures

80. With respect to the third part of the four-part test, we assessed whether less privacy-intrusive measures could have achieved the Emergency Orders' stated objective of 'decreasing the risk of introducing and spreading COVID-19 into Canada'. For this specific context, and based on the concerns raised by the complainants, this assessment will include an analysis of the following sub-questions:

    - Would the measures have been as effective and less privacy intrusive if the personal information was collected through alternative means (i.e., other than through ArriveCAN)?
    - Would the measures have been as effective if less personal information was collected (specifically individuals' vaccination status)?

Would the measures have been as effective and less privacy intrusive if the personal information was collected through alternative means?

81. Firstly, many complainants expressed frustration with the mandatory use of ArriveCAN, and the fact that they were not presented with the option of submitting the requisite information to a border officer. However, the alternative proposed by the complainants **would not have been 'less privacy intrusive'**, as travellers would have been required to submit the same information in person as they would have shared over ArriveCAN. The loss of privacy in both scenarios would therefore have been equivalent.

82. Additionally, the Emergency Orders' explanatory notes from the summer of 2021 suggest that it would have been difficult to effectively administer the Orders, and thus decrease the risk of introducing COVID-19, without ArriveCAN, given the application's marked efficiency in collecting information:

    > "The Government of Canada has replaced inefficient paper-based processes at Canada's ports of entry with electronic means, including the ArriveCAN app and website, to reduce the public health risks of traveller backlogs and to allow for timely oversight and tracking by public health officials of travellers entering Canada. Traveller volumes are expected to increase significantly in the coming months;

however, this increase is expected not to exceed the capacity of ArriveCAN. Therefore, there is no reasonable alternative to the increasing mandatory use of ArriveCAN to allow travellers to submit COVID-19 related information electronically in advance of their arrival."[67]

83. For these reasons, we find that the measures would not have been less privacy intrusive or as effective had the information been collected through a medium other than ArriveCAN.

Would the measures have been as effective if less personal information was collected?

84. Some complainants stated that they were upset by the mandatory collection of their vaccination status, and the use of this information to impose stricter entry requirements on those who were not fully vaccinated. Accordingly, our Office was asked to consider whether the measures could have been as effective if providing proof of vaccination status had not been mandatory.

85. One less privacy intrusive alternative proposed by certain complainants was permitting travellers to enter Canada (without quarantine) based on providing *either* proof of vaccination *or* a pre-arrival COVID-19 test.

86. In this respect it is notable that from July 5, 2021, to April 1, 2022, the Emergency Orders, with certain exceptions, required travellers to provide *both* proof of vaccination *and* a pre-arrival COVID test as conditions of entry without quarantine. As noted in paragraphs 77 above, PHAC's border testing data showed that when both vaccinated and non-fully vaccinated travellers needed a negative pre-arrival test to enter Canada, fully vaccinated travellers had consistently lower COVID-19 positivity rates in on-arrival testing. Permitting entry without quarantine for travellers who provided just a pre-arrival test would have been less privacy intrusive than requiring both a pre-arrival test and proof of vaccination. However, the evidence does not suggest it would have been as effective in reducing the chance that any given traveller had COVID-19 (and could therefore risk spreading it to others).

87. However, as of April 1, 2022, pre-arrival tests were no longer required for fully vaccinated international travellers while the requirement remained in place for non-fully vaccinated travellers. From this date through to the end of the Orders in September 2022, PHAC told OPC that test positivity rates at land ports of entry were relatively similar between the two traveller groups and for travellers entering Canada by air, COVID-19 test positivity was consistently *higher* among non-tested, fully vaccinated travellers than among tested, non-fully vaccinated travellers.[68] PHAC noted that this suggests the

---

[67] Canada Gazette, Part I, Volume 155, Number 33: ORDERS IN COUNCIL, QUARANTINE ACT *Minimizing the Risk of Exposure to COVID-19 in Canada Order (Prohibition of Entry into Canada from any Country Other than the United States),* P.C. 2021-824, issued June 6th, 2021, Explanatory Note - Government of Canada response to COVID-19 pandemic.
[68] For details see Canada's COVID-19 border measures data, viewed March 29, 2023.

effectiveness of pre-arrival testing in reducing the importation of COVID-19 into Canada. In subsequent correspondence, notwithstanding this higher positivity rate, PHAC advised our office that it was not in a position to validate the proposition that, as of April 1st, 2022, pre-arrival testing alone was *more* effective at reducing the importation of COVID-19 into Canada, for air entries.

88. In our view it is a positive step that PHAC both collected and reflected on evidence about the effectiveness of pre-arrival testing alone in reducing the importation of COVID-19 into Canada - once it was determined that both pre-arrival testing *and* proof of vaccination were no longer warranted in order to enter Canada without needing to quarantine.

89. However, PHAC did not demonstrate to our office that it considered less privacy intrusive alternatives such as permitting travellers to choose whether to provide a pre-arrival test *or* proof of vaccination in order to enter without quarantining, in light of its own data suggesting the effectiveness of pre-arrival testing in reducing importation of COVID-19 into Canada.

90. Nonetheless, later Emergency Orders' explanatory notes, which acknowledged the waning effectiveness[69] of vaccines in preventing infection, also highlighted the continued protection they provided against severe illness, serving to protect the health of Canadians and mitigate the burden on the health care system:

> "The COVID-19 vaccines are effective at preventing severe illness, hospitalization, and death from COVID-19. Against earlier variants of concern such as Delta, two doses of the vaccine decreased symptomatic and asymptomatic infection and hence could reduce the risk of transmission of SARS-CoV-2; however, effectiveness varied depending on the COVID-19 vaccine product received and decreased over time, following vaccination. […] Against Omicron and its sub-lineages, a primary vaccine series provides some protection against symptomatic or asymptomatic infection though for a modest period of time, but still offers reasonable protection against severe disease. A booster dose increases protection against severe disease, as well as against infection but protection remains lower than the protection against earlier variants such as Delta."[70]

91. As previously mentioned, section 4 of the *Quarantine Act* states that: "The purpose of this Act is to protect public health by taking comprehensive measures to prevent the introduction and spread of communicable diseases." It does not explicitly identify broader health goals such as mitigating the burden of communicable diseases on the healthcare system. Further, the Emergency Orders in place for the final months were framed as being for the purpose of decreasing the risk of introducing and spreading

---

[69] *COVID-19 vaccine: Canadian Immunization Guide*, National Advisory Committee on Immunization, last updated October 31st, 2022, Efficacy against symptomatic COVID-19 disease..

[70] Canada Gazette, Part I, Volume 156, Number 28: ORDERS IN COUNCIL, QUARANTINE ACT *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, P.C. 2022-836, issued June 25th, 2022, Explanatory Note.

COVID-19 and its new variants into Canada, **"in order to"** protect the health of Canadians and mitigate potential burden on the health care system; rather than **"and"** to protect the health of Canadians and mitigate potential burden on the health care system. However, PHAC is of the view that "comprehensive measures to prevent the introduction and spread of communicable diseases" necessarily include steps to reduce the seriousness or impact of an illness that is introduced or spread in Canada when it has not been possible to completely stop its introduction or spread, and that to do otherwise would in fact run counter to the statute's goals. As such, PHAC submitted that preventing individuals from falling seriously ill and being hospitalized as a result of the introduction or spread of a communicable disease in Canada and mitigating the associated burden on the health care system are integral to the purpose of the *Quarantine Act*.

92. In support of this interpretive position, the federal government's public messaging during the pandemic consistently indicated that increasing vaccination coverage to protect the health of Canadians and mitigate the potential burden on the health care system was an overall goal.

93. The continuing quarantine requirement imposed on non-fully vaccinated individuals after April 1, 2022, likely incentivised vaccination. We therefore accept, in line with PHAC's broad interpretation above, that the Emergency Orders had "protecting the health of Canadians and mitigating the potential burden on the health care system" as a direct objective. We consider that permitting pre-arrival testing alone as an optional alternative to proof of vaccination alone, while less privacy intrusive, would not have been as effective in achieving this broader objective as it would not have incentivized individuals to become vaccinated, or prevented unvaccinated foreigners (with the related higher risk of serious illness and hospitalization) from entering Canada.

94. However, in light of the insufficient demonstration to OPC that PHAC considered less privacy invasive alternatives, and the lack of clarity of the framing of the breadth of the objectives, **we recommended** that if PHAC considers similar mandatory collections for the purpose of addressing a pandemic in the future, it specifically examine and document its assessment of potentially less privacy-intrusive alternatives against clearly delineated objectives. Further, should the *Quarantine Act* be reviewed in the aftermath of the Pandemic, we would encourage Parliament to consider explicitly clarifying the scope of the purpose of the *Quarantine Act*.

95. PHAC committed to implement the recommendation with respect to examining potentially less privacy intrusive alternatives and confirmed that should the Quarantine Act undergo review it will take the OPC's comments into consideration.

Proportionality

96. With respect to the fourth part of the four-part test, whether the loss of privacy is proportional to the need, we analyzed whether the potential privacy impacts to travellers were proportional to the benefits that would result from the collection of their personal information.

97. In administering the Emergency Orders, the CBSA and PHAC collected a range of personal information, including, in addition to information that would generally be collected by CBSA when a traveler crosses the border, information which many consider to be particularly sensitive, such as travellers' medical information (vaccination status and COVID-test results) and quarantine address. Some complainants were especially troubled by the collection of their vaccination information. This loss of privacy must be measured against the benefits of the collections under the Emergency Orders.

98. In this case, entry of travellers into Canada risked the importation of COVID-19 into Canada, including potentially novel variants of concern. During the period when vaccinated travellers were also required to provide a pre-arrival COVID-19 test, but were not required to quarantine, PHAC's border testing consistently showed that non-fully vaccinated travellers were at least 2 to 4 times more likely to test positive for COVID-19. In our view, reducing this risk of spreading COVID-19 into Canada by requiring non-fully vaccinated travellers to quarantine brought meaningful benefits to Canadians.

99. During the final six months of the Emergency Orders, after PHAC had determined that pre-arrival tests for vaccinated travellers were no longer warranted, the proportionality of continuing to require travellers with pre-arrival tests to also provide proof of vaccination (or be subject to quarantine) was less clear cut, given the data suggesting the effectiveness of pre-arrival testing from this point forward. Nonetheless, individuals who may have been incentivised to get vaccinated by the quarantine measures benefitted from the demonstrated protection against severe disease offered by vaccines, and the health care system likely benefitted from the reduced risk of hospitalization for vaccinated individuals. Accordingly, we believe the benefits to Canadians from the collection of personal information under the Emergency Orders were proportional to the loss of privacy travellers suffered in disclosing their related personal information.

Conclusion

100. In sum, we found the collection, use, disclosure, retention and disposal of information by both the CBSA and by PHAC, for the purposes of administering and enforcing the Emergency Orders, to be compliant with the Act, and all related complaints to therefore be **not well-founded**.

101. While not a requirement of the *Privacy Act*, we also assessed the necessity and proportionality of the mandatory collection of vaccination status by CBSA and PHAC under the Emergency Orders. We found that overall, CBSA and PHAC's collection of personal information under the Emergency Orders was necessary and proportional. However, we identified gaps in PHAC's assessment of potentially less privacy intrusive alternatives, and related issues with respect to clarity of the objectives, in the final six months of the Orders.

102. Given the evidence that vaccination continued to reduce the risk of serious disease to infected individuals, with its related burden on the health care system, we determined that the mandatory collection of vaccination status therefore contributed to the

broader goal of protecting the health of Canadians and mitigating the burden on the health care system. PHAC indicated that this broad objective was necessarily included under the purpose clause of Section 4 of the *Quarantine Act*. We therefore ultimately concluded that the collections of personal information under the Emergency Orders met the necessity and proportionality test.

103. Nonetheless, in light of the insufficient demonstration to OPC that PHAC considered less privacy intrusive alternatives, and the lack of clarity of the framing of the breadth of the objectives, **we recommended** that if PHAC considers similar mandatory collections for the purpose of addressing a pandemic in the future, it specifically examine and document its assessment of potentially less privacy intrusive alternatives against clearly delineated objectives. Further, should the *Quarantine Act* be reviewed in the aftermath of the Pandemic, we would encourage Parliament to consider explicitly clarifying the scope of the purpose of the *Quarantine Act*.

104. PHAC committed to implement the above recommendation with respect to examining potentially less privacy intrusive alternatives and confirmed that should the Quarantine Act undergo review it will take the OPC's comments above into consideration.

Investigation into COVID-19 vaccination attestation requirements established by the Treasury Board of Canada for employees of the core public administration

Complaints under the *Privacy Act*

May 29, 2023

Description

We examined whether the vaccination attestation requirements established by the Treasury Board of Canada for employees of the core public administration, in response to the COVID-19 pandemic, complied with the collection, use and disclosure and transparency provisions of the Act. Additionally, we examined the necessity and proportionality of the measures considering the circumstances under which they were established.

Takeaways

- Federal institutions had the authority to collect information on employees' COVID-19 vaccination status under the *Financial Administration Act* and Part II of the *Canada Labour Code*; and systemic uses and disclosures of such information were consistent with the purposes for which it was collected.
- In accordance with section 11 (1) of the Act, personal information banks and classes of personal information not contained in personal information banks must be included in a public index updated at least annually. Where personal information has been under the control of a government institution for more than a year, and there has been no update to the public index, this will be evidence of non-compliance with section 11 of the *Privacy Act*.
- Though the principle of necessity and proportionality is not currently a requirement of the Privacy Act, limiting the collection of personal information to what is demonstrably necessary is a requirement of the Treasury Board of Canada Secretariat's ("TBS") Directive on Privacy Practices. We identified weaknesses in TBS's assessment and documentation, but found that the collections under the measures, implemented by institutions at TBS's direction, were necessary, effective, and proportional, under the circumstances.
- Institutions should assess and document necessity and proportionality, including consideration of potentially less privacy invasive alternatives, in a structured way when introducing privacy-invasive programs, in order to provide confidence that the privacy interests of Canadians are being respected.

Report of findings

Table of Contents

Overview

Following the Government of Canada's announcement in October of 2021 that employees of the core public administration ("CPA") would be required to be fully vaccinated against COVID-19 and to attest to their vaccination status, the Office of the Privacy Commissioner of Canada ("OPC" or "our office") received 40 complaints against 19 institutions in the core public administration. These institutions were Canada Border Services Agency; Canadian Space Agency; Correctional Service Canada; Employment and Social Development Canada / Service Canada; Finance Canada; Fisheries and Oceans Canada; Health Canada; Immigration, Refugees and Citizenship Canada; Indigenous Services Canada; Innovation, Science and Economic Development Canada; Justice Canada; National Defence; Public Health Agency of Canada; Public Safety Canada; Public Services and Procurement Canada; Royal Canadian Mounted Police; Shared Services Canada; Statistics Canada; and Treasury Board of Canada Secretariat.

Our office received additional complaints against separate employers which will be addressed in separate reports. The requirements for mandatory vaccination and attestation of vaccination status for employees of the CPA were established by the Treasury Board of Canada under the Policy on COVID-19 Vaccination for the Core Public Administration Including the Royal Canadian Mounted Police ("the Policy"). The Policy was suspended on 20 June 2022.

The complainants' main allegations were that the collection of employees' vaccination status, and in some cases religious or medical information in support of an accommodation request to be exempted from the requirements of the Policy, was unreasonable. After investigation and analyses we found that institutions' collection of personal information under the Policy complied with the requirement of section 4 of the *Privacy Act* ("the Act") as it related directly to an institution's operating programs or activities, namely, TBS's health and safety responsibilities as employer during a national emergency situation as a result of the COVID-19 pandemic.

Certain complainants also made allegations about transparency and inappropriate incidental disclosures of personal information, either in relation to the TBS operated Government of Canada Vaccine Attestation Tracking System ("GC-VATS") system used to collect the vaccination attestations, or in relation to individual institutions' handling of personal information.

With respect to transparency, we found no contraventions of subsection 5(2) of the Act which requires that individuals be informed of the purpose of collection of the personal information. However, we found that TBS contravened subsection 11(1) of the Act by not updating its index of personal information to reflect information collected under the Policy within a year of institutions beginning this collection. TBS has now published a personal information bank description for the *COVID-19 Vaccination Attestation and Worksite Testing Program*.

We also found no indications of contraventions on a systemic level of the disclosure provisions of the Act (i.e. section 8) with respect to GC-VATS or the handling of personal information collected under the Policy.

Our investigation also considered whether all aspects of the Policy were necessary and proportional to the attainment of its objectives. 'Necessity' is not a legal requirement under the Act, which requires a lesser threshold of "relates directly to", but it is a key privacy principle embedded in privacy laws in many jurisdictions including several Canadian provinces.

In May of 2021, Federal, Provincial and Territorial Privacy Commissioners recommended in a Joint Statement that governments and businesses consider the principles of necessity, effectiveness and proportionality, in relation to the establishment of vaccine mandates. TBS's own Directive on Privacy Practices requires that institutions limit the collection of personal information to what is demonstrably necessary. These related provisions and considerations contribute to and reflect a heightened expectation of privacy among Canadians.

In April 2020, the OPC issued a Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 (the Framework) and shared it with government institutions in an effort to outline key privacy principles, including necessity and proportionality, that should factor into their assessment of measures proposed to combat COVID-19 that have an impact on the privacy of Canadians.

Accordingly, given its importance, particularly in the context of privacy invasive measures contemplated in a public health crisis, we examined whether the collections under the Policy were necessary and proportional, recognizing that, as stated in the OPC's Framework, the urgency of limiting the spread of the virus was understandably a significant challenge for government and public health authorities and the COVID-19 crisis was a rapidly evolving situation that required swift and effective responses to address extraordinary public health needs.

After careful review, we determined that, while the TBS's responses to certain of our questions could and should have been more fulsome and forthcoming, under the circumstances in which it was developed and implemented, the Policy overall was necessary and proportional. We base this determination on the emergency situation that existed and the central role of the TBS and federal public servants in supporting the federal government's response to the pandemic, including the protection of the heath and safety of Canadians and the provision of important and often vital government and public services during this unprecedented public health crisis.

With respect to the complainants' argument that each department should have been able to adopt different policies in order to exempt teleworking employees from the vaccination requirements, we accept that it was necessary and prudent for the TBS to retain the ability and flexibility to require the onsite presence of its employees on short notice (including employees who regularly worked from home during the pandemic) in order to deal with emergency and other unforeseen situations during the pandemic. We further find that, particularly in the context

of the rapidly evolving pandemic situation, it would have been unfeasible for the TBS or individual Deputy Ministers to establish different policies for each of the institutions in the federal government.[1]

Given the importance of the issue, we have recommended to TBS that it assess any contemplated vaccination measures against the four-part test detailed in this report in advance of any potential future decision to reinstate some or all of the requirements of the Policy. We were disappointed that the TBS did not agree to implement this recommendation, which we feel is consistent with the TBS's own policy on the preparation of privacy impact assessments and is a proven, effective and efficient approach to ensuring that the considerations of necessity and proportionality are imbedded in a program upfront, to optimize the protection of Canadians' privacy rights. We reiterate this recommendation in this final report and would ask the TBS to reconsider its earlier response.

We take note of the TBS's commitment to meet its obligations under the *Privacy Act* and related policy instruments and would remind the TBS that these policy instruments would require the preparation of a Privacy Impact Assessment that would assess the necessity and proportionality of any potentially privacy intrusive measures.

Background

1. On 6 October 2021, the Government of Canada announced that all public servants in the CPA must attest to being fully vaccinated against COVID-19 or be put on leave without pay unless accommodated for medical reasons or on the basis of a prohibited grounds of discrimination. These requirements were formalized for employees of the CPA under the Treasury Board of Canada's Policy on COVID-19 Vaccination for the Core Public Administration Including the Royal Canadian Mounted Police ("the Policy"). The Canadian Armed Forces and other separate federal public service employers were asked to implement substantially similar policies for their employees. Complaints against these other employers will be addressed in separate reports of findings.
2. Under the Policy, all employees,[2] regardless of whether they were working remotely or in a government office, were required to attest to their vaccination status to their respective institutions and, if warranted, request an accommodation. Failure to disclose one's vaccination status resulted in an employee being placed on leave without pay. The same consequence was imposed on employees who were not vaccinated after a grace period or whose request for accommodation was denied.

[1] See Lavergne-Poitras v. Canada (Attorney General), 2021 FC 1232 at para 101.
[2] In the context of this investigation, the term "employees" includes individuals currently employed within the CPA as well as individuals who are candidates in the process of being appointed to positions in the CPA.

3. The Policy lists three separate objectives, all of which are related to protecting the health and safety of employees. They are:

    a. “To take every precaution reasonable, in the circumstances, for the protection of the health and safety of employees. Vaccination is a key element in the protection of employees against COVID-19.”

    b. “To improve the vaccination rate across Canada of employees in the core public administration through COVID-19 vaccination.”

    c. “Given that operational requirements may include ad hoc onsite presence, all employees, including those working remotely and teleworking must be fully vaccinated to protect themselves, colleagues, and clients from COVID-19.”

4. In order to collect vaccination attestations from employees of the CPA, government institutions were required to use a system called the Government of Canada Vaccine Attestation Tracking System (“GC-VATS”) developed by the Treasury Board of Canada Secretariat (“TBS”). GC-VATS is web platform within the TBS Application Portal.

5. Generally, employees of the CPA submitted their vaccination attestations through GC-VATS unless they were unable to do so electronically, in which case paper forms could be used. The paper forms were then scanned and uploaded to GC-VATS. A listing of the information stored in GC-VATS can be found in Appendix 1 of this report.

6. For individuals who requested an accommodation from the requirements of the Policy, supporting information was collected and retained directly by the home department of the individual rather than within the GC-VATS system.

7. Under the Policy, the Office of the Chief Human Resources Officer, a unit within TBS, is required to review the need for the Policy, at a minimum every 6 months, and report the results to the President of the Treasury Board.

8. On 14 June 2022, the Government announced that effective 20 June 2022 the vaccination requirement for the CPA would be suspended. This announcement followed the six-month review of the Policy by the Treasury Board. As part of the announcement, TBS indicated that, "[t]he government will continue to closely monitor domestic and international scientific evidence to assess the need for additional public health measures, including the possible reintroduction of vaccination mandates."

Jurisdiction

9. Several complainants alleged that requiring vaccination and attestation of vaccination status constituted a contravention of their rights guaranteed by the Canadian Charter of Rights and Freedoms (“the Charter”) and that therefore the requirements were unlawful. However, making findings on Charter compliance is outside of the scope of our Office’s jurisdiction and thus outside the scope of this report’s analysis.

Methodology

10. In coming to our conclusions over the course of the investigation, the OPC considered information from both individual institutions as well as from TBS, which functions as the official employer for staff within the CPA under the *Financial Administration Act*. Since individual institutions were directed by TBS, under the Policy, to collect the information from their employees relating to COVID-19 vaccination status as well as accommodation requests, in addition to seeking representations from these individual institutions, we sought and relied significantly on representations from TBS.

Analysis

Issue 1: Was the information collected by institutions related directly to an operating program or activity of the institution as required by the Act?

11. Many of the complainants allege that their respective institutions, pursuant to the Policy, required them to provide, on a mandatory basis, personal information relating to their COVID-19 vaccination status and, in certain cases, religious beliefs or medical history, and that this collection represents an unreasonable infringement of their privacy rights.[3]

12. Section 4 of the Act requires that institutions only collect personal information about individuals if that information relates directly to an operating program or activity of the institution. These programs or activities are normally established through legislation which authorizes the program or activity in question. Section 4 does not require that a collection be "necessary", just that there be "a direct, immediate relationship with no intermediary between the information collected and the operating programs or activities of the government."[4]

13. Though some complainants alleged that their vaccination status was being collected without their consent, it should be noted that the Act does not include a general requirement that institutions obtain individuals' consent for the collection of their personal information.

14. TBS indicated that the lawful authority for the collection of personal information pursuant to the Policy stems from sections 7 and 11.1 of the *Financial Administration Act*

---

[3] Certain complainants also raised, in relation to collection, that TBS had not completed a privacy impact assessment ("PIA") in advance of collection as required by the TBS Directive on Privacy Impact Assessment. While this allegation falls outside the scope of the Privacy Act and we did not examine it in depth, TBS told OPC that in this case it deferred the requirement to conduct a PIA prior to implementing the program, permitting itself an extension to 2 May 2022. On 26 April 2022 TBS submitted a completed PIA to our Office focused on the related implementation of the GC-VATS and the Rapid Testing Attestation Systems (RTAS).

[4] Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) v. Canada (Attorney General), 2016 FC 1289 at para. 141, aff'd 2019 FCA 212.

("FAA"). These sections of the FAA grant the Treasury Board the authority to act for the Queen's Privy Council for Canada on all matters relating to human resources management in the federal core public administration, including the determination of the terms and conditions of employment of persons employed in it. In relation to its responsibility over human resources, Treasury Board is authorized to provide for "any other matters, including terms and conditions of employment not otherwise specifically provided for in [section 11.1 for the FAA], that it considers necessary for effective human resources management in the public service."

15. Additionally, we note that federal institutions are responsible, under section 124 of Part II of the *Canada Labour Code*, to "ensure that the health and safety at work of every person employed by the employer is protected". Subsection 3.1.1 of the Policy identifies that it is an objective of the Policy, "[t]o take every precaution reasonable, in the circumstances, for the protection of the health and safety of employees. Vaccination is a key element in the protection of employees against COVID-19."

16. In support of the Policy, TBS submitted evidence from the Public Health Agency of Canada, dated August 2021, demonstrating that among other things:

    - The Delta variant of COVID-19, which was becoming dominant at the time, was more transmissible than previous variants and risked leading to more hospitalizations and deaths in the midst of what was then Canada's fourth wave of the global pandemic;
    - The approved COVID-19 vaccines were very effective at preventing severe illness, hospitalization and death; and
    - The approved COVID-19 vaccines also appeared to be somewhat effective at preventing outbreaks and the transmission of the virus, although further research was required on the level of effectiveness against the Delta variant.

17. Based on this evidence, we are satisfied that, at the time the Policy was put in place, the collection of information relating to the vaccination status of employees by institutions subject to the Policy related directly to the responsibilities of the institutions to implement TBS policies aimed at ensuring the health and safety of employees in the workplace.

18. The Policy fell within TBS's legal authority to set working conditions for the CPA, including health and safety measures. Furthermore, we are satisfied that knowing the vaccine status of employees was positively and immediately related to ensuring the health and safety of the workplace. The evidence from the Public Health Agency of Canada is that vaccines were effective at preventing severe illness and transmission and that COVID-19 continued to pose serious risks at the time the Policy was put in place.

19. As noted above, on 14 June 2022 TBS suspended the vaccination requirement under the Policy after conducting a review of the Policy in light of the evolving environmental context. It noted that "[t]he government will continue to closely monitor domestic and international scientific evidence to assess the need for additional public health

measures, including the possible reintroduction of vaccination mandates." In this context we note that this review exercise, and future periodic reviews should the requirements of the Policy be reintroduced, are critical to ensuring that any future related collections of personal information meet the threshold of being related directly to operating programs or activities – in this case, ensuring health and safety in the workplace.

20. The Policy also allowed for individuals to request an accommodation from the requirement to be fully vaccinated, "based on a certified medical contraindication, religion, or another prohibited ground for discrimination as defined under the *Canadian Human Rights Act*."[5]

21. In order to obtain an accommodation, subsection 4.3.4 of the Policy indicates that individuals are required to provide "their manager with complete and accurate information necessary to identify appropriate accommodation, including information on relevant limitations, restrictions, and if they are partially vaccinated."

22. The Treasury Board Directive on the Duty to Accommodate further specifies that "persons employed" are responsible for, "4.3.2 [p]roviding their manager with the information necessary to identify appropriate accommodation, including information on relevant limitations and restrictions" and "4.3.3 [c]ooperating and collaborating in good faith with their organization's representative(s) to find one or more means to accommodate such needs, taking into consideration issues of health, safety and cost".

23. We are of the view that collecting personal information to evaluate a request for accommodation under the Policy is directly related to a government institution's responsibilities under the *Canadian Human Rights Act* to avoid discriminating against employees based on prohibited grounds of discrimination.[6] By its nature, assessing if an individual's accommodation request is validly linked to a prohibited ground of discrimination will include collecting highly sensitive information such as medical conditions and religious beliefs. However, there is an immediate and direct relationship between the responsibility to avoid discrimination and collecting information from employees to justify their request for accommodation on the basis of one of these grounds. Indeed, it is difficult to see how a government institution could be expected to make a decision about an accommodation request without obtaining additional information, including, in some cases, intimate details about the nature of the employee's circumstances.

24. Based on the above, we conclude that the collections required under the Policy related directly to existing programs or activities, that being: (i) TBS' responsibilities as an Employer; and, (ii) for institutions that were subject to the Policy, their internal services / human resources activities. We found no instances of collections that were not directly

[5] S.3.2.1 of the Policy.
[6] *Canadian Human Rights Act* (R.S.C., 1985, c. H-6), ss. 7, 10, 15.

related to implementing the Policy. Therefore, we find the allegations with respect to this issue to be **not well-founded**.

Issue 2: Did institutions properly meet the transparency requirements of the Act?

25. Certain complainants alleged that they were not informed by their institutions about how information relating to their COVID-19 vaccination status would be used once collected. Certain complainants also alleged that TBS failed to publish a description of the "TBS central personal information bank (under development)" referenced in the GC-VATS Privacy Statement before collecting employees' vaccination attestations - which impeded their ability to understand what information was being collected.

26. Subsection 5 (2) of the Act requires that individuals be informed of the purpose for which their personal information is being collected under certain circumstances, while Section 11 of the Act requires TBS to "cause to be published," at least once a year, periodically an index of personal information banks ("PIBs") describing each PIB and including certain prescribed elements.

27. With respect to compliance with subsection 5 (2), the Privacy Statement that was presented to individuals when providing their vaccination status via GC-VATS, and on paper/electronic forms for those who were unable to use GC-VATS does describe the purpose of collection as required by subsection 5 (2). Specifically, the following information was included in the Privacy Notice presented by GC-VATS in October 2021:

> The personal information collected will be used to confirm your vaccination status and to consider requests for accommodation for those unable to be vaccinated. The personal information will be used, in conjunction with additional COVID-19 preventative measures, including rapid testing, to determine if you will be granted on-site access to the workplace and to determine whether you may report to work in person or remotely. Your personal information will also be used by your organization and TBS to monitor and report on the overall impact of COVID—19 and compliance with the vaccination program both within the organization and for the Core Public Administration, as described in standard personal information bank PSE 907, Occupational Health and Safety.

28. The information provided in the GC-VATS Privacy Notice, in conjunction with the Policy itself, which was readily available on the Government of Canada's website, is reasonable and sufficient to enable individuals to understand the purposes for which their information is being collected and therefore we do not find a contravention of subsection 5 (2).

29. With respect to compliance with Section 11, Subsection 11 (1) of the Act requires that TBS causes to be published on a periodic basis not less frequently than once each year, an index of all personal information banks, and all classes of personal information not in

personal information banks,[7] under the control of any government institution. The index must describe the PIBs and classes of information and set forth certain mandatory elements such as which institution controls the information, and, for information that has or could be used for an administrative purpose, what the information may be used for and the retention and disposal standards that apply to it.[8]

30. Vaccination attestation collection began in October 2021. We therefore expected the necessary update to the index would occur before the personal information in question had been under the control of government institutions for more than a year. However, TBS did not include the PIB description for *COVID-19 Vaccination Attestation and Worksite Testing Program* in the Personal Information Index[9] until December 22, 2022.

31. The fact that personal information collected about employees to administer the Policy was not included in TBS' personal information index for well over a year demonstrates non-compliance with section 11.

32. In this case, most of the information required to be included in the Index was included directly in the Privacy Notice above. That said, the notice did not include a statement outlining the retention and disposal standards applied to personal information in the bank, which is a required element under s. 11(1) of the Act.

33. Given the contravention of subsection 11 (1), and TBS's subsequent publication of the PIB description, we find the transparency complaints relating to PIBs to be **well-founded and resolved**.

Issue 3: Were disclosures of personal information collected under the Policy authorized under section 8 of the Act?

34. Subsection 8 (1) of the Act requires that personal information under the control of an institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with the conditions identified in subsection 8 (2). Paragraph 8 (2) (a) allows for disclosure "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose".

35. Certain complainants alleged that there had been inappropriate disclosure of information collected under the Policy. We examined allegations that the processes for handling accommodations request, and the use of GC-VATS, may have resulted in inappropriate disclosure of information either within individuals' own institution or to

---

[7] Section 10 of the Act requires that government institutions cause to be included in personal information banks all personal information under the control of the government institution that (a) has been used, is being used or is available for use for an administrative purpose; or (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.
[8] The full text of Section 11 of the *Privacy Act* is available on the Justice Laws Website.
[9] Described on the Sources of Federal Government and Employee Information on the Treasury Board Secretariat website.

staff at TBS as the operator of the GC-VATS system. We did not find any disclosure contraventions associated with the general handling of accommodation requests or the use of GC-VATS – as detailed further below.

36. **General concerns with accommodation requests process:** Several complainants raised general concerns that unreasonable disclosures of their personal information within their institution could have occurred in the process reviewing accommodation requests. We consequently obtained representations from all the respondents subject to the Policy describing how they limited access to accommodations related information to those who needed to know in order to manage the accommodations process. We saw no indications of issues with respect to processes and systems to prevent inappropriate disclosures.

37. In a few cases, we separately investigated allegations of specific disclosure incidents. Except in these cases where we had a specific set of facts to investigate we did not systematically audit the processes and systems in place for handling accommodation request information. We caution all institutions to ensure due diligence in protecting the information of individual employees when managing processes involving the information of many employees.

38. Several complainants also raised a concern that their colleagues, or other employees, such as those managing pay, could infer information about them, such as their vaccination status, from the fact that they were put on leave. However, as noted above, the Privacy Act permits disclosures "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose". In our view, the fact that an individual is on leave, which can occur for a variety of reasons, is information obtained or compiled for the purpose of managing the employee and their work. Therefore, proactive disclosure to relevant employees - such as those processing pay, or colleagues whose workload may be affected - that an individual is on leave is a consistent use with this original purpose and permitted under 8(2)(a) of the Act.

39. **Concerns with the use of GC-VATS:** With respect to the allegations related to GC-VATS, TBS represented that in general, access to individual employee data within GC-VATS is restricted to authorized individuals within the employee's own institution. Specifically, an employee's immediate supervisors have full access to the individual employee's vaccination attestation, including: (i) vaccination status as attested to by the individual employee, (ii) the result of a verification as recorded by the individual employee's immediate supervisor, and (iii) the reason for accommodations if/as requested by the individual employee. Higher-order managers (i.e. superiors to the employee's immediate supervisor, including all senior officials within the organizational structure in which the employee works) have more limited access to: (i) the individual employee's vaccination status as attested to by the individual employee and (ii) the result of a verification as recorded by the individual employee's immediate supervisor.

40. Certain other specific individuals within an employee's own institution with a role in fulfilling responsibilities under the policy (e.g. health and safety officials or human

resources staff) who have been pre-identified as having a "need to know" also have access to individual employees' attestation data through departmental reporting.

41. Specific individuals at TBS do have access to anonymized vaccination attestation data aggregated at a departmental-level in order to fulfill TBS' responsibilities under the Policy. TBS has indicated that these individuals do not have access to individuals' personal information through this reporting mechanism. TBS indicated that only specific individuals within the technical team supporting the GC-VATS solution may be given access to the underlying GC-VATS data for the purposes of diagnosing reported technical defects.

42. Given that all of the disclosures permitted by the access controls on GC-VATS are for the purpose for which the information was obtained, i.e. to implement the Policy, or for consistent uses with that purpose as described in the privacy notice given to individuals, we found no indications of contraventions of section 8 of the Act with respect to GC-VATS. Accordingly, we find the allegations with respect to this issue to be **not well-founded**.

Other

Was the information collected necessary and proportional?

43. Multiple complainants raised concerns about the necessity and the proportionality of the measures established under the Policy.

44. Though not a requirement of the Act, necessity and proportionality is a privacy principle that our Office strongly endorses and is embedded as a requirement in privacy laws in many domestic and international jurisdictions including multiple Canadian provinces. Limiting the collection of personal information to what is demonstrably necessary is also a requirement of TBS's own Directive on Privacy Practices.[10]

45. This principle is all the more important when institutions must respond quickly in times of crisis to implement measures that are intended to promote and protect public health and safety, given the elevated potential for the measures to infringe on individuals' privacy rights. In May 2021, prior to the introduction of the Policy by the Government of Canada, Federal, Provincial and Territorial Privacy Commissioners issued a joint statement entitled, "Privacy and COVID-19 Vaccine Passports", which highlighted the importance of considering necessity and proportionality in the development of COVID-19 vaccine passports, and that doing so need not be a barrier to effective public health management.

[10] "Limiting the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities" is a responsibility of executives and senior officials who manage programs or activities involving the creation, collection or handling of personal information under section 6.2.8 of the TBS Directive on Privacy Practices.

46. Given its importance, we examined the necessity and proportionality of the Policy requiring all employees to attest to their vaccination status and to provide information to support decision-making on providing accommodations from the requirements of the Policy.

47. To guide institutions in considering necessity and proportionality, our Office advocates a four-part test[11] that calls for institutions to ask themselves the following questions when establishing particularly privacy-invasive programs and services:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?
    - Is there a less privacy-intrusive way of achieving the same end?
    - Is the loss of privacy proportional to the need?

48. In our view the Policy is sufficiently privacy invasive to warrant careful consideration against these four questions, as it requires the collection of vaccination status from all federal employees and, where an accommodation is sought by an employee, additional information (including medical contraindications or religious beliefs) to support the request for accommodation. While an individual's attestation of their vaccination status is limited in nature, it nevertheless reveals personal health information, which our Office views as being a personal information category of elevated sensitivity. For those individuals who make accommodation requests, more invasive information relating to their religious beliefs or medical conditions must also be collected.

49. In reviewing the Policy, we kept in mind the reality that, as stated in the OPC's *Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19*, the urgency of limiting the spread of the virus was understandably a significant challenge for government and public health authorities and the COVID-19 crisis was a rapidly evolving situation that required swift and effective responses to address extraordinary public health needs.

50. Given that the information was collected by institutions in response to requirements established by TBS under their authority to establish conditions of work for the core public administration, we expected that TBS, as the policy authority, would be able to describe how it considered necessity and proportionality in the development of the Policy, and be able provide evidence and analysis supporting its conclusions.

51. With respect to the first point of the four-part test, necessity, we expect institutions to be able to explain, in detail, how a privacy-intrusive initiative is rationally connected to a defined pressing and substantial goal, and how the proposed collection or use of personal information will serve to meet the needs. This requires empirical evidence in

[11] Described in Expectations: OPC's Guide to the Privacy Impact Assessment Process by the Office of the Privacy Commissioner of Canada.

support of the initiative and should preclude the collection of personal information for speculative or "just in case" scenarios.

52. Section 3.1 of the Policy states the following objectives:

    - "To take every precaution reasonable, in the circumstances, for the protection of the health and safety of employees. Vaccination is a key element in the protection of employees against COVID-19."
    - "To improve the vaccination rate across Canada of employees in the core public administration through COVID-19 vaccination."
    - "Given that operational requirements may include ad hoc onsite presence, all employees, including those working remotely and teleworking must be fully vaccinated to protect themselves, colleagues, and clients from COVID-19."

53. In its representations to our Office, TBS provided, as noted in paragraph 15, evidence that the requirements established under the Policy were based on public health advice and scientific studies. Given that the requirements were instituted during the global COVID-19 pandemic, we are satisfied that the measures mandated under the policy were connected to the pressing and substantial goal of the "protection of the health and safety of employees".

54. With respect to the second element of the four-part test, whether the measures implemented under the Policy would be effective in meeting the objectives, we are satisfied that there was evidence of the effectiveness of vaccination in achieving the objectives in light of the circumstances present at the time the Policy was put in place. We accept, on this basis, that a vaccination mandate was effective in meeting the objective, and that the collection of vaccination status to implement this mandate was therefore effective in meeting the objectives that were established by TBS.

55. With respect to the third element, the necessity and proportionality principle requires a consideration of whether less privacy-intrusive measures could achieve the same end. This element requires TBS to demonstrate that less privacy-intrusive measures would not have been able to achieve TBS's important objective of protecting the health and safety of its employees.

56. Some complainants argued that rapid tests should have been offered to all as a less privacy-intrusive measure. Although OPC asked about reasonable alternatives to the Policy (including rapid testing), TBS did not provide us with information with respect to its consideration, if any, of such an option.

57. That said, in reviewing Canadian jurisprudence on mandatory vaccination policies we found a number of cases that[12] have considered public health advice with respect to

[12] See for example, Canada Post Corporation v. Canadian Union of Postal Workers, Award N00-20-00008, April 27, 2022 at para. 95; BC Hydro and Power Authority v International Brotherhood of Electrical Workers, Local 258, 2022 CanLII 25764 (BC LA) at para. 61; Toronto District School Board v. CUPE, Local 4400, 2022 CanLII 22110 (ON LA); Almagamated Transit Union, Local 113 v. Tornoto Transit Commission, 2021 ONSC 768 (CanLII) at paras. 99-109; Costa, Love, Badowich and Mandekic v. Seneca College of, 2022 ONSC 5111 (CanLII) at para. 109; Elementary Teachers' Federation of Ontario v. Ottawa-Carleton District School Board, 2022 CanLII 53799 (ON LA) at paras. 49-50; Toronto Professional Fire Fighters' Association, I.A.F.F. Local 3888 v. Toronto (City), 2022 CanLII 78809 (ON LA) at paras. 235-244; .

rapid testing as an alternative to mandatory vaccine mandates. These cases dealt with situations where affected individuals are largely required to be in shared physical spaces. The decision makers in these cases upheld mandatory vaccination policies that did not permit individuals to freely choose rapid testing as an alternative, citing relevant public health advice. Some cases cited provincial medical authorities in two cases, and expert epidemiological testimony in the other two cases. These sources noted that: (i) in contrast with the strong body of evidence for the protective effect of vaccines, there is a lack of concrete evidence, such as observational studies or controlled trials, demonstrating that rapid testing regimes reduce transmission, and (ii) rapid testing regimes do not prevent serious illness from infection where such infections occur.

58. As a result, we are satisfied that rapid tests would not have been a valid alternative in the circumstances.

59. TBS provided analysis from the Public Health Agency of Canada, supported by references to external evidence, demonstrating that at the time it put the Policy in place there was a substantial body of evidence on the efficacy of vaccines for protecting individuals coming into contact with others, such as in a shared workspace, from severe illness.

60. We accept in this regard that vaccination was demonstrated to be the most effective means to ensure that employees who attended onsite were protected from COVID-19.

61. However, the complainants argued that proof of vaccination status should not have been required for those employees on telework with no reasonably foreseeable need to work onsite on a permanent or ad hoc basis.

62. We note that Court and tribunal decisions that have considered vaccine requirements to date have emphasized the importance of assessing the relevant operating context, including whether employees work onsite or from home.[13]

63. TBS confirmed that the decision to require employees to be present on-site on an ad hoc basis or more regularly was left to Deputy Heads and/or individual managers to determine based on their operational needs. Further, TBS also confirmed that it did not consult with Deputy Heads prior to implementing the Policy about plans to require employees to return to the office or whether, indeed, there were reasonably foreseeable

[13] See for example, Lavergne-Poitras v. Canada (Attorney General), 2021 FC 1232 (CanLII) at paras. 69, 73-74, and 101); Toronto District School Board v. CUPE, Local 4400, 2022 CanLII 22110 (ON LA); Maple Leaf Foods Inc., Brantford Facility v. United Food and Commercial Workers Canada, Local 175, 2022 CanLII 28285 (CanLII) paras. 28-31; BC Hydro and Power Authority v. International Brotherhood of Electrical Workers, Local 258, 2022 CanLII 25764 (BC LA) at paras. 65-68.

operational requirements that could require all of their employees to have to attend onsite.

64. We confirmed with several institutions that they had no immediate, broad, return-to-office plans. Indeed, many employees have been working remotely for two years and have not been in their offices since March of 2020. Some complainants have alleged that they have never actually set foot in their institution's offices as they were appointed during the pandemic and have been working remotely since their first day with the institution.

65. TBS justified the application of the Policy to all employees on the basis that the operating model for government operations prior to the pandemic was based on a requirement for onsite presence and that while telework provisions had been put in place as a business continuity approach during the pandemic, all employees could at any time be required to be present on-site on an ad hoc basis for operational needs (such as attending the office for security or other reasons, opening and managing mail, processing information on enhanced secure networks, urgent requirements that require immediate onsite presence, or technical problems with the employee's ability to work remotely). The TBS added that it would have been impractical to only seek to confirm a teleworking employee's vaccination status when such presence was required given the long delay that would have entailed for unvaccinated employees to become vaccinated in order to provide services to the public.

66. The TBS indicated that many public servants were in the front lines providing in-person services to Canadians during the pandemic and that the TBS could not wait for emergencies or other type of unforeseen situations to then require and verify vaccination for teleworking employees, especially given the overall operations of the federal public service.

67. While we would have expected a more fulsome and forthcoming response from the TBS with respect to our questions on this issue, we are of the view that some deference is owed to the TBS with respect to its assessment of its needs for employee onsite presence during this unprecedented public health emergency.

68. The TBS and the federal government were on the front lines protecting the health and safety of Canadians and providing important and often vital services during a rapidly evolving situation. In the absence of evidence to the contrary, we accept that in this context it was necessary and prudent for the TBS to retain the ability to require the onsite presence of its employees on short notice (including employees who regularly worked from home during the pandemic) in order to deal with emergency and other unforeseen situations during the pandemic. We further find that, particularly in the context of the rapidly evolving pandemic situation, it would have been unfeasible for the TBS to ensure workforce availability and interoperability had deputy heads of institutions

been assigned the responsibility for establishing vaccination policies specific to the operational context of their own institutions across the federal government.[14]

69. For all these reasons, we conclude that TBS Policy has met the third element of the four-part test.

70. With respect to the fourth part of the four-part test: is the loss of privacy proportional to the need, we had expected that TBS would be able to demonstrate that they had analyzed whether the potential privacy impacts to employees resulting from the collection of information relating to their COVID vaccination status were proportional to the benefits that would result from the collection.

71. It should be noted that the Policy required the disclosure of limited information about an individual's vaccination status, information that at the time the Policy was first instituted, was also required to be disclosed to access many services in a number of provinces, including restaurants. Nevertheless, it remains medical information (sensitive by nature) and in certain cases could entail the disclosure of additional sensitive personal information for employees making accommodations requests.

72. This loss of privacy must be measured against the benefits of the Policy. For the reasons set out in the assessment of the third element, we are satisfied that the benefits of the Policy were to protect the health and safety of all TBS employees while ensuring that the TBS retained the ability and flexibility to require the onsite presence of its teleworking employees to respond to emergencies or other unforeseen situations when providing public services to Canadians during a global pandemic.

73. When measured against this objective, we find that the loss of privacy was proportional to the benefits in the context of this emergency situation.

74. Based on the evidence and representations before us, we are satisfied that the Policy met the necessity and proportionality requirements.

75. While the vast majority of the personal information collected under the Policy was collected in the fall of 2021, additional personal information continued to be collected (such as from newly recruited staff), and employees who refused to provide the requested personal information continued to be subject to administrative consequences including being placed on unpaid leave status until the Policy was suspended on 20 June 2022. An important aspect of assessing necessity and proportionality, particularly in a rapidly evolving public health context, is the need to reassess on a timely basis as circumstances evolve. We note, importantly, that the Policy acknowledged this by setting a six-month review, which commenced in April, 2022. As a result of this review, the measures established under the Policy were suspended when TBS deemed that they were no longer warranted based on the current public health situation.

76. We asked TBS to provide information relating to its assessment of necessity and proportionality as part of the review process it undertook prior to suspending the Policy

[14] See Lavergne-Poitras v. Canada (Attorney General), 2021 FC 1232 (CanLII) at para 101.

in June 2022. In response it provided hyperlinks to a range of public studies on the effectiveness of vaccines against omicron variants of COVID-19 without any contextual analysis, but declined to provide further information citing cabinet confidences. We therefore cannot comment on the integrity of TBS's review process.

Recommendations

77. Given the importance of the issue, we have recommended to TBS that it assess any contemplated vaccination measures against the four-part test detailed in this report in advance of any potential future decision to reinstate some or all of the requirements of the Policy. We were disappointed that the TBS did not agree to implement this recommendation, which we feel is consistent with the TBS's own policy on the preparation of privacy impact assessments and is a proven, effective and efficient approach to ensuring that the considerations of necessity and proportionality are imbedded in a program upfront, to optimize the protection of Canadians' privacy rights.

78. We note that the TBS has a leadership role within the federal administration in their application of privacy policy and promotion of compliance, and we reiterate the above recommendation and would urge the TBS to reconsider its earlier response.

79. We take note of the TBS's commitment to meet its obligations under the *Privacy Act* and related policy instruments. We would remind the TBS that these policy instruments would require the preparation of a Privacy Impact Assessment that would assess the necessity and proportionality of any potentially privacy intrusive measures.

Conclusion

80. We conclude that the Policy was largely implemented in conformity with the legal requirements of the Act, with the exception of TBS's failure to update its index of personal information to reflect personal information collected to administer the Policy within the timeframe required under the Act.

81. On a policy level and although not currently a legal requirement, we also conclude that the TBS policy was necessary and proportional. However, we would have expected more fulsome and forthcoming responses from the TBS during this investigation and we encourage the TBS to put in place measures to fully assess and document how it meets the necessity and proportionality requirements when assessing potentially privacy-intrusive measures.

82. We believe that this investigation highlights the need to better reflect the principle of necessity and proportionality in public sector privacy law, as the government advances their plans to modernize the *Privacy Act* in the near future.

Appendix 1 – Listing of information collected in GC-VATS

GC-VATS is prepopulated with the following information on individuals which was already collected by the employer:

- Last name
- Given name
- Manager's Name
- Department
- Place of work (country)
- Place of work (province or territory)
- Group
- Level
- Position number
- PRI (paper attestations only)
- Email address
- Date of Birth (paper attestations only)
- Manager's PRI (paper attestations only)
- Manager's DOB (paper attestations only)

Additionally, GC-VATS collects the following the specific information from individuals as part of the attestation process:

- Employee acceptance
- Attestation of vaccination status
- Verification status
- Manager's verification confirmation

Investigation into COVID-19 vaccination attestation requirements established by Department of National Defence for members of the Canadian Armed Forces

Complaints under the *Privacy Act*

May 29, 2023

Description

We examined whether the vaccination attestation requirements established by Department of National Defence (DND) for members of the Canadian Armed Forces (CAF) in response to the COVID-19 pandemic complied with the collection, use, and disclosure provisions of the *Privacy Act* (the Act); including whether access controls in DND's Monitor MASS (Military Administration Support System) system were sufficient. Additionally, we examined the necessity and proportionality of the measures considering the circumstances under which they were established.

Takeaways

- DND had the authority to collect information on CAF members' COVID-19 vaccination status under the National Defence Act and Part II of the Canada Labour Code; and uses and disclosures of such information were generally consistent with the purposes for which it was collected.
- For systems, such as DND's Monitor Mass, which are used to house sensitive personnel information (including in this case COVID-19 vaccination status) centralized oversight of access permissions is important to avoid inappropriate access, without a valid purpose, to sensitive personal information.
- Though the principle of necessity and proportionality is not currently a requirement of the Privacy Act, limiting the collection of personal information to what is demonstrably necessary is a requirement of the TBS Directive on Privacy Practices. In this case we found that the collection of personal information under the measures implemented by DND for members of the CAF was necessary, effective, and proportional, under the circumstances.

Report of findings

Table of Contents

Overview

Following the Government of Canada's announcement in October of 2021 that federal public servants would be required to be fully vaccinated against COVID-19 and the Department of National Defence's ("DND") issuance of the CDS Directive on CAF COVID-19 Vaccination ("the CDS Directive") which required members of the Canadian Armed Forces ("CAF") to be fully vaccinated and attest to their vaccination status, our office received 16 complaints against DND/CAF.

Our office also received complaints against the Treasury Board of Canada Secretariat ("TBS") and institutions of the core public administration (including one against DND by a civilian employee) as well as complaints against other public organizations that are not subject to TBS's Policy on COVID-19 Vaccination for the Core Public Administration Including the Royal Canadian Mounted Police ("TBS's Policy") and instead have their own management authorities established under their institution's legislation. Those complaints are addressed in separate reports.

Several complainants alleged that the collection of CAF members' vaccination status, and in some cases religious or medical information in support of an accommodation request to be exempted from the requirements of the CDS Directive, was unreasonable. After investigation and analysis we found that DND/CAF's collection of personal information under the CDS Directive complied with the requirement of section 4 of the Privacy Act (the "Act") as it relates directly to DND operating programs or activities, namely, DND's workplace health and safety responsibilities during a national emergency situation as a result of the COVID-19 pandemic.

Certain complainants alleged that DND/CAF's use of personal information relating to their vaccination status was improper. We determined that the use of this information by DND/CAF was consistent with the purposes for which it had been collected and, as such, complied with section 7 of the Act.

Many complainants also raised concerns in relation to DND/CAF's use of Monitor MASS to record members' vaccination status. They alleged that access controls and permissions were insufficient to prevent unauthorized access to their personal information. We did not find any instances of inappropriate access to CAF members information; however, we recommended that DND/CAF implement measures to periodically validate that units properly review and revoke permissions that provide access to CAF members' sensitive information in Monitor MASS. DND has declined to implement this recommendation.

Certain complainants also alleged that they had declined to provide DND/CAF with information relating to their vaccination status which resulted in them being identified as "Unvaccinated" in Monitor MASS. They alleged that this information was not an accurate reflection of their vaccination status, and that DND/CAF did not take all reasonable steps to ensure that the complainants' vaccination status was accurate, up-to-date and complete. We determined that

DND/CAF had, in fact, provided members with the opportunity, instructions, and tools necessary to ensure that information relating to their vaccination status was as accurate, up-to-date and complete as possible. CAF members who were unwilling to attest to their vaccination status could select as a reason "[u]nwilling to share vaccination status" to reflect their decision or status more accurately. This did not materially affect DND / CAF's decision-making process with respect to imposing administrative consequences on CAF members who were unwilling to attest.

Based on the above, we concluded that the CDS directives were implemented in conformity with the legal requirements of the Act.

Additionally, although not a requirement under the Act, we also examined the principles of necessity and proportionality as they pertain to the collections established under the CDS directive. We determined that, in the context of the global COVID-19 pandemic, the CDS Directive was, overall, necessary and proportional given the emergency situation that existed; the real potential that CAF members would need to deploy within Canada and internationally; and the role of the CAF in supporting the federal government's response to the pandemic. Similar to other federal employers, DND/CAF has clear obligations under the Canada Labour Code to protect health and safety of its employees (i.e. CAF members) in the workplace and we are satisfied that based on the conditions and public health guidance at the time, that vaccination was the most effective method to prevent infection and serious disease from COVID-19 in order to ensure the health and safety of the Defence Team and the operational readiness posture of the CAF.

As such, we are satisfied that the CDS Directive addressed the necessity and proportionality principles in the context of the global COVID-19 pandemic.

Background

1. On 6 October 2021, the Government of Canada announced that all public servants in the core public administration would need to attest to being fully vaccinated against COVID-19 or be put on leave without pay unless accommodated for medical reasons or on the basis of a prohibited grounds of discrimination. These requirements were formalized for employees of the core public administration under TBS's Policy.

2. The Canadian Armed Forces (CAF), which is supported by Department of National Defence (DND), and other separate federal public service employers were asked to implement substantially similar policies for their employees.

3. Subsequently, on 6 October 2021, the Chief of the Defence Staff (CDS) of the CAF issued the CDS Directive. This was supplemented on 15 November 2021 by the CDS Directive 002 on CAF COVID-19 Vaccination – Implementation of Accommodations and Administrative Action.("CDS Directive 002"). CDS Directive 002 was later amended on 2022 December 2021. These amendments provided details on additional flexibility for

members in remote locations and those currently on operational deployments; and described additional requirements for the processing of requests for accommodation.

4. Under the Directive, all CAF members,[1] including those working from home, were required to attest to their COVID-19 vaccination status. Those who could not be vaccinated due to grounds protected under the *Canadian Human Rights Act* could request an accommodation. Failure by a member to disclose their vaccination status would result in "administrative consequences" which could include a recorded warning, counselling and probation, and an administrative review which could lead to release from the CAF. The same consequences would be imposed on CAF members who were not vaccinated after a grace period or those whose request for accommodation was denied if they remained unwilling to be vaccinated.

5. The Directive referred significantly to TBS's Policy, including in matters relating to requesting an accommodation, in order to ensure alignment. In this regard, the CDS Directive and TBS's policy, established similar requirements with similar objectives. It should be noted however that TBS's Policy did not contemplate unvaccinated employees (or those who were unwilling to attest to their vaccination status) losing their jobs in the same manner in which CAF members could potentially be released from the CAF following an administrative review.

6. The Directive identified that the measures were being implemented, "in order to protect members of CAF and the Defence Team, and to demonstrate responsible leadership to Canada and Canadians through the Defence Team's response to the pandemic".[2]

7. In order to collect vaccination attestation information, CAF members were required to input their vaccination status into Monitor MASS, an operational human resource management application developed and operated by DND/CAF. For members who did not have access to Monitor MASS, paper forms could be submitted to the member's supervisor who would then enter the information for the individual in Monitor MASS.

8. On 11 October 2022, the CDS issued CDS Directive 003 on CAF COVID-19 Vaccination for Operations and Readiness ("CDS Directive 003"), which superseded the previous CDS Directives on CAF COVID-19 Vaccination. While this directive provided certain conditions under which CAF members would not need to be fully vaccinated against COVID-19 (i.e. where vaccination is not required for operational readiness reasons), it retained the

[1] This did not include civilian employees of DND, or contractors, whose vaccination and attestation requirements were established under TBS's Policy.

[2] CDS Directive on CAF COVID-19 Vaccination, para. 19.

requirement that all CAF members would need to attest to their COVID-19 vaccination status.

Jurisdiction

9. Several complainants alleged that requiring vaccination and attestation of vaccination status constituted a contravention of their rights guaranteed by the *Canadian Charter of Rights and Freedoms* ("the Charter"), and that therefore the requirements were unlawful. However, making findings on Charter compliance is outside of the scope of our Office's jurisdiction and thus outside the scope of this report's analysis.

Methodology

10. Given that DND / CAF was asked to align with the requirements of TBS's Policy and that, as such, the policy largely informed the broad requirements of the related CDS directives, we have relied additionally upon TBS's representations in relation to TBS's Policy. We refer readers to the Report of Findings for our *Investigation into COVID-19 vaccination attestation requirements established by the Treasury Board of Canada for employees of the core public administration* for additional background and context.

Analysis

Issue 1: Was the information collected by DND/CAF related directly to an operating program or activity of the institution as required by the Act?

11. Several of the complainants allege that DND, pursuant to the Directive, required them to provide, on a mandatory basis, personal information relating to their COVID-19 vaccination status and, in certain cases in order to obtain an accommodation from these requirements, information about their religious beliefs or medical history. These complainants allege that this collection represents an unreasonable infringement of their privacy rights.

12. Section 4 of the Act requires that institutions only collect personal information about individuals if that information relates directly to an operating program or activity of the institution. These programs or activities are normally established through legislation which authorizes the program or activity in question. Section 4 does not require that a collection be "necessary", just that there be "a direct, immediate relationship with no

intermediary between the information collected and the operating programs or activities of the government."[3]

13. While certain complainants alleged that their vaccination status was being collected without their consent, it should be noted that the Act does not include a general requirement that institutions obtain individuals' consent for the collection of their personal information. We also note that vaccination status information was collected directly from CAF members; and, that members were informed, in the CDS Directive as well as in the Monitor MASS privacy notice, of the purpose of the collection, in accordance with section 5 of the Act.

14. DND responded that it collected members' COVID-19 vaccination status in fulfillment of its responsibilities under the Canada Labour Code and that the collection related directly to ensuring the health and safety of CAF members in the workplace.

15. DND further indicated that the information was collected pursuant to sections 4 and 18 of the National Defence Act (NDA) in relation to the control and administration of the CAF; and, more specifically, in order to ensure the health and safety of the Defence Team and the operational readiness posture of the CAF.

16. We accept that the CAF has a unique role within the Government of Canada in responding to events within Canada and around the world; and that DND therefore has a need to understand whether individual CAF members are deployable and under which circumstances and limitations. Additionally, it is not always possible to foresee when or where individual CAF members, or their units, will need to be deployed.

17. In support of the Directive, DND submitted evidence from the Public Health Agency of Canada, dated 3 September 2021, demonstrating that among other things:

    a. The Delta variant of COVID-19, which was becoming dominant at the time, was more transmissible than previous variants and risked leading to more hospitalizations and deaths in the midst of what was then Canada's fourth wave of the global pandemic; and,

    b. The approved COVID-19 vaccines were very effective at preventing severe illness, hospitalization and death.

18. Based on this evidence, we are satisfied that, at the time the Directive was put in place, the collection of information relating to the vaccination status of CAF members related directly to the responsibilities of DND to ensure the health and safety of CAF members

---

[3] *Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) v. Canada (Attorney General)*, 2016 FC 1289 at para. 141, aff'd 2019 FCA 212.

and DND civilian employees in the workplace and to ensure the operational readiness posture of the CAF.

19. The Directive contemplated three potential vaccination status options for CAF members: "fully vaccinated"; "unable to be vaccinated"; and "unwilling to be vaccinated". The last status would include those members who were either unvaccinated or vaccinated but unwilling to disclose their vaccination status, and were not approved for an accommodation under grounds defined in the Canadian Human Rights Act.

20. The Directive allowed for individuals to request an accommodation if they could not "be fully vaccinated due to a certified medical contraindication, religious ground, or any other prohibited ground of discrimination as defined in the Canadian Human Rights Act (CHRA)".[4] Details for requesting accommodations were later specified in CDS Directive 002 on CAF COVID-19 Vaccination – Implementation of Accommodations and Administrative Action published in November 2021 and subsequently updated in CDS Directive 02 on CAF COVID-19 Vaccination – Implementation of Accommodations and Administrative Action – Amendment 1 in December 2021.

21. In order to request an accommodation on medical grounds, CAF members were required to provide information about their medical contraindications using forms completed and signed by a healthcare provider.[5] In order to request an accommodation on religious grounds, CAF members were required to "articulate the requirement for the religious request by sworn attestation using the GC affidavit form *Religious Belief*, explaining the basis of the religious nature of the exemption and why it prevents vaccination".[6] Finally, in order to request an exemption based on grounds of discrimination under the CHRA, a member was required to "articulate the requirement for accommodation articulating the grounds of discrimination under the CHRA by using an affidavit, explaining the grounds for discrimination basis of the request and why it prevents vaccination".[7]

22. We are of the view that collecting personal information to evaluate a request for accommodation under the Directive is directly related to a government institution's responsibilities under the *Canadian Human Rights Act* to avoid discriminating against employees based on prohibited grounds of discrimination.[8] There is an immediate and direct relationship between this responsibility and collecting information from employees to justify their request for accommodation on the basis of one of these grounds. In this context, it is difficult to see how DND could be expected to make a

---

[4] Para. 12 of the Directive.
[5] Para. 13. d. 3. of CDS Directive 02 on CAF COVID-19 Vaccination – Implementation of Accommodations and Administrative Action – Amendment 1
[6] Ibid., para. 13. d. 4.
[7] Ibid., para. 13. d. 5.
[8] *Canadian Human Rights Act* (R.S.C., 1985, c. H-6), ss. 7, 10, 15.

decision about an accommodation request without obtaining additional information about the nature of the CAF member's circumstances.

23. On 11 October 2022, the CDS issued CDS Directive 003 on CAF COVID-19 Vaccination for Operations and Readiness, which superseded the previous CDS Directives on CAF COVID-19 Vaccination. While this directive provided certain conditions under which CAF members would not need to be fully vaccinated against COVID-19 (i.e. where vaccination is not required for operational readiness reasons), it retained the requirement that all CAF members would need to attest to their COVID-19 vaccination status.

24. Based on the above, we conclude that the collections required under the Directive related directly to existing programs or activities, that being: (i) ensure the health and safety of the CAF members and civilian employees in the workplace; and, (ii) to ensure the operational readiness posture of the CAF. We found no instances of collections that were not directly related to implementing the Directive. Therefore, we find the allegations with respect to this issue to be **not well-founded**.

Issue 2: Was the use of the personal information collected under the Directive authorized under section 7 of the Act?

25. Some complainants alleged that DND's use of information relating to their vaccination status, for the purpose of making a decision on the application of administrative consequences for unvaccinated individuals, was inappropriate.

26. Section 7 of the Act establishes the conditions under which information, collected by institutions, can be used. Specifically, subsection 7 (a) establishes that information can be used "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose."

27. As identified earlier in this report, we accept that the purpose of collecting the vaccination status of CAF members relates directly to the responsibilities of DND to ensure the health and safety of CAF members and DND civilian employees in the workplace and to ensure the operational readiness posture of the CAF.

28. When connecting to Monitor MASS, users were presented with a screen informing them that:

    - "The purpose for collection and use of this information is to fulfill the responsibility of your supervisor to ensure the health and safety [of] CAF members. This is a requirement under the DM/CDS Directive – CAF COVID-19 Vaccination Policy."

- "The personal information collected will be used to confirm your vaccination status and to consider request for accommodation for those unable to be vaccinated. The personal information will be used, in conjunction with additional COVID-19 preventative measures, including rapid testing, to determine if you will be granted on-site access to the workplace and to determine whether you may report to work in person or remotely. Your personal information will also be used by your organization to monitor and report on the overall impact of COVID-19 and compliance with the vaccination policy"; and,

- "Refusal to provide the requested information will result in administrative consequences such as CAF members being restricted in their employment until they are fully compliant."

29. We did not encounter any evidence substantiating that DND's use of the information collected was inconsistent with the purposes listed above; and, as such, we conclude that DND used the information for the purposes for which it was collected or in a manner consistent with those purposes. Accordingly, we find the allegations with respect to this issue **not well-founded**.

Issue 3: Did the use of Monitor MASS for collection and storage of CAF members' vaccination status result in unauthorized disclosure of information?

30. Many complainants alleged that the access controls in Monitor MASS are insufficient and that, as a result, their information was at risk of inappropriate disclosure to other members of their units who had no requirement for access to such information.

31. Subsection 8 (1) of the Act requires that personal information under the control of an institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with the conditions identified in subsection 8 (2). Paragraph 8 (2) (a) allows for disclosure "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose".

32. The Monitor MASS User Guide[9] states that, "Monitor MASS (Military Administration Support System or MM) is an application used for operational human resource management in real time, which assists the Chain of Command (CoC) in the daily management of their personnel. Monitor Mass gathers information from different systems that affect the daily employment of the soldiers within a unit." The User Guide

[9] MCS Pers (Monitor MASS) User Guide, Version 5.2.3 by Military Command Software Centre, CA/DLCI 3-4 (Director Land Command Information), National Defence.

also specifies that Monitor MASS is authorized for storage and processing of information up to the Protected B level (i.e. information whose unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, e.g. to individuals or businesses).

33. Monitor MASS is used by DND to collect and store COVID-19 vaccination status attestations from CAF members. Members are required to log into the system and input their vaccination status.

34. Details of a CAF member's COVID-19 vaccination status can be viewed by individuals within the member's chain-of-command (i.e. supervisors / managers) at the unit who have the "View Sensitive Data" privilege enabled for their account in Monitor MASS.

35. In our discussions with members of the Military Command Software Centre ("MCSC"), which is the team responsible for developing, managing and maintaining the Monitor MASS application for DND, we were informed that privilege management (including the ability to access sensitive data about CAF members) is typically delegated to the unit level and such decisions are the responsibility of the unit Commanding Officer ("CO"), or Officer in Charge (OC - for smaller/subordinate CAF units). Privileges at the unit level are implemented by the unit's Monitor MASS administrator on behalf of the CO/OC. As such, privilege management is significantly decentralized in Monitor MASS.

36. Members of the MCSC indicated to us that this decentralized approach is by intent and that it enables individual units to determine which roles and permissions to assign to their members in a way that best meets the unit's individual circumstances. We accept that, to a certain extent, individual units will have differing needs depending on that nature of the unit's role, composition and the environment or command under which they exist (e.g. Canadian Army, Royal Canadian Navy, Royal Canadian Airforce, Special Operations Command); and that such needs may change over time depending on the unit's deployment status and staffing levels.

37. We believe however that it is prudent in such a decentralized model to ensure that robust central audit and oversight activities are in place to validate that individual units and commands are properly exercising their responsibilities to grant permissions and revoke them when individuals move on or when the permissions are otherwise no longer required.

38. DND advised us in their representations that on 12 January 2022, the Senior Officer responsible for the MCSC emailed a communiqué to command and unit Monitor MASS administrators reminding them of the need to use Monitor MASS' data access/privacy controls to support their unit's "functional requirements and to ensure appropriate protection of privacy controlled data". The communiqué also reminded administrators of the need to "ensure that governance policies are in place with one or more appointed Administrators in Monitor MASS who have a high level of understanding of the roles

when providing permissions." Finally, units were advised to "conduct a review of the 'View Sensitive Data' privilege for each member to ensure access to information is an essential requirement in the performance of their duties."

39. While we view the direction in the communiqué as appropriate under the circumstances, we did not find any evidence that MCSC followed up with Monitor MASS administrators to validate that they had taken action, nor was there any evidence that MCSC had collected any metrics to determine the extent to which this action was implemented and effective. As such, from a management perspective, it is unclear whether the communiqué achieved its intended outcomes.

40. Given the decentralized access control / privilege management model in use for Monitor MASS, and in consideration of the sensitivity of the information stored in Monitor MASS (including members' COVID-19 vaccination status), we recommended that DND / CAF establish measures to periodically validate that: (i) individual commands and units have implemented and maintain appropriate governance policies for permissions management within the units; and, (ii) units are regularly reviewing 'View Sensitive Data' privileges assigned to members within the unit as well as for those transferring out of the unit. This will help to support CAF members' privacy and maintain the "need-to-know" principle.

41. DND declined to implement our recommendation. DND has responded to our recommendation indicating that in their view the measures that are in place 'provide sufficient assurance that access controls are managed and monitored and that the management of personal information within Monitor MASS respects the privacy rights of CAF members.' We do not feel that the measures described by DND provide sufficient assurance that privileges allocated at the unit level in Monitor Mass are implemented in accordance with DND's direction; and we are not confident that these privileges are being appropriately monitored and controlled by DND. As such, we feel that this remains a risk to the privacy of CAF members. We urge DND to implement the recommendation.

42. We did not find any evidence, nor was there any specific examples raised, of actual inappropriate disclosures of CAF members' COVID-19 vaccination status through Monitor MASS. Therefore, we find the allegations relating to insufficient access controls in Monitor MASS leading to inappropriate disclosures is **not well-founded**.

Issue 4: Did DND take reasonable steps to ensure that personal information that was used for determining the COVID-19 vaccination status of CAF members was accurate?

43. Some complainants allege that they declined to submit a vaccination status attestation in the form and manner specified by DND / CAF, or that they declined to submit a vaccination status attestation altogether; and that, as a result, their vaccination status in Monitor MASS was set to indicate that they were "unvaccinated". They allege that this

resulted in the collection, retention and use of inaccurate data about the members. They further allege that, as a result, DND / CAF used inaccurate information in making decisions relating to the application of administrative consequences.

44. Subsection 6 (2) of the Act requires that institutions take all reasonable steps to ensure that any personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

45. It appears that CAF members were reasonably informed of the manner and process to follow to set their own vaccination status in Monitor MASS. DND / CAF communicated to CAF members, via the CDS directives, the process to follow as well as the possible vaccination statuses, and their meanings. Members were also provided the necessary tools to ensure that their status was properly and accurately entered into Monitor MASS. Even if members had no personal access to Monitor MASS on their own, DND / CAF provided an alternative method in the way of a paper form that the complainants in this matter could have used to communicate their correct vaccination status to their supervisor.

46. Individuals who were unwilling to attest to their vaccination status were required to select "unvaccinated" in Monitor MASS, when in fact this may not have been a true representation of their status. However, Monitor MASS also included a "reason" field which would permit those individuals to indicate that they were "[u]nwilling to share vaccination status".

47. Although subsection 6(2) of the *Privacy Act* has not attracted a large volume of jurisprudence, a comparable provision in Alberta's *Health Information Act* (R.S.A. 2000 c. H-5, s. 61) has been interpreted as requiring that sufficiently accurate "for the purpose for which it will be used or disclosed."[10]

48. In practice, the coding applied (i.e. "Unvaccinated" rather than only indicating that the individual is unwilling to attest) does not appear to have affected the decision-making process in the sense that both those who are unwilling to be vaccinated and those unwilling to attest were subject to the same administrative consequences. Additionally, the "reason" field did provide a further clarification to enable an accurate representation of members' vaccination status.

49. Notwithstanding the decision-making neutrality of the coding, it would have been optimal, and more clear, to provide employees the ability to select a field indicating "unwilling to attest", thus avoiding any ensuing confusion.

---

[10] *Alberta Health Services (Re)*, 2021 CanLII 16364 (AB OIPC) at para. 82.

50. Based on this, we have determined that DND / CAF did take reasonable steps to ensure that the complainants' vaccination status were accurate, up-to-date and complete. As such we find the allegations relating to this issue **not well-founded**.

Other

Was the information collected necessary and proportional?

51. Our office also considered the necessity and proportionality of the vaccine mandates and the vaccination attestation measures put in place by federal institutions during the COVID-19 pandemic. Given that DND/CAF and other federal separate employers were asked to align with TBS's Policy, our analysis here focuses largely on any significant differences between the necessity and proportionality for the CAF and the core public administration.

52. To guide institutions in considering necessity and proportionality, our Office advocates a four-part test[11] that calls for institutions to ask themselves the following questions when establishing particularly privacy-invasive programs and services:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?
    - Is there a less privacy-intrusive way of achieving the same end?
    - Is the loss of privacy proportional to the need?

53. With respect to the first point of the four-part test, necessity, we have considered that the requirements were instituted during the global COVID-19 pandemic which represented an exceptional set of circumstances to which the Government of Canada and the CAF, more specifically, had to respond. We are satisfied that the measures mandated under the CDS Directive were connected to the pressing and substantial goals of ensuring the health and safety of CAF members in the workplace and maintaining the operational capability and deployability of the Canadian Armed Forces. DND further explained in their representations to our office that vaccination was also intended to help mitigate the risk of transmission of the virus to vulnerable groups that the CAF was called upon to serve in the context of the pandemic.

54. With respect to the second part of the test, DND provided evidence that the CDS Directive was based on public health advice from the Public Health Agency of Canada

[11] Described in Expectations: OPC's Guide to the Privacy Impact Assessment Process by the Office of the Privacy Commissioner of Canada.

and scientific studies; and aligned with the requirements established in TBS's Policy for the core public administration. Based on the information provided by DND as well as our analysis in the context of our investigation of the requirements established for employees of the core public administration, we are satisfied that a vaccination mandate was effective in meeting the objectives; and, that the collection of information relating to members' vaccination status to implement this mandate was therefore effective in meeting the objectives that were established under the CDS Directive.

55. With respect to the third element of the test, the necessity and proportionality principle requires a consideration of whether less privacy-intrusive measures could achieve the same end. This element requires DND to demonstrate that less privacy-intrusive measures would not have been able to achieve their important objectives of protecting the health and safety of its employees. We were not provided with any significant information that DND had considered any potential less intrusive alternatives (such as rapid testing). However, we are satisfied, as with our investigation relating to the core public administration, that other alternatives, including rapid tests, would not have been as effective in the circumstances to ensure that individuals who attended onsite workplaces were protected from COVID-19.

56. As detailed in our report of findings in relation to vaccination attestation requirements for the core public administration, we received analysis from the Public Health Agency of Canada, supported by references to external evidence, demonstrating that at the time DND/ CAF put the CDS Directive in place there was a substantial body of evidence on the efficacy of vaccines for protecting individuals coming into contact with others, such as in a shared workspace, from severe illness. As in our report of findings in relation to vaccination attestation requirements for the core public administration, we accept that vaccination was demonstrated, at that time, to be the most effective means to ensure that individuals who attended onsite workplaces were protected from COVID-19.

57. However, we also noted that Court and tribunal decisions that have considered vaccine requirements to date have emphasized the importance of assessing the relevant operating context, including whether employees work onsite or from home.[12]

58. In fact, we acknowledge that CAF members could, at any time, be required to be present on-site on an ad hoc basis for operational needs; and that the CAF, in particular, may be

---

[12] See for example, *Lavergne-Poitras v. Canada (Attorney General)*, 2021 FC 1232 (CanLII) at paras. 69, 73-74, and 101); *Toronto District School Board v. CUPE, Local 4400*, 2022 CanLII 22110 (ON LA); *Maple Leaf Foods Inc., Brantford Facility v. United Food and Commercial Workers Canada, Local 175*, 2022 CanLII 28285 (CanLII) paras. 28-31; *BC Hydro and Power Authority v. International Brotherhood of Electrical Workers, Local 258*, 2022 CanLII 25764 (BC LA) at paras. 65-68; *BC Hydro and Power Authority and Powertech Labs Inc. v. MOVEUP (Canadian Office & Professional Employees' Union Local 378*, 2022 CanLII 91093 (BC LA) at paras. 51-59; *Toronto Professional Fire Fighters' Association, I.A.A.F. Local 3888 v. Toronto (City)*, 2022 CanLII 78809 at paras. 237, 261.

called upon to rapidly deploy domestically and internationally in response to threats, emergencies and disasters into jurisdictions that may have differing requirements for COVID-19 vaccination. We accept that it is not possible to know with certainty in advance when the CAF may be called upon to deploy, although there are individuals and units that are on heightened states of readiness.[13] We also acknowledge that bringing unvaccinated individuals up to full vaccination status is not something that can be done quickly on an 'as-needed' basis. As such, given the pandemic conditions at the time, we find that it was reasonable for DND/CAF to require that all members either become fully vaccinated or request an accommodation from the requirements of the CDS Directive. Additionally, we accept that in order to know which personnel are deployable that collecting the vaccination status for all members was, and remains, a reasonable and effective approach for DND/CAF.

59. With respect to the fourth part of the four-part test: is the loss of privacy proportional to the need, we would expect DND to be able to demonstrate that the potential privacy impacts to CAF members, resulting from the collection of information relating to their COVID vaccination status, were proportional to the benefits that would result from the collection.

60. The CDS Directive required the disclosure of limited information about CAF members' vaccination status, information that at the time the CDS Directive was first instituted, was also required to be disclosed to access many services in a number of provinces, including restaurants. In fact, the CAF did collect this information prior to the COVID-19 pandemic in relation to members' vaccination status against other illnesses. Nevertheless, it remains medical information (sensitive by nature) and in certain cases could entail the disclosure of additional sensitive personal information for employees making accommodations requests. This loss of privacy must be measured against the benefits of the CDS Directive.

61. For the reasons set out in the assessment of the first and third elements, we are satisfied that the benefits of the CDS Directive included: to ensure that the CAF remained prepared and resourced to meet operational imperatives; to protect the health and safety of the Defence Team; and to mitigate the risk of transmission of the virus to vulnerable groups that the CAF could be, and were, called upon to serve in the context of the global pandemic.

---

[13] Along similar lines, in the labour arbitration context, in *Toronto Professional Fire Fighters' Association, I.A.A.F. Local 3888 v. Toronto (City)*, at para. 237, supra note 12, the Arbitrator took note of the inherently unpredictable work environment for firefighters, and the need to deploy with little notice, and potential come into close contact with members of the public. This can be comparable to the work environment of the CAF.

62. When measured against these objectives, we find that the loss of privacy was proportional to the benefits in the context of this emergency situation.

63. Based on the evidence and representations before us, we are satisfied that the CDS Directive addressed the necessity and proportionality requirements.

Conclusion

64. We conclude that the CDS directives were implemented in conformity with the legal requirements of the Act. The complaints examined in this report are therefore **not well-founded**.

65. We did however recommend that DND/CAF implement measures to periodically validate that units properly review and revoke permissions that provide access to CAF members' sensitive information in Monitor MASS. DND declined to implement this recommendation. We urge DND to do so.

Appendix 1 - Listing of vaccination attestation information collected by respondents

DND has indicated that the following vaccination attestation-related information is collected in Monitor MASS:

- CAF member's name
- CAF member's service number
- Attestation:
    - Fully vaccinated (date – second dose)
    - Partially vaccinated (date – first dose)
    - Unvaccinated requesting accommodation due to:
        - A certified medical contraindication or disability;
        - A religious belief that prohibits full vaccination; or
        - An inability to be vaccinated based on a ground of discrimination under the Canadian Human Rights Act.
    - Unvaccinated:
        - Unwilling to share vaccination status;
        - Unwilling to be vaccinated;
        - Unwilling to comply with the CDS Vaccination Directive (policy); or
        - Accommodation request denied.
    - Attestation not completed
        - Reason – LWOP (leave without pay)/MATA/PATA (maternity/parental leave)/ Release/Unreachable.

Investigation into COVID-19 vaccination attestation requirements established by certain separate employers of the federal public service

Complaints under the *Privacy Act*

May 29, 2023

Description

We examined whether the vaccination attestation requirements established by certain federal government institutions ("separate employers") that are not part of the core public administration, for their employees, in response to the COVID-19 pandemic complied with the collection, use, and disclosure provisions of the *Privacy Act* (the Act). Additionally, we examined the necessity and proportionality of the measures considering the circumstances under which they were established.

Takeaways

- The separate employers examined had the authority to collect information on employees' COVID-19 vaccination status under their enabling legislation and Part II of the Canada Labour Code; and uses and disclosures of such information were generally consistent with the purposes for which it was collected.
- Though the principle of necessity and proportionality is not currently a requirement of the Privacy Act, limiting the collection of personal information to what is demonstrably necessary is a requirement of the Treasury Board of Canada Secretariat's (TBS) Directive on Privacy Practices. In this case we found that the collection of personal information under the measures implemented by these institutions was necessary, effective, and proportional, under the circumstances.
- Institutions should assess and document necessity and proportionality in a structured way when introducing or modifying privacy-invasive programs, in order to provide confidence that the privacy interests of Canadians are being respected.
- When setting access permissions for sensitive employee information institutions should consider what types of information constitute a "need to know" requirement for any given support employee with access.

Report of findings

Table of contents

Overview

1. Following the introduction, in October of 2021, of COVID-19 vaccination mandates and associated vaccination status attestation requirements for employees of separate employers[1] in the federal public service, our office received multiple complaints from affected employees against Business Development Bank of Canada ("BDC"), Canada Post Corporation ("CPC"), Canada Revenue Agency ("CRA"), Canadian Food Inspection Agency ("CFIA"), National Research Council of Canada ("NRC"), and Parks Canada ("PC"), collectively referred to as "the respondents" or "the employers" in this report.

2. Our office also received complaints against the Treasury Board of Canada Secretariat ("TBS") and institutions of the core public administration by employees who are subject to TBS's Policy on COVID-19 Vaccination for the Core Public Administration Including the Royal Canadian Mounted Police ("TBS's Policy") as well as complaints against the Department of National Defence by members of the Canadian Armed Forces (CAF), who are not subject to TBS's Policy but are subject to a similar directive, the CDS Directive on CAF COVID-19 Vaccination. Those complaints are addressed in separate reports.

3. Several complainants alleged that the collection of employees' vaccination status, and in some cases religious or medical information in support of an accommodation request to be exempted from the requirements of their employer's policies, was unreasonable. After investigation and analysis, we found that the respondents' collection of personal information, under their respective policies, complied with the requirement of section 4 of the Privacy Act (the "Act") as it relates directly to the respondents' operating programs or activities, namely, their workplace health and safety responsibilities during a national emergency situation as a result of the COVID-19 pandemic. Our investigation did not assess whether the vaccination requirements were an unjustified infringement of individuals' right to be secure against unreasonable search or seizure, guaranteed by the Canadian Charter of Rights and Freedoms.

4. Certain complainants also alleged that the respondents inappropriately disclosed personal information relating to their vaccination status. We determined that disclosures of this information by the respondents were consistent with the purposes for which it had been collected and, as such, complied with section 8 of the Act.

5. Based on the above, we concluded that the respondents' COVID-19 policies were implemented in conformity with the legal requirements of the Act.

---

[1] In the context of this report, the term "separate employers" is used to refer to Canadian federal public institutions that are not named in Schedule I or Schedule IV of the Financial Administration Act ("the FAA").

6. Additionally, although not a requirement under the Act, we also examined the principles of necessity and proportionality as they pertain to the collections established under the respondents' policies. We determined that, in the context of the global COVID-19 pandemic, these policies were, overall, necessary and proportional given the emergency situation that existed. Federal employers have clear obligations under the Canada Labour Code to protect the health and safety of their employees in the workplace and we are satisfied that, based on the conditions and public health guidance at the time, vaccination and the associated attestation requirements were the most effective method to prevent infection and serious disease from COVID-19 in order to ensure the health and safety of employees and the individuals they serve.

7. As such, we are satisfied that the respondents' policies addressed the necessity and proportionality principles in the context of the global COVID-19 pandemic. However we did recommend that all institutions undertake a structured analysis of necessity and proportionality when implementing or modifying potentially privacy-invasive programs. All respondents agreed to this recommendation.

Background

8. On 6 October 2021, the Government of Canada announced that all public servants in the core public administration would need to attest to being fully vaccinated against COVID-19 or be put on leave without pay unless accommodated for medical reasons or on the basis of a prohibited grounds of discrimination. These requirements were formalized for employees of the core public administration under the TBS's Policy.

9. Separate employers within the federal public service, were asked to implement substantially similar policies for their employees. As a result, these separate employers established their own policy direction for their employees that reflected similar objectives and established vaccination requirements consistent with those of the core public administration, including requirements for attestation by employees of their COVID-19 vaccination status.

10. The respondents established the following policy instruments to formalize COVID-19 vaccination requirements for their employees:

    a. BDC: BDC Vaccination Directive

    b. CPC: CPC Mandatory Vaccination Practice

    c. CRA: Policy on COVID-19 Vaccination for the Canada Revenue Agency

    d. CFIA: Policy on COVID-19 Vaccination for the Canadian Food Inspection Agency

    e. NRC: Policy on COVID-19 Vaccination for the National Research Council

    f. PC: Policy on COVID-19 Vaccination for the Parks Canada Agency

11. Following the announcement of COVID-19 vaccination requirements for employees of separate employers, we received complaints from affected employees against the respondents. Our examination of these complaints and their associated allegations establishes the basis for this report of findings.

Jurisdiction

12. Several complainants alleged that requiring vaccination and attestation of vaccination status constituted a contravention of their rights guaranteed by the *Canadian Charter of Rights and Freedoms* ("the Charter"), and that therefore the requirements were unlawful. However, making findings on Charter compliance is outside of the scope of our Office's jurisdiction and thus outside the scope of this report's analysis.

Methodology

13. Our office investigated the allegations against each institution individually and obtained representations from each institution. Based on these discrete investigations, our office believes that the complaints relating to separate employers have issues in common and are most effectively addressed in a single report rather than separate reports for each respondent.

14. Given that separate employers were asked to align with the requirements of TBS's Policy and that, as such, the policy largely informed the broad requirements of their related policies, we have relied additionally upon TBS's representations in relation to TBS's Policy. We refer readers to the Report of Findings for our Investigation into COVID-19 vaccination attestation requirements established by the Treasury Board of Canada for employees of the core public administration for additional background and context.

Analysis

Issue 1: Was the information collected by the respondents related directly to an operating program or activity of the institution as required by the Act?

15. Many of the complainants allege that their employers required them to provide, on a mandatory basis, personal information relating to their COVID-19 vaccination status and, in certain cases in order to obtain an accommodation from these requirements, information about their religious beliefs or medical history. These complainants allege that this collection is being done without proper authority and that it represents an unreasonable infringement of their privacy rights.

16. A listing of the information for COVID-19 vaccination attestations collected by respondents can be found in Appendix 1 of this report.

17. Section 4 of the Act requires that institutions only collect personal information about individuals if that information relates directly to an operating program or activity of the institution. These programs or activities are normally established through legislation which authorizes the program or activity in question. Section 4 does not require that a collection be "necessary", just that there be "a direct, immediate relationship with no intermediary between the information collected and the operating programs or activities of the government."[2]

18. While certain complainants alleged that their vaccination status was being collected without their consent, it should be noted that the Act does not include a general requirement that institutions obtain individuals' consent for the collection of their personal information.

19. All respondents referred, either in their written responses to our Office or in their policies, to Part II of the Canada Labour Code ("the Code") which establishes occupational health and safety requirements for employers in federally regulated workplaces to prevent or limit workplace-related accidents and injuries, including those that could result from occupational diseases such as exposure to COVID-19, in the workplace. Employers establish occupational health and safety programs to oversee and implement their obligations under Part II of the Code.

20. In the context of the global COVID-19 pandemic, we accept that the collection of information relating to employees' COVID-19 vaccination status reasonably relates to the employers' occupational health and safety programs because it allows the employers to understand which employees are protected against severe outcomes resulting from potential exposure to the virus. Additionally, this information informs the employer about which employees are available to attend the workplace, if required.

21. Employers are also required to accommodate employees who cannot be vaccinated due to a medical contraindication, religious ground, or any other prohibited ground of discrimination as defined in the Canadian Human Rights Act ("CHRA"). To that end, employers request information from their employees about the nature of the grounds under which the employee is requesting an accommodation in order to make decisions about granting accommodations and to determine accommodation measures.

22. Collecting personal information to evaluate a request for accommodation is directly related to a government institution's responsibilities under the CHRA to avoid discriminating against employees based on prohibited grounds of discrimination.[3] There is an immediate and direct relationship between this responsibility and collecting

---

[2] Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN) v. Canada (Attorney General), 2016 FC 1289 at para. 141, aff'd 2019 FCA 212.

[3] *Canadian Human Rights Act* (R.S.C., 1985, c. H-6), ss. 7, 10, 15.

information from employees to justify their request for accommodation on the basis of one of these grounds. In this context, it is difficult to see how employers could be expected to make a decision about an accommodation request without obtaining additional information about the nature of the employee's circumstances.

23. In addition to the authorities and responsibilities described above, many respondents have certain specific authorities for the establishment of conditions of work, which may include the collection of personal information relating to individuals' COVID-19 vaccination status.

24. BDC is governed by the *Business Development Bank of Canada Act*. Section 10 of this act authorizes BDC to employ officers and employees and to "fix the terms and conditions of their employment or hiring."

25. CPC indicated in their representations to our office that they establish conditions of work for employees under section 12 of the *Canada Post Corporation Act*, which authorizes CPC to "fix the terms and conditions of their employment or engagement, as the case may be".

26. CRA indicated that it has the authority to determine "the terms and conditions of employment of persons employed by the Agency" under paragraph 30(1)(d) and to "determine and regulate the pay to which persons employed by the Agency are entitled for services rendered, the hours of work and leave of those persons and any related matters" under paragraph 51(1)(i) of the *Canada Revenue Agency Act*.

27. Subsections 13(1) and (2) of the *Canadian Food Inspection Agency Act* provide the President of CFIA with the power to "[a]ppoint the employees of the agency", and to "set the terms and conditions of employment for employees of the Agency and assign duties to them."

28. NRC has the authority to employ individuals under subsections 5(1)(b), 5(1)(g), and 5(1)(h) of the *National Research Council Act*. NRC also referred us to section 8 of the NRC Act which establishes that "[t]he President is the chief executive officer of the Council and has supervision over and direction of the work of the Council and of the officers, technical and otherwise, appointed for the purpose of carrying on the work of the Council." NRC further specified in their representations that the President of the National Research Council "has overall responsibility for the work of the NRC, as a separate agency. Terms and conditions of employment apply to members. With the NRC being a separate employer, the President is responsible for the proper management of the terms and conditions of employment."

29. The Chief Executive Officer of PC has the authority under paragraph 13(3)(b) of the *Parks Canada Agency Act* to, "set the terms and conditions of employment, including termination of employment for cause, for employees and assign duties to them".

30. Based on the above, we are satisfied that the information collected by the respondents relates directly to an operating program or activity as is required under section 4 of the

Act. Specifically, we accept that the information was collected in support of the respondents' occupational health and safety programs. We are also satisfied that respondents did have sufficient authority to establish these collections as a condition of employment. Accordingly, we find the allegations with respect to inappropriate collection of information relating to employees' vaccination status, including information in support of requests for accommodation, to be **not well-founded**.

Issue 2: Were uses and disclosures of information relating to employee vaccination status and requests for accommodation authorized under sections 7 and 8 of the Act?

31. Section 7 of the Act requires that personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or for a purpose for which the information may be disclosed to the institution under subsection 8(2).

32. Subsection 8(1) of the Act requires that personal information under the control of an institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with the conditions identified in subsection 8(2). Paragraph 8(2)(a) allows for disclosure "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose".

33. Certain complainants alleged that there had been inappropriate uses or disclosures of information collected under institutions' policies resulting from the use of systems to collect, process and monitor employee vaccination attestations. We examined whether institutions had taken appropriate steps to limit use and disclosure of the information in these systems for purposes authorized under section 7 and 8. We also examined specifically, for those institutions using the Government of Canada Vaccination Attestation Tracking System ("GC-VATS"), whether the use of GC-VATS may have resulted in inappropriate disclosures of information either within individuals' own institution or to staff at TBS as the operator of the GC-VATS system. We did not find any use or disclosure contraventions associated with the general handling of vaccination attestation information, accommodation requests or the use of GC-VATS by separate employers.

34. We separately investigated complaints of a breach of employees' COVID-19 vaccination status information, relating to CPC, where such information was disclosed to other employees of CPC, in error, for which there was no authorized purpose under section 8 of the Act.

35. We obtained, from all respondents, representations describing how they collect information relating to their employees' vaccination status, with specific attention to the safeguards (including access restrictions and related safeguards) implemented to protect the information collected.

GC-VATS (used by CFIA and PC)

36. Both CFIA and PC used TBS's GC-VATS to collect vaccination attestations from their employees. Access to individual employee data within GC-VATS is restricted to authorized individuals within the employee's own institution. Specifically, an employee's immediate supervisors have full access to the individual employee's vaccination attestation, including: (i) vaccination status as attested to by the individual employee, (ii) the result of a verification as recorded by the individual employee's immediate supervisor, and (iii) the reason for accommodations if/as requested by the individual employee. Higher-order managers (i.e. superiors to the employee's immediate supervisor, including all senior officials within the organizational structure in which the employee works) have access only to: (i) the individual employee's vaccination status as attested to by the individual employee and (ii) the result of a verification as recorded by the individual employee's immediate supervisor.

37. Certain other specific individuals within an employee's own institution with a role in fulfilling responsibilities under the policy (i.e. health and safety officials or human resources staff) who have been pre-identified as having a "need to know" also have access via GC-VATS to individual employees' attestation data through departmental reporting.

38. TBS has indicated to us, in the context of our investigation into vaccination attestation requirements in the core public administration, that specific individuals at TBS do have access to anonymized vaccination attestation data aggregated at a departmental-level via GC-VATS for the purposes of statistical analysis and reporting. According to TBS, these individuals do not have access to individuals' personal information through this reporting mechanism. We do note that aggregated and deidentified data can sometimes be considered personally identifiable information. We did not examine whether this was the case here, as ultimately the uses were determined to be consistent with the collection.

39. TBS has also indicated that certain specific individuals within the technical team supporting the GC-VATS solution may be given access to the underlying GC-VATS data for the purposes of diagnosing reported technical defects in order to support the proper functioning of the solution.

40. We find that the uses and disclosures described above, relating to the use of GC-VATS, are consistent with the purpose for which the information was collected, specifically, to implement COVID-19 vaccination mandates and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under section 7 and paragraph 8(2)(a) of the Act.

BDC

41. BDC collected vaccination attestations using its Workday Human Capital Management System (Workday). BDC informed us that Workday is BDC's system of record for all

information related to its human resources and that it had created a specific “Vaccination Covid-19 module” within Workday to collect and store the information collected as part of their vaccination status attestation process. Access to vaccination attestation information in Workday is restricted using role-based access controls and only employees added to specific “need-to-know” groups have access to information in the Vaccination Covid-19 module.

42. BDC has indicated that access to the information provided by employees as part of the vaccination status attestation is limited to employee members of the following groups:

    a. HR Employee Relations

    b. HR Business Partners

    c. Workday system access control (i.e. those who assign access rights in Workday)

43. BDC did not explain specifically why the groups indicated above needed access to this information. However, we accept that BDC has flexibility to determine which individuals within the institution require access to this information to support the implementation of BDC’s Vaccination Directive, and that the stated roles above are inherently related to that supporting function.

44. We find that the information sharing described above, relating to individuals’ vaccination status within BDC, are consistent with the purpose for which the information was collected, specifically, to implement BDC’s Vaccination Directive and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraphs 7(a), and 8(2)(a) of the Act.

CPC

45. CPC used a combination of methods to collect vaccination attestations from employees. A phone-based system (“1-800-attestation line”) was used for most employees, as well as a digital attestation portal for deaf and hard of hearing employees. CPC provided representations identifying that several groups within CPC have access to information relating to employee vaccination status. This access is based on a determination by CPC of the internal program areas that need access to the information in order to properly administer the CPC’s Mandatory Vaccination Practice (CPC MVP).

    a. Team leaders have access only to ‘Compliant’ or ‘Non-Compliant’ status for individuals within the team leader’s organization to verify compliance with the CPC MVP. The details of how employees are, or are not, compliant are not accessible to these individuals.

    b. Certain members of the Human Resources team have access to ‘Compliant’ or ‘Non-Compliant’ status at the national level for the purposes of establishing new hire and staffing processes in respect of individuals’ compliance to the CPC MVP. The details of how employees are, or are not, compliant are not accessible to these individuals.

c. Certain members of CPC's Production Control and Reporting ("PC&R") team have access to 'Compliant' or 'Non-Compliant' status at the national level to prepare operations reporting and impact analysis. The details of how employees are, or are not, compliant are not accessible to these individuals.

d. Certain members of the Security & Investigation Services ("S&IS") team have access to data on non-compliant employees in order to manage access to CPC facilities.

e. Certain members of the Business Analytics team have full access to all information collected in order to manage and support the attestation reporting data with employee information. CPC did not specify why full access, rather than more limited access or use of aggregated data was needed for these individuals.

f. Certain members of the National Health and Safety Compliance and Policy team have full access to all information collected in order to monitor compliance with the CPC MVP across CPC.

g. Certain members of the National Disability Management team have access to all information collected in order to process requests for medical accommodations from employees who cannot be vaccinated and for preparing relevant reports. CPC did not specify why access to "all information collected" was needed or whether this access was limited to information of individuals who had requested an accommodation under medical grounds.

h. Certain members of the Human Rights team have access to all information collected in order to process accommodation requests under religious or other human rights grounds from the employees who cannot be vaccinated, and for preparing relevant reports. CPC did not specify why access to "all information collected" was needed or whether this access was limited to information of individuals who had requested an accommodation on religious or other human rights grounds.

i. Certain members of the Safety Audit and Compliance team have access to information on the employees randomly selected for audits only, which may include proof of vaccination records.

46. We find that the information sharing described above, relating to individuals' vaccination status within CPC, are consistent with the purpose for which the information was collected, specifically, to implement the CPC MVP and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraph 7(a) and 8(2)(a) of the Act.

47. Notwithstanding the above, given the breadth of support units to which access was provided, we are concerned as to why full access (i.e. "all information collected") was given to each authorized member within the units. We recommended that in such circumstances consideration be given as to what types of information constitute a "need

to know" requirement for any given support employee with access. CPC has agreed to this recommendation.

CRA

48. CRA collected employee vaccination status attestations using an attestation solution that is hosted in its Corporate Administration Systems ("CAS"). CAS is used for collecting and storing employee administrative information such as staffing information, leave information, performance evaluations, etc. CRA has indicated that the attestation solution is authorized to operate at the Protected B level, having gone through a security assessment and authorization process in accordance with CRA and TBS security policies.

49. CRA explained in its written representations that the attestation solution in CAS uses organizational structure information to restrict access to view the employee's attestation to only the employee, the employee's direct supervisor, and that supervisor's direct manager.

50. CRA has also indicated that the attestation solution allows certain individuals, who have defined roles, to view this information for reporting or system administration purposes. These roles are restricted to only a few employees who are responsible for providing people management data in the Agency. CRA has established an approval process wherein justification for this access is needed to assign new individuals to these roles.

51. CRA has further explained that Agency-level centralized reporting for the purposes of policy and program oversight is limited to de-identified, statistical data and that data suppression techniques are applied to data required for basic monitoring.

52. For employees who were unable to record their attestation in CAS, CRA required that those employees complete a manual attestation form (in PDF format) and send it by encrypted email to a generic inbox managed by a limited number of employees in the Labour Relations ("LR") program. Once received, those LR employees recorded the attestation into CAS for the employee and stored the PDF form in a folder of the generic inbox to limit access.

53. We find that the information sharing described above, relating to individuals' vaccination status within CRA, are consistent with the purpose for which the information was collected, specifically, to implement the Policy on COVID-19 Vaccination for the Canada Revenue Agency and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraphs 7(a) and 8(2)(a) of the Act.

CFIA

54. In addition to the disclosures listed above relating CFIA's use of GC-VATS, CFIA also explained that, for employees who do not have access to GC-VATS, the attestation was documented via paper form and sent by the employee's manager to an email account

with restricted access. The information was then recorded in an Excel document and loaded into CFIA's Records, Document and Information Management System ("RDIMS"), with access limited to those involved in the tracking/reporting of compliance to CFIA's Policy on COVID-19 Vaccination for the Canadian Food Inspection Agency.

55. Data stored in CFIA's RDIMS system (which is authorized for storing information up to the Protected B level) is restricted to a limited number of CFIA's HR representatives who are directly involved in the monitoring of compliance to CFIA's policy, as well as those required to take actions based on the attestation status of individuals. CFIA has indicated that the full list of employee attestations is limited to the small HR team involved in monitoring compliance to CFIA's policy as a whole, with specific portions of the data being provided only on an "as required basis" to specific users (i.e. human resources professionals directly involved in the implementation of the Policy on COVID-19 Vaccination for the Canadian Food Inspection Agency).

56. CFIA identified three specific lists that were collated based on employee attestations and shared in support of the implementation of their policy:

    a. A list of partially vaccinated employees and employees requesting accommodation was shared with the HR Professionals responsible for distribution of rapid-testing kits;

    b. A list of employees who were not in compliance with the policy was provided to select pay and labour relations specialists in human resources to facilitate the placement of these employees on administrative leave without pay; and,

    c. A list of employees randomly selected for verification of their attestation was provided to an HR team of three people involved in roll out of the attestation verification process.

57. We find that the information sharing described above, relating to individuals' vaccination status within CFIA, are consistent with the purpose for which the information was collected, specifically, to implement the Policy on COVID-19 Vaccination for the Canadian Food Inspection Agency and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraph 7(a) and 8(2)(a) of the Act.

NRC

58. NRC collected vaccination attestations from their employees using NRC-VATS, which is based on TBS's GC-VATS application but is a separate application implementation by NRC.

59. NRC has indicated that access to personal data collected in NRC-VATS has been limited to those individuals needing the information to fulfill an administrative purpose related to the implementation of NRC's Policy on COVID-19 Vaccination for the National

Research Council. NRC has identified the following roles and access privileges in NRC-VATS:

a. An “Individual (employee)” is able to access their attestation as well as their employee attestation and accommodation review. Individuals can input and view their own information to verify that it is up-to-date and that it accurately reflects their vaccination status. The individual is able to revise their own information if it is not correct (i.e. up-to-date).

b. An “Approving Director” has team-level access. Approving Directors can view the attestation details of only their team members. They are able to document accommodations proposed for individual staff members.

c. An “HR Administrator” has an all staff-level of access. HR Administrators can view all NRC employee attestations and accommodations by type. Full access is provided for statistical and policy-related reporting purposes; as well as for trouble-shooting purposes to resolve issues and questions.

d. A “System Administrator” has system-level of access. System Administrators have access to the database via the server log-in. Full access is required to maintain system operations and troubleshoot as needed to assist with any technical issues.

60. NRC has also indicated that statistical, non-personal information from NRC-VATS was shared outside of NRC, to TBS and to Innovation, Science and Economic Development Canada (“ISED”) for policy reporting purposes. NRC did not specify how this information was determined to be, or rendered, “non-personal”.

61. NRC has further explained that a paper-based form was made available to NRC employees who were not willing to provide their attestation in NRC-VATS, as an alternate means for collecting their vaccination status attestations. After the forms were filled-in to collect the information required under their policy, the completed forms are stored by NRC Human Resources in accordance with NRC’s information management and security protocols.

62. We find that the information sharing described above, relating to individuals’ vaccination status within NRC and the sharing of statistical information about vaccination rates for NRC’s employees with TBS and ISED, are consistent with the purpose for which the information was collected. The information was disclosed to implement the Policy on COVID-19 Vaccination for the National Research Council and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraphs 7(a) and 8(2)(a) of the Act.

PC

63. In addition to the uses and disclosures listed above relating PC’s use of GC-VATS, PC also explained that because some PC employees did not have access to GC-VATS that

electronic or paper forms were used to collect vaccination attestations. These could be submitted electronically via email or via letter mail.

64. Forms that were completed digitally or scanned after completion were to be submitted to a generic email account to which access was limited to certain members of PC's Corporate Labour Relations Team. Once the digital form was processed, they were placed in PC's GC DOCS (i.e. electronic records) repository where only three members of the Labour Relations Team had access.

65. Paper forms that were mailed into PC, were opened and processed by only one employee and placed in confidential boxes provided by PC's secure storage facility service provider in a locked room to which no other people have access. Similarly, for paper forms that were submitted digitally, any printed copies were filed in the same central location and shipped to PC's secure storage facility.

66. We find that the uses and disclosures described above, relating to individuals' vaccination status within PC, are consistent with the purpose for which the information was collected, specifically, to implement the Policy on COVID-19 Vaccination for the Parks Canada Agency and obtain vaccination attestations from employees in support of workplace health and safety; and they are therefore permitted under paragraphs 7(a) and 8(2)(a) of the Act.

Accommodation Requests

67. Several complainants raised general concerns that unreasonable disclosures of their personal information within their institution could have occurred in the process reviewing accommodation requests. We consequently obtained representations from all respondents describing what measures, if any, were taken to limit access to, and disclosure of, accommodation-related information to those who needed to know in order to manage the accommodation processes. We saw no indications of issues with respect to processes and systems to prevent inappropriate disclosures associated with the general handling of accommodation requests.

68. Several complainants also raised a concern that their colleagues, or other employees, such as those managing pay, could infer information about them, such as their vaccination status, from the fact that they were put on leave. However, as noted above, the Privacy Act permits disclosures "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose". In our view, the fact that an individual is on leave, which can occur for a variety of reasons, is information obtained or compiled for the purpose of managing the employee and their work. Therefore, proactive disclosure to relevant employees – such as those processing pay, or colleagues whose workload may be affected – that an individual is on leave is a consistent use with this original purpose and permitted under 8(2)(a) of the Act.

69. Given that the uses and disclosures described above are for the purpose for which the information was obtained, i.e. to implement COVID-19 vaccination mandates and obtain vaccination attestations from employees in support of workplace health and safety, or for

consistent uses with those purposes, we found no indications of contraventions of section 7 or 8 of the Act. Accordingly, we find the allegations with respect to the unauthorized use and disclosure of information relating to employees' vaccination status, including information in support of accommodation requests, to be **not well-founded**.

Other

Was the information collected necessary and proportional?

70. Our office also considered the necessity and proportionality of the vaccine mandates and the vaccination attestation measures put in place by federal institutions during the COVID-19 pandemic. Given that separate employers were asked to align with TBS's Policy, our analysis here focuses largely on any significant differences between the necessity and proportionality for the employers and the core public administration.

71. To guide institutions in considering necessity and proportionality, our Office advocates a four-part test[4] that calls for institutions to ask themselves the following questions when establishing particularly privacy-invasive programs and services:

    - Is the measure demonstrably necessary to meet a specific need?
    - Is it likely to be effective in meeting that need?
    - Is there a less privacy-intrusive way of achieving the same end?
    - Is the loss of privacy proportional to the need?

72. The respondents did not provide evidence that they had performed a structured analysis of the necessity and proportionality of their vaccine mandates and related vaccination status attestation measures prior to implementation. We do, however, acknowledge that separate employers were asked by the Government of Canada to align with TBS's Policy and, as such, did benefit from the examination of public health guidance and studies that informed TBS's implementation of that policy.

73. With respect to the first point of the four-part test, necessity, we have considered that the requirements were instituted during the global COVID-19 pandemic which represented an exceptional set of circumstances to which the Government of Canada, including separate employers, had to respond. All respondents identified that they had responsibilities under the *Canada Labour Code* to prevent or limit workplace-related accidents and injuries, including those that could result from COVID-19 infection. We are satisfied that the measures mandated under the respondents' policies were connected

[4] Described in Expectations: OPC's Guide to the Privacy Impact Assessment Process by the Office of the Privacy Commissioner of Canada.

to the pressing and substantial goals of ensuring the health and safety of employees in the workplace; and, as such, were connected to the respondents' occupational health and safety programs. Additionally, respondents indicated that all employees could potentially be required to attend the workplace onsite on an ad-hoc basis in response to operational needs.

74. With respect to the second part of the test, all respondents indicated that they were following public health measures or advice from public health agencies. CRA, CFIA and NRC further specified that they also consulted guidance[5] from Health Canada's Public Service Occupational Health Program. In our analysis of this matter, given that separate employers were asked to align to TBS's Policy, we have additionally referred to the evidence we received from TBS in the context of our investigation of vaccination attestation requirements for the core public administration. Based on that information, which demonstrated the effectiveness of vaccines in preventing severe illness, hospitalization and death from COVID-19, we are satisfied that there was evidence of the effectiveness of vaccination in ensuring the health and safety of employees in the workplace at the time the vaccination mandates and attestation requirements were put in place in the fall of 2021. We accept, on this basis, that a vaccination mandate was effective in meeting the objectives of promoting workplace health and safety; and, that the collection of vaccination status to implement this mandate was therefore also effective in meeting those objectives. Additionally, the collection of vaccination status information from employees would be an effective means to determine which employees would be available to attend on-site at the workplace should the need arise.

75. With respect to the third element of the test, the necessity and proportionality principle requires a consideration of whether less privacy-intrusive measures could achieve the same end. This element requires institutions to demonstrate that less privacy-intrusive measures would not have been able to achieve their important objectives of protecting the health and safety of their employees. We were not provided with any significant information that the respondents had considered any potentially less intrusive alternatives (such as rapid testing). However, we are satisfied that vaccination was the most effective means available to ensure that individuals who attended onsite workplaces were protected from COVID-19.

76. We received analysis developed by the Public Health Agency of Canada, supported by references to external evidence, demonstrating that at the time Government of Canada announced its plans for introducing vaccination mandates that there was a substantial body of evidence on the efficacy of vaccines for protecting individuals coming into contact with others, such as in a shared workspace, from severe illness.

77. Conversely there was relatively limited evidence of the effectiveness of potential alternative measures, including rapid testing, in protecting individuals from severe illness

[5] Public Service Occupational Health Program COVID-19 Guidance by Health Canada Public Service Occupational Health Program.

resulting from COVID-19. In reviewing Canadian jurisprudence on mandatory vaccination policies we found a number of cases that[6] have considered public health advice with respect to rapid testing as an alternative to mandatory vaccine mandates. These cases dealt with situations where affected individuals are largely required to be in shared physical spaces. The decision makers in these cases upheld mandatory vaccination policies that did not permit individuals to freely choose rapid testing as an alternative, citing relevant public health advice. These decisions cited provincial medical authorities in two cases, and expert epidemiological testimony in the another two. These sources noted that: (i) in contrast with the strong body of evidence for the protective effect of vaccines, there is a lack of concrete evidence, such as observational studies or controlled trials, demonstrating that rapid testing regimes reduce transmission, and (ii) rapid testing regimes do not prevent serious illness from infection where such infections occur.

78. While we accept that vaccines are effective in this context, we also noted that Court and tribunal decisions that have considered vaccine requirements to date, have emphasized the importance of assessing the relevant operating context, including whether employees work onsite or from home.[7]

79. Respondents advanced arguments that all employees, including those working full-time from home, needed to be available to attend at the office on short notice, for example, to participate in ad-hoc on-site meetings, to access sensitive material, or because of IT support requirements.

80. While we would have expected more fulsome and forthcoming responses from respondents with respect to our questions on this issue, we are of the view that some deference is owed to employers with respect to their assessment of their needs for employee onsite presence during this unprecedented public health emergency. We accept that, should the need indeed arise for onsite presence, that the time needed for

---

[6] See for example, Canada Post Corporation v. Canadian Union of Postal Workers, Award N00-20-00008, April 27, 2022 at para. 95; BC Hydro and Power Authority v International Brotherhood of Electrical Workers, Local 258, 2022 CanLII 25764 (BC LA) at para. 61; Toronto District School Board v. CUPE, Local 4400, 2022 CanLII 22110 (ON LA); Amalgamated Transit Union, Local 113 v. Toronto Transit Commission, 2021 ONSC 768 (CanLII) at paras. 99-109; Costa, Love, Badowich and Mandekic v. Seneca College of, 2022 ONSC 5111 (CanLII) at para. 109; Elementary Teachers' Federation of Ontario v. Ottawa-Carleton District School Board, 2022 CanLII 53799 (ON LA) at paras. 49-50; Toronto Professional Fire Fighters' Association, I.A.F.F. Local 3888 v. Toronto (City), 2022 CanLII 78809 (ON LA) at paras. 235-244.

[7] See for example, Lavergne-Poitras v. Canada (Attorney General), 2021 FC 1232 (CanLII) at paras. 69, 73-74, and 101); Toronto District School Board v. CUPE, Local 4400, 2022 CanLII 22110 (ON LA); Maple Leaf Foods Inc., Brantford Facility v. United Food and Commercial Workers Canada, Local 175, 2022 CanLII 28285 (CanLII) paras. 28-31; BC Hydro and Power Authority v. International Brotherhood of Electrical Workers, Local 258, 2022 CanLII 25764 (BC LA) at paras. 65-68; BC Hydro and Power Authority and Powertech Labs Inc. v. MOVEUP (Canadian Office & Professional Employees' Union Local 378, 2022 CanLII 91093 (BC LA) at paras. 51-59; Toronto Professional Fire Fighters' Association, I.A.A.F. Local 3888 v. Toronto (City), 2022 CanLII 78809 at paras. 237, 261.

an unvaccinated employee to become fully vaccinated could be problematic for operational purposes. We also accept, based on this, that employers do need to know which employees are, at any given time, available to attend on site – and that this would likely necessitate collecting the vaccination status of all employees. For these reasons we accept that it was reasonable, under the circumstances, to require all employees to attest to their vaccination status.

81. With respect to the fourth part of the four-part test: is the loss of privacy proportional to the need, we had expected that the respondents would be able to demonstrate that they had analyzed whether the potential privacy impacts to employees resulting from the collection of information relating to their COVID vaccination status were proportional to the benefits that would result from the collection but we received little evidence from any of the respondents demonstrating that they undertook a structured proportionality assessment.

82. It should be noted that the respondents' policies required the disclosure of limited information about an individual's vaccination status, information that at the time these measures were first instituted, was also required to be disclosed to access many services in a number of provinces, including restaurants. Nevertheless, it remains medical information (sensitive by nature) and in certain cases could entail the disclosure of additional sensitive personal information for employees making accommodations requests.

83. This loss of privacy must be measured against the benefits of the measures. For the reasons set out in the assessment of the third element, we are satisfied that the benefits of these measures were to protect the health and safety of the respondents' employees while ensuring that the respondents retained the ability and flexibility to require the onsite presence of its teleworking employees to respond to emergencies or for other compelling reasons.

84. When measured against this objective, we find that the loss of privacy was proportional to the benefits in the context of this emergency situation.

85. Based on the evidence and representations before us, we are satisfied that the vaccination attestation measures implemented by the respondents reasonably addressed the principles of necessity and proportionality.

86. We did however recommend that, in the future, all institutions explicitly consider necessity and proportionality in a structured way[8] when introducing or modifying privacy-invasive programs, in order to provide confidence that the privacy interests of Canadians, in this case their employees, are being respected. We were pleased that all respondents in this report have agreed to this recommendation.

---

[8] For example, as described in Expectations: OPC's Guide to the Privacy Impact Assessment Process.

Conclusion

87. We conclude that the respondents' requirements relating to vaccination attestation by their employees were implemented in conformity with the legal requirements of the Act. The complaints examined in this report are therefore **not well-founded**.

88. We did however recommend to CPC that when granting access to sensitive personal information to all members within units, that consideration be given as to what types of information constitute a "need to know" requirement for any given support employee with access. CPC has agreed to this recommendation.

89. We also recommended that all institutions explicitly consider necessity and proportionality in a structured way when introducing or modifying privacy-invasive programs. All respondents agreed to this recommendation.

Appendix 1 - Listing of vaccination attestation information collected by respondents

GC-VATS (used by CFIA and PC)

GC-VATS is prepopulated with the following information on individuals which was already collected by the employer:

- Last name
- Given name
- Manager's Name
- Department
- Place of work (country)
- Place of work (province or territory)
- Group
- Level
- Position number
- PRI (paper attestations only)
- Email address
- Date of Birth (paper attestations only)
- Manager's PRI (paper attestations only)
- Manager's DOB (paper attestations only)

Additionally, GC-VATS collects the following the specific information from individuals as part of the attestation process:

- Employee acceptance
- Attestation of vaccination status
- Verification status
- Manager's verification confirmation

BDC

BDC collected the following information via their "Vaccination Covid-19 module" in Workday:

- Vaccination Status (options: “Fully Vaccinated”, “Partially vaccinated” or “Unvaccinated”)
- Date of last dosage, if fully or partially vaccinated
- Intention of getting an additional dose if partially vaccinated (options: “Yes” or “No”)
- Date of additional dose
- Reason for accommodations

CPC

CPC collected the following information through the 1-800-attestation line:

- Employee ID and year of birth (for authentication)
- Vaccination status, where options were:
    - Fully vaccinated;
    - Partially vaccinated;
    - Unable to be vaccinated due to medical reason;
    - Unable to be vaccinated due to religious or other grounds; or,
    - Unwilling to be vaccinated

CPC initially collected the following information through the digital attestation portal for deaf and hard of hearing employees:

- Vaccination status, where options were:
    - fully vaccinated, with attested dates and brand(s) of vaccines
    - partially vaccinated, with attested date and brand of vaccine
    - unvaccinated, and if intended to be or not (until February 3, 2022)

As of February 3, 2022, the available selections via the digital attestation portal are identical to those in the 1-800 attestation line.

CFIA

See information collected in GC-VATS (used by CFIA and PC), above.

CRA

The following related tombstone data was already being collected in CAS:

- Name
- PRI
- Manager's name

Employees were required to select their vaccination status from the following options and, based on their status, make additional selections as follows:

- Fully Vaccinated
    - Enter dates of vaccination
- Partially Vaccinated
    - Enter dates of vaccination
- Unvaccinated – Request Accommodation
    - Due to a medical contraindication – Requires written documentation from the employee's treating medical physician or nurse practitioner indicating the grounds for not receiving or delaying the COVID-19 vaccine.
    - Under grounds of discrimination
    - Religion – Requires a sworn affidavit signed before a commissioner for taking affidavits, providing information about the sincere religious belief that prohibits full vaccination.
    - Other (Canadian Human Rights Act) – Requires specific information for the reason that the employee is unable to be vaccinated
- Unvaccinated – Unwilling

NRC

The following information was collected via NRC-VATS

- Employment Status (continuing vs non-salaried worker)
- Vaccination Status for COVID-19
- Date received first vaccine (COVID-19)
- Accommodation Requested-medical
- Accommodation Requested-religious

- Accommodation Requested-other prohibited grounds
- Accommodation Decision (Approved / Denied) for the individual
- Accommodation Proposed (Telework / Regular Testing) for the individual
- Individual's Acceptance / Rejection of Proposed Accommodation
- Individual's Response Submitted to NRC-VATS
- Individual's compliance / non-compliance with rule 4.3.2 of the Policy
- Individual's non-compliance with the Policy, as defined in section 6.1

PC

See information collected in GC-VATS (used by CFIA and PC), above.

Erroneous quarantine notifications from ArriveCAN

Complaint under the *Privacy Act*

May 29, 2023

Description

Beginning June 28th, 2022, approximately 10,200 Apple device users received erroneous notifications from the ArriveCAN application, instructing them to quarantine under emergency measures imposed during the COVID-19 pandemic. These notifications were due to a defect in ArriveCAN version 3.0 not detected prior to release which generated inaccurate information about affected travellers' quarantine exemption status. Due to the design of the system, the inaccuracies were not corrected by screening officers at the border. The defect was fixed three weeks later, and affected individuals were notified a week after that. We determined that the Canada Border Services Agency (CBSA) did not take all reasonable steps to ensure the accuracy of the personal information it used for an administrative purpose, as required by subsection 6(2) of the Privacy Act (the Act). Despite our recommendation to CBSA to do so, it refused to correct the inaccurate and sensitive information it still holds for the affected travellers concerning quarantine status.

Takeaways

- The accuracy provision of the Act applies to information that institutions generate, produce or derive about an individual, including data produced through automated, algorithmic, actuarial or statistical processes.
- A high degree of due diligence is required under subsection 6(2) of the Act to ensure the accuracy of personal information when administrative decision using that information may have important consequences for individuals.
- To ensure the accuracy of information generated by automated processes, institutions are notably expected to implement, among other measures:
    - Rigorous pre-release testing for issues that could lead to the highest negative impacts on individuals.
    - Effective human intervention with respect to high impact decisions on individuals.
    - Effective and timely correction and recourse for individuals.

Report of findings

Table of contents

Overview

In the wake of the COVID-19 pandemic, 80 Emergency Orders issued by the Governor in Council pursuant to the *Quarantine Act* were in effect from February 3rd, 2020 to September 30th, 2022. The purpose of these Emergency Orders was to prevent the introduction and spread of COVID-19 in Canada, by subjecting travellers to certain requirements prior to and after entering Canada. To determine a given traveller's applicable entry requirements and to ensure that these requirements were being respected, the Canada Border Services Agency ("CBSA") and the Public Health Agency of Canada ("PHAC") collected personal information from individuals entering Canada, primarily through the ArriveCAN mobile application and web application ("ArriveCAN").

On June 28th, 2022, version 3.0 of ArriveCAN was released. An error in this version caused approximately 10,000 fully vaccinated Apple device users to receive erroneous messages to quarantine, despite respecting all the conditions of the quarantine exemption for fully vaccinated travellers. CBSA indicated that it identified the defect on July 14th, 2022 and resolved it on July 20th, 2022.

Given that the information and instructions generated by ArriveCAN were inaccurate for certain Apple device users, the complainant alleges that the CBSA had failed to take all reasonable steps to ensure that the personal information used to determine an individual's quarantine requirements was as accurate as possible.

Ultimately, we found that the CBSA did not meet the requirements of the *Privacy Act*, as it did not take all reasonable steps to ensure the accuracy of the information that it used for an administrative decision-making process. Accordingly, our Office finds that the CBSA failed to respect its obligations under subsection 6(2) of the *Privacy Act*, and this complaint is therefore **well-founded**.

After the error was detected, CBSA introduced expanded testing for ArriveCan releases and indicated that it will continue to adopt more nimble testing procedures for situations like the pandemic where the speed of changing business requirements and releases results in compressed testing timelines. CBSA disagreed with our finding that it failed to take all reasonable steps to ensure accuracy. It also refused to implement our recommendation to correct the inaccurate and sensitive information it holds for the affected travellers concerning quarantine status. We call on CBSA to reconsider its refusal to correct the erroneous data generated by the ArriveCan error and to put in place all necessary measures should it decide to proceed with similar tools in the future.

Background

1. From February 3rd, 2020[1] to September 30th, 2022[2], 80 emergency orders ("Emergency Orders" or "Orders") were in effect pursuant to section 58 of the *Quarantine Act*. The Emergency Orders were issued by the Governor in Council, on the recommendation of the Minister of Health, and imposed conditions on individuals entering Canada in order to reduce the risk of importing and spreading the coronavirus disease 2019 ("COVID-19").

2. The last Emergency Order[3], which was issued on June 25th , 2022 and in effect during the events in question, notably required:

    - **all individuals** to disclose information relating to their COVID-19 vaccination status[4] and other prescribed information through the ArriveCAN mobile application or web application ("ArriveCAN")[5];

    - individuals who **were not fully vaccinated** to submit themselves to pre-arrival[6], on-arrival and post-arrival[7] COVID-19 testing, as well as a 14-day quarantine[8]; and

    - individuals who **were fully vaccinated** to provide evidence of their COVID-19 vaccination ('proof of vaccination credential', 'vaccination credential', 'proof of vaccination'). Individuals who qualified as fully vaccinated were exempt from the 14-day quarantine.

3. Based on the information they submitted, ArriveCAN would determine whether incoming travellers were exempt from the obligation to quarantine. This determination relied on information provided directly from users (e.g., date of birth), as well as information generated automatically by ArriveCAN (e.g., validity of the proof of vaccination credential[9]). If ArriveCAN: (i) determined that a traveller **arriving by air** was required to quarantine, or (ii) was unsure whether they were exempt (e.g, if the authenticity of the proof of vaccination credential could not be verified), then the traveller's ArriveCAN submission would be

---

[1] *Minimizing the Risk of Exposure to 2019-nCoV Acute Respiratory Disease in Canada Order*, PC Number 2020-0059, issued February 3rd, 2020.
[2] *Government of Canada to remove COVID-19 border and travel measures effective October 1*, News release from Public Health Agency of Canada, issued September 26th, 2022.
[3] *Minimizing the Risk of Exposure to COVID-19 in Canada Order*, PC Number 2022-0836, issued June 25th, 2022.
[4] *Id.*, paragraph 20(2)(a).
[5] *Id.*, subsections 19(4) and 20(8), and section 23. Note: 'electronic means specified by the Minister of Health' refers to ArriveCAN.
[6] *Id.*, sections 11 to 13.
[7] *Id.*, section 15.
[8] *Id.*, sections 22 and 23.
[9] Note: For each proof of vaccination credential, an "ocr_result" would be produced based on the results of an optical character recognition scan for a fixed set of criteria (e.g., traveller's name, the name of an approved vaccine, etc.). For credentials with a quick response ("QR") code, a "qr_result" would also be generated based on ArriveCAN's ability to decrypt and validate the credential's 'payload' using the credential issuer's public key. These steps served to validate, to varying degrees of certainty, the authenticity of the vaccination credentials.

reviewed by a CBSA officer upon their arrival at the port of entry (e.g. an international airport). At **land** ports of entry (e.g., highway crossing along the Canada-US border), all ArriveCAN submissions were reviewed by a CBSA officer.

4. ArriveCAN submissions were accessible to CBSA officers through the "Contact Trace Desktop App", an information and case management system designed specifically for the administration of the Emergency Orders. After examining a traveller's submission, the CBSA officer would make changes to the traveller's file if warranted based on either their validation or rejection of the traveller's supporting documents (e.g., proof of vaccination credential, attestation of medical exemption). Post -entry requirements would then be communicated to the traveller. For example, if a traveller was not fully vaccinated or if their vaccination credential was rejected, a CBSA officer would instruct the traveller to test and to quarantine.

5. On June 28th, 2022, version 3.0 of ArriveCAN was released. In this iteration of the application, travellers using the iOS version of ArriveCAN (i.e., the version of ArriveCAN for Apple mobile devices) who had saved their submission form after selecting the travellers for the trip and who later returned to the form to complete the submission would incorrectly have their "quarantine_exempted" value set as 'false' by ArriveCAN. We note that this value was determined by the ArriveCAN application and was thus not a data field submitted directly by the user.

6. When entering Canada and having their ArriveCAN submission reviewed by a CBSA officer, travellers affected by this error would nevertheless appear as fully vaccinated and exempt from the quarantine requirements in the Contact Trace Desktop App. This was due to the fact that the Contact Trace Desktop App **did not** use the "quarantine_exempted" value from ArriveCAN, and instead conducted its own assessment of the traveller's post-entry requirements. Individuals affected by the error were therefore **not** instructed to quarantine by CBSA officers when crossing the border.

7. After entering into Canada, ArriveCAN would send automated notifications and emails to users whose "quarantine_exempted" value was set as false (i.e., all travellers affected by the error), instructing them to quarantine and to report on their health status, or else risk receiving fines of up to $5,000. Individuals who did not respond to these notifications could then receive compliance verification calls from PHAC representatives. These representatives would have believed that the affected individuals were required to quarantine, as the data transferred to PHAC included the erroneous "quarantine exempted" value.

8. Ultimately, the CBSA indicated it identified this error on July 14th, 2022, and released an update for ArriveCAN by July 20th, 2022[10] which no longer contained the defect.

[10] Note: Prior to July 20th, the Vancouver Sun news outlet reported on the glitch. A number of other news reports were then released after the error had been resolved.

9. Accordingly, from June 28th to July 20th, 2022, approximately 10,200[11] Apple device users received erroneous quarantine instructions directly from ArriveCAN (via an application notification) and from an email generated by ArriveCAN.

10. The CBSA has stated that, since before the error in question [12], fully vaccinated travellers who received erroneous notifications and who subsequently called the ArriveCAN or COVID-19 support lines for guidance were instructed to:

    - not respond to the notifications;
    - update ArriveCAN to the latest version; and
    - answer the compliance verification call they would receive and explain their situation to the public health officer[13].

11. PHAC advised impacted travellers by email on July 26th, 2022, and again on August 4th, 2022, to ignore the erroneous quarantine notifications they had received and confirmed that they were not actually required to quarantine.

Analysis

Issue: Did the CBSA take all reasonable steps to ensure that personal information used for an administrative decision was as accurate as possible?

12. The complainant has taken issue with the existence of the error caused by version 3.0 of ArriveCAN, and its significant impact on the rights of affected travellers, who were instructed to quarantine, prevented from filing any new ArriveCAN submissions[14] and who may have experienced heightened psychological stress from the ensuing confusion. The complainant states that the CBSA should have done more to prevent this situation from transpiring.

---

[11] For context, the CBSA noted that nearly 47 million travellers submitted their personal information in ArriveCAN from April of 2020 to September of 2022 to determine their quarantine requirements without incident.

[12] Version 3.0 of ArriveCAN was released on June 28th, 2022. Despite the CBSA only identifying the error on July 14th, 2022, ArriveCAN support staff had been providing the instructions listed in paragraph 10 since as early as May of 2022 to respond to user generated errors.

[13] Note: In a news article published on July 22nd, 2022, travellers affected by the error claimed that a PHAC enforcement officer had confirmed by phone that they were required to quarantine, despite being fully vaccinated. Our Office did not confirm the veracity of this account.

[14] Note: During the period ArriveCAN believed an individual was required to quarantine, that individual was unable to file a new ArriveCAN submission, which was mandatory for those entering into Canada. One news outlet reported on an individual residing in a border community who traveled frequently to and from Canada, and who was affected by the error. Given that the failure to make an ArriveCAN submission prior to arriving at the border would result in a $5,000 fine and that the error prevented affected travellers from creating new submissions, this individual chose to forgo their regular travel across the border.

13. Subsection 6(2) of the Act requires government institutions to take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

14. Section 3 of the Act defines:

    - '*personal information*' as information about an identifiable individual that is recorded in any form; and
    - '*administrative purpose*' as the use of personal information about an individual in a decision making process that directly affects that individual.

15. In *Ewert v. Canada*, 2018 SCC 30 ("*Ewert*"), the Supreme Court of Canada interpreted the accuracy requirement in subsection 24(1) of the *Corrections and Conditional Release Act* (S.C. 1992, c. 20) (CCRA), a provision nearly identical to subsection 6(2) of the *Privacy Act*[15], as applying not only to information gathering and record keeping, but also to tools which analyze collected information and which produce new information[16]. Furthermore, Alberta's Office of the Information and Privacy Commissioner recently applied *Ewert* to privacy legislation in *Edmonton Police Service (Re)*, 2021 CanLII 13336 (AB OIPC) at paragraphs 39-40.

16. Similarly, within the context of the *Privacy Act*, we consider subsection 6(2) to not only apply to information collected from an individual, but to information generated by an institution about an individual as well. This includes data produced through automated, algorithmic, actuarial or statistical processes, such as ArriveCAN's assessment of travellers' quarantine exemption status.

Sub-issue I: Is the information in question 'personal information used for an administrative purpose'?

17. The information identified as being erroneous was the "quarantine_exempted" data field in ArriveCAN, which was normally generated based on ArriveCAN's assessment and calculation of other data fields[17]. For example, if: (i) the traveller's proof of vaccination credential was found to be valid, (ii) the traveller benefitted from a medical exemption, or (iii) the traveller was a child accompanied by a fully vaccinated adult, then the "quarantine_exempted" value would be set to 'true', thereby indicating that the individual was exempt from the quarantine obligation. For individuals who were affected by the error, the "quarantine_exempted" data field was never properly calculated and was thus saved as its default value: 'false'.

---

[15] *Corrections and Conditional Release Act*, S.C. 1992, c. 20, subsection 24(1): "The Service shall take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible." For comparison, see *Privacy Act*, R.S.C. 1985, c. P-21, subsection 6(2): "A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."
[16] *Ewert v. Canada*, 2018 SCC 30, paragraph 42 and paragraph 45.
[17] Note: These 'other data fields' were the "proof_of_vaccine_final_decision", "medical_exempt_final_decision" and "child_with_fully_vaccinated_adult" data fields.

18. This data field constitutes personal information under the Act, as it relates to an identifiable individual and is recorded electronically within both ArriveCAN and the CBSA's information management system. We consider each traveller to be an identifiable individual as they must provide their full name, date of birth, email, phone number, quarantine location address, travel information (e.g., flight number), travel document ID (e.g., passport number) and proof of vaccination credential as part of their ArriveCAN submission, all of which can be used to deduce the traveller's identity.

19. CBSA asserted that it was collecting the information for PHAC's administrative use rather than its own use. We do not dispute that PHAC ultimately used the information in question for administrative purposes as well (for follow-up enforcement communications), but information can be used by multiple departments for their respective administrative purposes. Further, in our view, the erroneous information was clearly used by CBSA for an administrative purpose (i.e. a decision-making process directly affecting the individuals). Specifically, the information was used by the ArriveCan application, under CBSA's control, to "decide" to: (i) instruct the affected travelers to quarantine, via the notifications/emails the ArriveCan application automatically sent, and (ii) notify PHAC, for enforcement purposes, that the individuals were required to quarantine. These decisions, while unintended and at odds with decisions made by CBSA screening officers at the border, nonetheless directly affected the individuals.

20. For these reasons, we find that the data field affected by the error constituted personal information used for an administrative purpose by the CBSA, and that it was thus subject to the accuracy requirements prescribed by subsection 6(2) of the Act.

Sub-issue II: Did the CBSA take all reasonable steps to ensure that the information was as accurate, up-to-date and complete as possible?

21. Given the Emergency Orders' important consequences on the rights and mobility of incoming travelers, it is our view that a high degree of due diligence was required under subsection 6(2) of the Act to ensure the accuracy of the information that was contained in ArriveCAN and that was used in administrative decisions relating to the Orders.

22. There are a number of measures that have been prescribed by policy requirements or recommended as best practices in public guidance which are instructive in assessing what reasonable steps institutions are required to take to ensure the accuracy, currency and completeness of information generated by automated processes. These notably include:

    (i) passive oversight and monitoring of the system's results, particularly to detect anomalous outcomes[18];

---

[18] *Directive on Automated Decision Making*, Treasury Board of Canada Secretariat – Policies, directives, standards and guidelines, last modified June 28th , 2021, section 6.3.2 ; *Directive on Service and Digital*, Treasury Board of Canada Secretariat – Policies, directives, standards and guidelines, last modified May 6th, 2022, section 4.2.1.5; *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Elham Tabassi for the National Institute of Standards and Technology – U.S. Department of Commerce, NIST AI 100-1,

(ii) the possibility for human intervention[19];

(iii) opportunities for individuals to access the information used in decision making, and to contest/flag inaccurate information[20];

(iv) information/decision traceability, explainability and logging[21]; and

(v) testing and independent review of the system prior to implementation[22].

23. In their representations to our Office, the CBSA indicated that they took the following steps to ensure the accuracy of such information:

a) Individuals who were not definitively assessed by ArriveCAN as being exempt from the quarantine requirements were screened by a CBSA officer (i.e., a human intervener), who would review their ArriveCAN submission and verify whether the traveller was indeed required to quarantine;

b) The CBSA performed over 1,800 test cases for the version of ArriveCAN containing the defect (i.e., ArriveCAN v3.0, released on June 28th) prior to the version's release, in addition to over 2,700 regression test cases[23];

c) Fully vaccinated travellers who received erroneous notifications from ArriveCAN and who called the ArriveCAN or COVID-19 support lines for guidance were instructed to not respond to the notifications, to update ArriveCAN to its latest version and to explain their situation during compliance verification calls they would receive;

d) The CBSA had resolved the error by July 20th, 6 days after the date it indicated it discovered the error on July 14th, 2022; and

---

published January 26th, 2023, MEASURE 1.1, MEASURE 2.4, MEASURE 3.1, MEASURE 4.1, MEASURE 4.2, MANAGE 2.3 and MANAGE 4.1.

[19] *Directive on Automated Decision Making*, *supra* footnote 18, sections 6.3.3, 6.3.5, 6.3.6, and 6.3.9; *Directive on Privacy Practices*, Treasury Board of Canada Secretariat – Policies, directives, standards and guidelines, last modified June 18th, 2020, section 4.2.16.2; *AI RMF 1.0*, *supra* footnote 18, GOVERN 6.2, MAP 3.5, MANAGE 2.4 and MANAGE 4.1; *Recommendation of the Council on Artificial Intellingence* ("OECD AI"), Organisation for Economic Co-operation and Development, OECD/LEGAL/0449, adopted on May 21st, 2019, Principle 1.2.b).

[20] *Privacy Act*, R.S.C. 1985, c. P-21, section 12; *Directive on Automated Decision Making*, *supra* footnote 18, sections 6.3.6 and 6.4.1; *Directive on Privacy Practices*, *supra* footnote 19, sections 4.2.10.5 and 4.2.19; *Directive on Service and Digital*, *supra* footnote 18, sections 4.2.1.1 and 4.2.1.2; *AI RMF 1.0*, *supra* footnote 18, GOVERN 2.1, MEASURE 3.3, MANAGE 4.1, MANAGE 4.2 and MANAGE 4.3; *OECD AI*, *supra* footnote 19, Principle 1.3.iv.

[21] *Privacy Regulations*, SOR/83-508, section 4; *Directive on Automated Decision Making*, *supra* footnote 18, sections 6.2.3 and 6.2.8; *Directive on Privacy Practices*, *supra* footnote 19, section 4.2.17; *Directive on Service and Digital*, *supra* footnote 18, section 4.3.1.12; *AI RMF 1.0*, *supra* footnote 18, MEASURE 2.9, MEASURE 2.13, MEASURE 3.1 and MANAGE 4.1; *OECD AI*, *supra* footnote 19, Principles 1.3.iii. and 1.4.b).

[22] *Directive on Automated Decision Making*, *supra* footnote 18, sections 6.3.1 and 6.3.4; *AI RMF 1.0*, *supra* footnote 18, GOVERN 4.3, MEASURE 2.3 and MEASURE 2.5; *OECD AI*, *supra* footnote 19, Principle 1.4.a).

[23] Regression testing re-executes completed tests to ensure existing functionalities are not affected by new changes.

e) After resolving the error, emails were sent out to affected travellers on July 26th, 2022 and on August 4th, 2022, advising them that they were not required to quarantine and that they had been receiving notifications in error.

24. Notwithstanding the above, we find that the CBSA did not take the following reasonable steps, to ensure the accuracy of the information used by CBSA, via ArriveCAN, to make decisions affecting the individuals in question. Specifically these measures relate to: (i) rigorous pre-release testing for issues that could lead to the highest negative impacts on individual users; (ii) effective human intervention with respect to high impact decisions on individuals and (iii) effective and timely correction and recourse for individuals.

Rigorous pre-release testing for issues that could lead to the highest negative impacts on individual users

25. CBSA argued that "it is unfortunately not possible nor industry standard to identify all possible errors in advance of a release. Reasonableness cannot be equated to perfection." We agree. However, CBSA did not demonstrate that the conditions which triggered the error (i.e. using an apple device to return to complete a saved form after previously selecting the trip's travellers) were an unusual or unforeseeable edge case.

26. We would expect an institution making use of automated decision-making systems, even ones designed only to 'assist' human decision makers, would identify the types of erroneous outcomes that could cause the highest negative impact on affected individuals, and ensure rigorous testing for errors that could lead to those adverse outcomes.

27. CBSA also argued that the context of emergency response in which ArriveCAN app was developed and evolved over time should be acknowledged. Following its initial release, the CBSA indicated that it developed 177 subsequent ArriveCAN releases across three platforms over 2 ½ years as a result of constantly changing requirements under Emergency Orders issued under the *Quarantine Act* on a 30 or 60 day renewal cycle. CBSA indicated that it uses industry best practices with regards to system and application testing in its maintenance of over 180 IT systems, and that this testing regime includes extensive regression testing, automated testing so that more time can be dedicated to testing new features, and pair testing. However, it also stated that the need to respond to changing requirements above "forced compromises to established best practices under normal IT working conditions."

28. We appreciate that the onset of the COVID-19 pandemic resulted in exceptional work conditions on many fronts. However, the incident in question occurred well after the onset of the pandemic and more than two years after the launch of ArriveCan. While during the initial phase of a crisis, certain latitude might be reasonable, two years in, we would expect an institution operating a system relying on a software application to allocate adequate time and resources to test for high impact errors prior to release. CBSA did not indicate that any particular and pressing change requirement stemming from a recently issued Emergency Order led to the error in question. Further, the error did not appear to have occurred due to any change to vaccination requirements during the time period when version 3.0 was released.

29. Further, the risk that travellers could be erroneously notified through ArriveCan of a requirement to quarantine despite being fully vaccinated appears to have been a risk that CBSA had turned their minds to well before the release of version 3.0 of ArriveCan on June 28, 2022. Since at least April 27, 2022, on the "contact us" page that individuals receiving quarantine notifications were directed to in case of issues, CBSA included a form for users to complete if they were "experiencing technical or account and password issues with ArriveCAN [or] *receiving notifications from ArriveCAN to quarantine or report symptoms even though you qualified as fully vaccinated at the border*." [emphasis added]

30. In this context we remain of the view that CBSA did not take all the reasonable steps with respect to pre-release testing to prevent inaccurate personal information being used in decision-making affecting individuals.

31. In response to the error, the CBSA expanded its ArriveCAN testing to include:

    - an additional 100 regression test cases to detect issues with the 'save' feature of the ArriveCAN form;
    - automated regression test capability (i.e., executing regression tests automatically, using automation frameworks and software platforms with minimal human input);
    - scheduling and performing *ad hoc* test cases during each release (i.e., testing the live version of ArriveCAN post-release); and
    - increasing the number of tester resources.

    CBSA also indicated that it will continue to adopt more nimble testing procedures for exceptional circumstances like a pandemic where the speed of changing business requirements and releases result in compressed testing timelines.

Effective human intervention with respect to high impact decisions on individuals

32. We would expect that where a system relies on human-decision makers to make the final decisions on impactful 'adverse' decisions, that clear 'positive action' by an identifiable human decision-maker should be required to initiate any impacts flowing from that decision. In other words:

    a) the human decision-maker should take some positive action (selecting a digital option, signing a form, etc) to clearly indicate what their decision is;

    b) this should be accompanied by a record of what information the human decision maker relied on; and

    c) that 'positive action' should be the trigger to initiate any results flowing from the adverse decision. i.e. the system should be designed so the suggested decision by the automated system cannot trigger any adverse action 'by default'.

33. In this respect it is important to note that at the time of the incident the suite of tools and processes used to enforce the Emergency Orders, which included ArriveCan, was designed to include human decision-making in any case where an individual was required to quarantine. This was an important positive design feature. Having a human in the loop for

critical and impactful decisions – such as validating whether an individual has been correctly identified as needing to quarantine – can significantly reduce the risks associated with automated decision-making, including the risk that inaccuracies in personal information introduced via software errors are not caught and corrected.

34. This was highlighted in the Algorithmic Impact Assessment (AIA)[24] completed for ArriveCan in October of 2021 by PHAC which noted that "While decisions concerning eligibility to enter Canada and post-border public health requirements may be impactful, the impacts of ArriveCAN outputs aren't necessarily significant and can be considered reversible. For example, if ArriveCAN is unable to recognize a traveller's proof of vaccination, a border services officer will manually inspect the proof of vaccination and determine eligibility and post-border requirements accordingly. In this scenario, the impact of the platform's outputs is both reversible and brief in duration." This contributed to the AIA's conclusion that the impact of the automated decision-making in that case was only level 2 on a scale of 1 to 4.

35. However, in this case, several design choices meant that in the case of individuals affected by this error, the final decision (i.e. the one communicated to individuals and PHAC for follow-up enforcement) was *not* made by the CBSA screening officer. Specifically:

    a) First, while the ArriveCan application was used to direct individuals to a CBSA screening officer and subsequently to send quarantine notifications, the CBSA Officer reviewed travellers information (uploaded from ArriveCan) in a separate application: the ContactTrace Desktop application. This application did not display the field containing ArriveCan's erroneous conclusion that the affected travellers needed to quarantine.

    b) Second, and most critically, the information in the "quarantine exempt" field in ArriveCan (used to generate the erroneous quarantine notifications) was only updated in cases where the CBSA screening officer changed something visible to them in the ContactTrace application. This did not occur for affected travellers in this incident as the CBSA screening officers in question were unaware anything needed changing.

36. In our view, and particularly in light of the fact that CBSA had contemplated the risk of erroneous quarantine decisions being communicated by ArriveCan to individuals (see paragraph 29), CBSA did not take adequate steps to ensure the effectiveness of human intervention to confirm that these impactful decisions were made on the basis of accurate information. It should have ensured that the adverse decisions 'actioned' by ArriveCan (when it sent quarantine notifications to individuals and informed PHAC) were, *verifiably*, the decision of the human decision maker *in all cases*.

Effective and timely correction and recourse for individuals

37. We would expect that an institution relying on automated communications to convey impactful decisions with a potential immediate and prolonged prejudicial effect would have

[24] AIA is a mandatory risk assessment tool required by TBS's Directive on Automated Decision-Making, prior to the production of any Automated Decision System by federal government institutions.

in place robust mechanisms to: (i) monitor for potential errors, (ii) enable individuals to raise accuracy concerns and (iii) correct errors in a timely manner.

38. It is a positive remedial step that the erroneous notifications redirected individuals to an ArriveCan "contact us" page that included a range of contact options for individuals, including a 24/7 Service Canada phone line and a specific form to complete if individuals felt that they had been wrongly notified to quarantine despite being fully vaccinated. CBSA indicated that it was via these mechanisms that it ultimately detected and subsequently corrected the software error, and sent an email to all affected individuals on July 26.

39. However, despite these mechanisms being in place, according to CBSA it took more than two weeks to detect the error and more than three weeks to stop the error from affecting decision-making about new travellers. CBSA indicated that since May 2022 (i.e. well in advance of this incident), travellers who reached an agent through the phone lines above and complained that they had received an erroneous quarantine notification from ArriveCan despite being fully vaccinated, were instructed to ignore the notifications and explain their situation to the PHAC enforcement officer when the officer called. However, it took nearly a month until a correction was sent to all affected individuals. Further, CBSA has still not corrected the erroneous information in its own data holdings.

40. We acknowledge that the volume of travellers processed on any given day, and therefore the volume of individuals raising issues with ArriveCan through these mechanisms before and during the incident, was likely very high. CBSA also noted, and we accept, that as the error affected only 0.5% of all submissions received during the affected period, and given the shifting travel patterns at the time, passive monitoring of submissions would have been unlikely to detect the error in question. However, in our view, a significant (and presumably elevated) number of individuals complaining that ArriveCan had told them to quarantine despite them being fully vaccinated should have raised flags and been resolved in a matter of days not weeks given the high adverse impact on affected individuals. Further, we emphasize that this incident happened more than two years after the beginning of the pandemic and the introduction of ArriveCan, and we would therefore expect a commensurate level of resourcing and maturation of incident response mechanisms.

41. We therefore conclude that CBSA did not take all the reasonable steps to ensure that concerns raised by affected individuals about inaccurate information being used to make decisions, were actioned and corrected in timely way – commensurate to the adverse impact on already affected individuals and individuals who could become affected.

42. In conclusion, we find that the three issues identified above, individually and collectively, constitute a failure by CBSA to take all reasonable steps to ensure the accuracy of the information that it used in an administrative decision, and thereby contravene subsection 6(2) of the Act. We therefore find the complaint **well-founded**.

Recommendation

43. To address this contravention of the Act, we recommended that within six months of the issuances of this report, CBSA update inaccurate information (i.e., the "quarantine exempted" value) generated by the error for all individuals.

44. CBSA disagreed with our finding that it did not take all reasonable steps to ensure the accuracy of the information that it used in an administrative decision, as required by subsection 6(2) of the Act. Further, it informed our office of its refusal to implement the above recommendation, stating that the objective of correcting the erroneous information was not clear. Specifically, it noted that:

    a) the COVID-19 border measures had ended on October 1st, 2022;

    b) the information was no longer being used by the CBSA for any administrative purpose;

    c) the data would be automatically disposed of after the two-year retention period; and

    d) all affected individuals had already been notified of the error in July of 2022.

45. While we acknowledge that the CBSA does not intend to use the information in question, we would expect an institution to correct erroneous information that it holds, especially sensitive information with past and potential adverse impacts. Further, while left uncorrected, there is a risk that this erroneous information could be relied upon by PHAC and/or other government entities (if access were to be authorized), to inform trend analyses and future compliance and enforcement activities, such as the issuance of fines and the prosecution of offences under the *Quarantine Act*. In light of these circumstances, we urge the CBSA to collaborate with PHAC, and with any other external party to whom the ArriveCAN data was disclosed, to correct the erroneous information within six months.

Conclusion

46. We found that CBSA did not take all reasonable steps to ensure the accuracy of the information that it used in an administrative decision, as required by the accuracy provisions of subsection 6(2) of the Act.

47. After the error was detected, CBSA took certain positive remedial steps, including: (i) introducing expanded testing for ArriveCan releases and (ii) indicating that it will continue to adopt more nimble testing procedures for situations like the pandemic.

48. CBSA disagreed with our finding that it failed to take all reasonable steps to ensure accuracy. It also did not agree to implement our recommendation to correct the inaccurate information it holds for the affected travellers. We therefore find the complaint **well-founded** and not resolved.

49. We call on CBSA to reconsider its refusal to correct the erroneous data generated by the ArriveCan error and to put in place all necessary measures should it decide to proceed with similar tools in the future.

Investigation into the collection and use of de-identified mobility data in the course of the COVID-19 pandemic

Complaints under the *Privacy Act*

May 29, 2023

Description

The investigation examined whether mobility data collected and used by PHAC in its response to the pandemic contains personal information as defined under Section 3 of the Privacy Act (the Act). Specifically, whether PHAC and its data providers have implemented de-identification techniques and safeguards against re-identification that are deemed sufficient to reduce the risk of an individual being identified below the "serious possibility" threshold.

Takeaways

- Data de-identification and aggregation are two privacy-enhancing techniques that are useful for privacy protection if they reduce the risk of re-identification of individuals below acceptable thresholds.
- De-identification alone is generally insufficient to ensure data anonymization. It must be accompanied by additional safeguards against re-identification.
- Data aggregation must involve a sufficient number of individuals to reasonably reduce the risk of singling out individuals.
- Transparency about the purposes for which personal information is collected and used is crucial to maintaining trust between individuals and organizations that collect and use their data.

Report of findings

Table of contents

Overview

The Office of the Privacy Commissioner of Canada received 12 complaints under the Privacy Act (the "Act") against Public Health Agency of Canada ("PHAC") and Health Canada ("HC") regarding the collection and use of Canadians' mobility data, which is comprised of geolocation data collected over time and other associated information.

The complainants allege that PHAC secretly collected data on 33 million mobile devices during the COVID-19 pandemic, and that according to a request for proposal, published in December 2021, it planned to continue to collect Canadians' mobility data over the ensuing five years.

PHAC reported that it has effectively relied on mobility data of just under 14 million Canadians to gain insightful information and meaningful analysis on the movement of populations in Canada, which has assisted in tracking the spread of the COVID-19 virus and for planning, assessing and adjusting the government's response to the pandemic.

PHAC claimed that it relied only on de-identified and aggregated data and that it never collected or used any personal identifiable information and thus the Privacy Act does not apply.

Through our investigation, as a necessary analytical condition, we first examined whether mobility data collected and used by PHAC in its response to the pandemic contains personal information as defined under Section 3 of the Act. More specifically, we assessed whether there was a serious possibility, in the circumstances, that an individual could be identified using the mobility data, procured by PHAC, alone or in combination with other available information. Our investigation did not assess whether or not PHAC's data providers collected and used location data in compliance with privacy laws.

Following analyses of the representations received and review of information on this topic and the concept of identification, we have concluded that the combination of the de-identification measures and the safeguards against re-identification implemented by PHAC and its data providers has reduced the risk of identifying individuals below the "serious possibility" threshold. We therefore consider the complaints in this matter to be **not well-founded.**

Notwithstanding our investigation's conclusion that PHAC did not contravene the *Privacy Act* with regard to the collection and use of mobility data in the course of the COVID-19 pandemic, we have made a number of recommendations to PHAC in particular, with instructive relevance to all organizations that produce, use or procure de-identified information in the course of their activities. We are encouraged that PHAC has accepted our recommendations.

Background

1. On December 31, 2019, a novel coronavirus, COVID-19, was reported in Wuhan in the Chinese province of Hubei. COVID-19 is a very contagious virus that may cause severe and fatal respiratory illness. On March 11, 2020, the World Health Organization ("WHO") declared COVID-19 as a global pandemic.

2. According to health experts, the COVID-19 virus spreads mainly via inhalation of infectious respiratory droplets, known as aerosols, that are released by infected people who are in proximity. PHAC officials determined that gaining "mobility insights" on population movements, interactions and gatherings would assist in understanding how the virus may spread and proliferate.

3. Mobility insights are also useful in planning, monitoring, and refining/assessing the effectiveness of certain key measures that are implemented by health authorities to combat the pandemic (stay at home, quarantine, lockdowns, etc.). For example, the number of trips between cities is an indicator of how connected these cities are and therefore the likelihood that an outbreak in one will spread to the other.

4. Mobility insights collected by PHAC were derived from data that PHAC indicated was de-identified and aggregated information about the movements of individuals over time (mobility data). This information was deduced from location-data that is continuously produced by devices/equipment that are often at the same physical proximity as their users. The most common examples of these devices/equipment are cell phones and other devices with data plans.

5. PHAC, like certain of its international counterparts, collected mobility-data based insights in its response to the COVID-19 pandemic. To that end, it collected insights aggregated from two types of data streams:

    i. **Mobile cell-tower/operator data**, which comprises records created each time a mobile phone pings an operator's cell-tower. PHAC procured this type of data from the telecom operator TELUS and leveraged the data analytics expertise of the Communications Research Centre Canada ("CRC") who was processing TELUS Data to generate mobility reports to provide aggregated data and statistics to PHAC's scientists for analysis.
    ii. **Mobile geolocation data**, which is information about the geographic location transmitted by a mobile application installed on a mobile device, using the device's built-in GPS capabilities. PHAC acquired this category of data from a private company named BlueDot, which in turn procured it from two data providers: Pelmorex and Veraset. During the first months of pandemic, Health Canada set up the initial contract with BlueDot to assist PHAC which undertook the actual collection of data. The contract was subsequently transferred to PHAC and Health Canada was not involved in any other manner in this project.

6. TELUS informed the OPC of TELUS' "*Data for Good*" program and CRC informed our office about PHAC's intent to use data in a de-identified and aggregated form in Canada's response to the pandemic. OPC offered the services of its Business Advisory and Government Advisory directorates to review the technical means used to de-identify data and provide advice. CRC and TELUS did not follow up on OPC's offer.

7. PHAC's Privacy Management Division ("PMD") also conducted a privacy analysis on September 22, 2020, in order to identify any potential privacy risks associated with the use of TELUS mobility data and the publication of the derived insights. It concluded that the data that PHAC would be receiving from TELUS is not about identifiable individuals because of the de-identification and aggregation processes it would undergo and that therefore the Privacy Act does not apply. It subsequently entered into a contract with TELUS and BlueDot to procure de-identified aggregated mobility data that it used to derive insights on the movement of Canadians.

8. On December 17, 2021, a few months after the contract with TELUS had expired, PHAC published a Request For Proposal[1] ("RFP") to acquire mobile operator data to continue to leverage this category of data for mobility insights. Following the publication of the RFP[2] on public procurement website, media articles raised privacy concerns relating to the use of mobility data, and the OPC subsequently received 12 complaints.

9. On January 13, 2022, the Standing Committee on Access to Information, Privacy and Ethics ("ETHI") adopted a motion to undertake a study on the collection and use of mobility data by the Government of Canada. The ETHI Committee issued a corresponding report in May 2022 and recommended therein, amongst other things, that government agencies be transparent when they harness the potential of big data in their activities and that federal privacy laws be modernized to adequately address the use of de-identified and aggregated data.

Analysis

Issue: PHAC did not collect personal information as defined under the Act

10. Section 3 of the Privacy Act defines personal information as information "about" an "identifiable" individual.

11. In Gordon v. Canada (Health), 2008 FC 258, the Federal Court decided that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.[3]

---

[1] On January 31, 2022, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) called upon the government to suspend the Request For Proposal (RFP) to procure cellular data until it reports its findings and recommendations to the House.
[2] PHAC extended the closing date of the Request for Proposal (RFP), until February 18, 2022, at the request of a potential bidder due to the impact of the holiday season, and of the COVID-19 pandemic on their operating capacity. Given that there is no procedural mechanism to suspend an RFP, PHAC chose instead to let the RFP close and identified that it would not select a vendor until after the Standing Committee on Access to Information, Privacy and Ethics (ETHI) submitted its findings and recommendations
[3] See also the more recent case of *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*, 2019 FC 1279

12. Therefore, we considered the degree to which data collected by PHAC can be linked to identifiable individuals either directly or indirectly, through inference and/or in association with other data sources. For the reasons described below, we concluded that due to the de-identification of the data, and the suite of protections used in this case to reduce the risk of re-identification, there is no serious possibility that the information collected by PHAC, and CRC on its behalf, can identify any individual.

13. To that end, we examined each data stream separately and for each one, we analyzed both: (i) data that CRC, on PHAC's behalf, was able to access in the data providers' systems and (ii) data CRC and PHAC were able to download and store in their own systems. This segmentation was required because the degree of de-identification and safeguards against re-identification are different in each data stream and at each phase.

14. In our investigative analysis, we relied on: (i) representations received from PHAC, (ii) information and guidance on anonymization and (iii) the work of the ETHI Standing Committee. We also sought and received representations from TELUS, BlueDot and CRC as relevant third parties to the investigation.

De-identification and residual risk of re-identification

15. De-identification may encompass a residual risk of re-identification of individuals that depends on many factors. Such factors are either: (i) **intrinsic** to the data itself and the de-identification techniques; or (ii) **external** and depend on sub-factors including:

    - the availability of additional data that can be cross-checked with the de-identified data;
    - who has access to the dataset and for what purposes, their motivation to re-identify data and their knowledge that a specific individuals' information is included in the dataset; and
    - the expertise and the resources used in the re-identification process.

16. In fact, multiple studies and research have succeeded in re-identifying data sets that were publicly released in de-identified format. This includes the Netflix study[4] and the AOL data release [5].

17. In the Netflix study, researchers demonstrated that an adversary who has access to discrete information points about an individual can easily identify his/her records in the Netflix movie prize database which contained subscribers' movie rating. In the AOL search release example, it is demonstrated that simply removing users' identifiers may not be sufficient to properly anonymize data.

---

[4] Arvind Narayanan and Vitaly Shmatikov. 2008. Robust De-anonymization of Large Sparse Datasets.
[5] AOL search log release

18. Moreover, risk of re-identification is not a static consideration and may increase over time with the improvement of re-identification techniques and the availability of additional resources and data that may be linked to the de-identified dataset.

19. For the foregoing reasons, it remains a complex exercise to definitively quantify the risk of re-identification. Several examples in the literature propose calculation methods which are not deterministic but rather rely on probabilistic calculations, based on assumptions about several factors and the type of re-identification cyber-attack.

The *Privacy Act* does not include specific provisions on de-identified or anonymized data

20. The Privacy Act does not expressly address de-identified or anonymized data. Its provisions all apply equally to the collection, use and disclosure, by federal institutions subject to the Act, of any information that meets the test of being "personal information". Therefore, the first issue, in this case, is to determine whether PHAC (including CRC acting on its behalf), collected any information that meets this test for being 'personal information' described above. If it does, then it would be necessary to consider whether the collection and any subsequent use or disclosure were compliant with the provisions of the Privacy Act. If it does not meet the test for 'personal information' then the Privacy Act does not apply.

21. As a note, our office has called for legislative change to bring a more nuanced approach to the handling and governance of de-identified information to respect both the potentially privacy protective nature of using de-identified data, and the inherent risks of re-identification. Given the importance and instructive value, we have explored the related issues in more depth in the "Other" section of this report.

Does access to data at TELUS' system constitute 'collection' under the Act?

22. As a preliminary matter we considered what constitutes 'collection' for the purposes of the Act in this case. As noted in the background section, CRC, on behalf of PHAC, had access to view certain individual-level data on TELUS' system, but could only download aggregated data.

23. It is clear that when a copy of information is saved in the institution's information management systems (i.e. in emails in an employee's inbox, its document management system, in hard copy, etc.) the information has been 'collected'. Similarly, if information is saved on another platform, but in an account under the control of an employee of an institution acting in a professional capacity, it is clearly 'collected' by that institution. In a situation where an institution's employee, in the course of work, sees (or hears) information but does not retain a physical or virtual copy, it may be less clear if it is 'collected' by the institution. In the present case, PHAC and CRC officials accessed data from TELUS, but also recorded aggregated information resulting from their queries.

24. Even if information is seen but not collected, there may nevertheless be a subsequent 'use' of that information for the purposes of the Privacy Act. This can happen where information is simply reviewed – for instance, where an individual's ID is visually inspected to ensure they are 18 before allowing access to a space, or in this case, where individual level data is reviewed to design appropriate parameters for downloadable aggregated information. In other words, in our view, the information within TELUS' systems reviewed by CRC on PHAC's behalf for the purpose of designing aggregated download is not automatically out of scope of the Privacy Act.

25. In order to determine whether this information, and the information subsequently downloaded in aggregate form, constitutes *personal* information we considered research, guidance and standards of practice with respect to de-identification and other protections against the identification of individuals. These sources included the Treasury Board Secretariat's Privacy Implementation Notice 2020-03, other industry standards in the health field, and research specific to mobility data.

Determining Adequate Protection Against Risk of Re-identification

26. For the purpose of this report, "De-identification" means a process whereby any personal identifiers, such as names, phone numbers or device IDs in a mobility data context, are stripped from the data about a specific individual (often replaced with a randomly assigned identifier).

27. In our view, based on current research, for mobility data, de-identification alone is insufficient to render data 'non-personal' and outside the scope of the Privacy Act. 'Mobility Data' represents data that reveals the geographic location of where a person or device has been at multiple points in time. Depending on the circumstances, such data can be used to infer information about a device user, such as their place of home or work. This could in turn be compared to other readily available information to link the de-identified data to an identifiable individual and then glean information about where else they have been. Towards accuracy of technology, a study[6] conducted on 1.5 million users of a mobile phone operator in a western country concluded that four spatio-temporal points are enough to uniquely identify 95% of the individuals because mobility traces are highly unique and consistent.

28. We would therefore expect that for an organization to avoid collecting personal information in a mobility data context, it would need to ensure sufficient additional protections against re-identification are in place **in addition to de-identification measures**.

29. There are a range of different types of protections against re-identification, and new techniques may also be developed in future. Two common types of protections, both of which were used in this case, are: (i) contractual and physical protections on access and use, and (ii) aggregation.

---

[6] de Montjoye, YA., Hidalgo, C., Verleysen, M. *et al.* Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep* **3,** 1376 (2013).

30. Contractual and physical protections on access and use reduce the risk of re-identification of de-identified data by limiting the number of individuals/organizations who could have the **opportunity** to attempt re-identification, and by limiting the **likelihood** those individuals will attempt re-identification.

31. Aggregation reduces the risk of re-identification by combining data about multiple individuals together so that any one individual's own data is obscured.

32. Generally speaking, in order for information to be considered 'non-personal' and therefore outside of the scope of the Privacy Act the following conditions would need to be met:

    i. where an institution has access to properly de-identified mobility data there would need to be robust contractual and physical protections in place to: (a) limit access to that data to a limited number of individuals, and (b) limit the purposes for which individuals are permitted to use the data (i.e. to not allow re-identification attempts). For (b) this should include, at a minimum, a contractual requirement to not attempt re-identification, and safeguard controls such as audit capability and monitoring of data access/use to guard against unauthorized re-identification attempts.

    ii. where an institution has access to aggregated mobility data, (a) a sufficient number of individuals would be aggregated in each 'cell' to reasonably reduce the risk of extrapolating the data of a single individual (in accordance with current statistical guidelines or expert advice), and (b) access to the aggregated information would be controlled as above for access to de-identified data.

33. Regarding recommended cell sizes, the Treasury Board Secretariat's **Privacy Implementation Notice 2020-03 (Protecting privacy when releasing information about a small number of individuals)**, states *"there is no minimum cell size that is appropriate for all data releases, and Treasury Board of Canada Secretariat policies do not specify a mandatory minimum cell size. However, the following best practices may serve as a starting point for a case-by-case analysis: A minimum cell size of 10 is often cited as a best practice for public data releases of data that is less sensitive, while a minimum cell size of 20 is cited for more sensitive data*".

34. The next sections will illustrate how PHAC and its data providers applied the foregoing safeguards in each data stream they relied on to derive mobility insights.

Data stream 1: Mobile cell-tower/operator data

35. Interaction between cell phones and telecom cell towers is critical to the functioning of the telecom network and serving mobile users. Indeed, all cell phones regularly generate and transmit data to a nearby telecom cell tower when they connect to it or use operator's mobile services, for sending or receiving calls, texting, browsing the internet, etc. The frequency of interaction depends on phone usage. Normally, a phone sends a message

when it gets close to a new cell tower, when its connection status changes and when it needs to establish connections to access mobile services. Most phones will also send limited messages to the cell tower when they are stationary and idle.

36. Consequently, Telecom operators can collect and record information about their clients' location and movement (i.e. SIM id, timestamp and location of the tower serving the client) because cell towers have precise latitude and longitude coordinates that make it possible to infer the location and movement of the cell phones they are serving and interacting with.

37. TELUS stated its appreciation for the potential value of mobility data, including in combatting a global health crisis such as the COVID-19 pandemic. Since 2015, they had commenced the development of a data analytics platform, called TELUS Insights, designed to generate actionable intelligence from de-identified client mobility data.

38. Following the outbreak of the COVID-19 pandemic, TELUS launched, in April 2020, a program named "*Data for Good"* that operates on the TELUS Privacy-by-Design certified insights platform. PHAC chose to leverage TELUS' program, signing a contract with TELUS on February 10, 2021. It later signed a Memorandum of Understanding ("MOU") with CRC on July 05, 2021, to capitalize on CRC's expertise to conduct mobility analysis using location data. Both the contract and the MOU expired on October 8, 2021.

39. TELUS and CRC advised our Office that data within the TELUS Insights Platform does not indicate precisely where an individual device may be located since it is derived using the location of the cell towers rather than the geographic location of the mobile devices. Information about movement is inferred when a mobile device switches from one cell tower area to another and ends when the mobile device remains connected to the same tower for longer than 30 seconds. Thus, depending on cell tower coverage in the area, location data is estimated within a physical diameter of between 70km (in rural areas) to the smallest possible diameter of 100m. That said, sometimes, it is possible to determine device's location with more precision given the fact that cell towers that serve data are different from those that serve voice. With users often accessing both services, they can be more precisely located when in the range of two or more cell towers.

Prior De-identification

40. All direct identifiers (MSISDN[7], IMEI[8], IMSI[9]) in TELUS insights are removed or transformed by TELUS before third parties, including CRC on behalf of PHAC, access the data - so that the data within the Insights platform cannot be linked back to an individual. More specifically, each identifier is hashed more than once using SHA 256 hashing, which is a hash encrypting function that transforms input data ("message"), regardless of its size, into

[7] Mobile Station Integrated Services Digital Network is the mobile phone number.
[8] International Mobile Equipment Identity is a unique mobile phones' serial number.
[9] International Mobile Subscriber Identity is a number that uniquely identifies every user of a cellular network.

a fixed number of digits, known as the "hash," "digest" or "digital fingerprint." It is considered a one-way function because it is nearly impossible to turn the digest back into the original data.

41. Data accessible on TELUS' platform relates to 9 million devices and consists of: hashed device identifiers, timestamps, device country and area code, network cell identifier (identifies the sector of the cellular tower that the device was connected to), time the device was first and last seen on the cell tower, the duration of connection to this cell tower, and the approximate geographic coordinates of the cell tower.

Access control & data minimization

42. TELUS advised that the de-identified data within the Insights Platform is robustly safeguarded with physical, administrative, and technical controls, including Virtual Private Cloud Service controls to ensure access is restricted to authorized users as well as regular vulnerability scans, including logging and monitoring of activity on the Insights Platform. TELUS also explained that the ingested de-identified mobility data in the Insights Platform is temporally spatialized by at least 15 minutes and that it reviews each request, including use case, to access by a '*Data for Good*' client to determine what "data views" will be made available to the authorized data scientists.

43. In PHAC's case, five CRC employees and two PHAC employees were authorized to access device-level data at the TELUS insights platform, using a two-factor authentication system.

The enclave model[10]

44. In the enclave model, data may be kept in some kind of segregated enclave that restricts the export of the original data, and instead accepts queries from qualified researchers, runs the queries on the de-identified data, and responds with results[11].

45. TELUS uses a similar model - information at the device-level, even though it is de-identified, cannot be copied outside the TELUS platform. Rather, based on mobility insights reports that PHAC is interested in, CRC runs the corresponding queries on the device-level de-identified data. The aggregated results generated by the queries are then stored in a table, hosted at TELUS' cloud.

46. Access and use of TELUS insights platform is guided and supervised. Thus, prior to approving the transfer of the aggregated data in the generated table to CRC's cloud and subsequently to PHAC's cloud, TELUS reviews the generated data to ensure that required safeguard levels against re-identification are met.

---

[10] K El Emam and B Malin, "Appendix B: Concepts and Methods for De-identifying Clinical Trial Data," in Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk, Institute of Medicine of the National Academies, The National Academies Press, Washington, DC. 2015.

[11] NISTR 5053, De-Identification of Personal Information, P.14.

Aggregation

47. TELUS' review includes a determination that only aggregated counts are included. For example, data is sorted by Forward Sortation Area (FSA versus full postal code) or Census Canada Dissemination Area, and only aggregated counts relating to more than 20 devices are included. PHAC's representations to our Office confirmed that results are aggregated geographically (at least at the census sub-division), temporally (at least over 24 hours) and for a minimum of 20 devices.

48. Aggregated data imported by PHAC/CRC is subsequently used to calculate different mobility indicators that reflect population movement over 24-hour period for different geographic areas (province/territory, health region, census metropolitan area, or census sub-division). Examples of mobility indicators include aggregated percentiles of maximum distance travelled, maximum distance travelled far from home, total distance travelled, percentage of time at or within fixed distance of home and percentages of devices that travelled between different geographic areas.

Safeguards against re-identification in TELUS' data stream

49. TELUS, CRC and PHAC included multiple safeguards in this data stream to reduce the risk of re-identification of mobility data used by PHAC during the COVID-19 pandemic, namely:

    i. **Prior De-identification:** TELUS encrypts all device IDs prior to populating the insights platform with its customers' mobility data. Therefore, information that CRC accessed, on behalf of PHAC, in the TELUS insights platform did not contain any direct identifiers.

    ii. **Aggregation:** CRC is restricted to importing only aggregated data from TELUS insights platform and no data at the device level, even though it is de-identified, can be copied outside of TELUS platform. More specifically, data that CRC imported on behalf of PHAC was aggregated spatially, at least at the census sub-division level, temporally to span at least over 24-hours period and with cells that contains at least 20 devices. This minimum cell size is compliant with TBS' guidance in the subject matter. Further, it is above the minimum threshold (11) that was determined in the expert report[12] in a case[13] before the court that dealt with risk of re-identification.

    iii. **Release model**: TELUS' *Data for Good* is a non-public data release which limits the availability of the data set to select number of identified recipients. As a condition of receiving the data, recipients must agree to terms and conditions regarding the

[12] Public Expert Report of Dr. Khaled El Emam, dated March 24, 2021 ("Expert Report"), **Respondent's Public Record, Tab 3**.

[13] In the intervening time between the provision of the preliminary report to the respondent and the publication of the final report, the Federal Court released its decision in Cain v. Canada (Minister of Health), 2023 FC 55. The Court found the expert report to be persuasive (paras. 136-137), and endorsed the minimum threshold of 11 (para. 152).

privacy and security of the data set out in a data sharing agreement. The terms in this case required users at PHAC and CRC who had access to the data to not attempt to re-identify it.

Additionally, access to the TELUS insights platform is guided and supervised. TELUS reviewed requests to extract/download derived insights to ensure that privacy rules were met and to further mitigate any risk of re-identification prior to authorizing their export. Finally, only authorized and select employees from CRC and PHAC can access and use mobility data provided by TELUS, and TELUS established monitoring controls to review access activity and downloading logs to ensure compliance with policies and protocols.

iv. **Contractual clauses:** Both PHAC and TELUS included in the contract governing their commercial relationship binding provisions to use only de-identified information. Specifically, in the contract's statement of work that PHAC addressed to TELUS, TELUS was required to provide PHAC with access to de-identified information that ensures data anonymization in order to generate aggregate indicators and insights on the mobility of individuals in Canada.

Similarly, TELUS data sharing terms stipulates that PHAC must not use the derived data for any other purpose except for the one specified in the contract and that it may not correlate, associate, link or combine any of the derived data with other data sources, except as set out in an exhibit consented to in writing by TELUS. Further, these terms require PHAC to ensure that none of its representatives attempts to relate the derived data to any identifiable individual. TELUS confirmed that it allowed PHAC to correlate downloaded aggregated mobility data only with census data at the health region and FSA levels.

Data stream 2: Mobile geolocation data

50. In addition to cell-tower based data; PHAC relied on other sources to derive insights on the mobility of Canadians. Specifically, it used geolocation data, that is generally collected using mobile apps, GPS tracking Software Development Kits (SDKs), Bluetooth, Geotagged social media posts, etc.

51. Mobile applications offer a wide range of private sector services (weather, fitness, emails, maps, etc.). Certain apps collect the phone's geolocation data in real time using the phone's built-in GPS system - which is then available to app operator and could be disclosed by the operator to third parties.

52. PHAC signed a contract with BlueDot to procure geolocation data between March 26, 2020 and March 20, 2022. BlueDot, in turn acquired this category of data from two providers: 1- Pelmorex Corp, a Canadian weather information and media company that collects location data via its free mobile app such as the Weather Network app, and 2- Veraset LLC, an American company that sells raw and processed movement data that it acquires from third parties, other aggregators, SDK's and direct app relationships.

53. Under Canadian private sector privacy law, both the collection of phone geolocation information and any subsequent disclosures of personally identifiable data to third parties will generally require the user's valid consent. Pelmorex directly collects geolocation data (timestamp of the collection, geolocation coordinates, and pseudonymized user ID) from its app users. According to BlueDot, Pelmorex obtains users' consent for collection of this data (which it uses to deliver the app's weather-related services) and only discloses aggregated mobility data to BlueDot, not any individual personal information.

Prior De-identification

54. According to its privacy policy, Veraset collects information from third parties it describes as 'trusted'. That said, it does not define or elaborate on how the 'trusted' third parties obtain users' consent ahead of the collection.

55. Veraset does provide individual-level data to BlueDot - however, it claims to first strip the individual-level data of direct personal identifiers and includes a requirement in its contract with BlueDot that it not attempt to re-identify the individuals.

Aggregation

56. Once received by BlueDot, certain pre-aggregated data is sent directly to PHAC without further processing, whereas other data, mainly information at the device level, is aggregated by BlueDot spatially at the census tract or census sub-division ("CSD") geographic unit and/or temporally over a 24-hour period before sending it to PHAC.

57. Examples of the mobility insights that PHAC receives from BlueDot to estimate contact rates among Canadians include: (i) the number of devices at certain points of interest (parks, hospitals, retail stores, etc.), (ii) aggregated statistics on distance travelled around primary location of devices, (iii) movement between geographic regions within Canada and (iv) traffic originating from USA and other countries.

58. BlueDot advised that its agreement with PHAC stipulates that data provided to the health agency will be aggregated but without specifying any minimum cell size for the aggregated data (minimum number of devices that should be in each indicator). It explained, nevertheless, that it decided in April 2020 to follow Statistics Canada's precedent of excluding data based on less than 5 measurements and that on January 17, 2022, PHAC asked that indicators that were based on less than 20 devices be excluded.

Access control

59. Aggregated data from the BlueDot data stream is either uploaded directly to PHAC's cloud or included into written reports that are sent by email to PHAC. Authorized individuals from PHAC can also access similar information via a "Mobility Dashboard" that was developed by BlueDot.

Safeguards against re-identification in BlueDot's data stream

60. According to BlueDot's representations and data samples, the information flow from this data stream comprises several layers that increase the level of data de-identification and therefore reduces the associated risk of re-identification, namely:

    i. **Prior de-identification:** BlueDot did not receive any information that can be linked directly to identifiable individuals as data is either: (i) pre-aggregated or (ii) includes only a hashed device ID when it is at the device level.

    ii. **Aggregation:** PHAC receives from BlueDot only aggregated data and never data at the device level. More specifically, data provided to PHAC consisted of: (i) the number of devices that visited certain points of interest, (ii) mobility indicators (percentile of maximum and total travelled distance, percentage of time at and away from home) within census units, health regions and provinces, (iii) the number of devices that travelled between two Canadian health regions and (iv) the number of devices that arrived in Canada from a global epidemic hotspot. All the previous statistics were calculated over a 24-hour period and for cells whose minimum size was 5 devices and subsequently 20 devices, as of January 18, 2022. As explained above, this minimum cell size is compliant with TBS' guidance in the subject matter and above the minimum threshold (11) that was determined in the expert report in a case before the courts that dealt with risk of re-identification.

    iii. **Contractual clauses:** The statement of work that BlueDot received from PHAC requires BlueDot to "anonymously" analyze data at its disposal to help the health agency address specific questions related to social distancing, self-isolation at home, movements to/from healthcare institutions across the country, in addition to other analytics related to dispersion of COVID-19. BlueDot has also specified that it is contractually forbidden from attempting to re-identify data it receives at the device level from Veraset.

    iv. **Release model:** PHAC was not given access to raw data at BlueDot's system. Instead, BlueDot prepared and uploaded aggregated datasets to PHAC's cloud and provided it with a weekly/biweekly report. BlueDot's mobility dashboard that PHAC could access contains the same mobility indicators that were shared with PHAC either via email or through an upload to the cloud. Also, only approved PHAC employees can access the dataset uploaded to its cloud system.

Safeguards in both data streams that reduce the serious possibility the risk to identify individuals

61. De-identification is widely recognized, across the globe, including by our office, to be a potential tool to assist in protecting individuals' privacy while realizing the benefits associated with big data. This was of particular relevance during the current pandemic, given the benefits of mobility insights to understand and curb the spread of COVID-19.

62. To that end, in the case under this investigation, TELUS and Veraset relied on a robust algorithm (SHA 256) to hash direct identifiers and de-identify data at the device-level. Furthermore, access to the granular information at the device-level by PHAC/CRC is either not allowed (BlueDot data stream) or supervised and controlled (TELUS data stream).

63. In both data streams, information under PHAC's and/or CRC's control has been aggregated according to several criteria, either temporally and/or spatially, with minimum cell sizes between 5 and 20, a minimum size that is accepted and recommended by many experts in Canada, which increased the degree of data anonymity of the datasets under PHAC's or CRC's control.

64. Further, only select employees from PHAC/CRC were authorized to access mobility data either at the device-level, on a 'view only' basis, or in aggregated form.

65. Finally, PHAC and its epidemiologists in this specific project were looking for macro trends on the population movement and were not engaged in contact-tracing. Therefore, PHAC had no motivation to re-identify data and this is expressly reflected in its contracts and the RFP related to this matter.

66. As explained in detail in paragraph 32, in this case, in order for information to be considered 'non-personal' for the purposes of collection of properly de-identified data by a federal institution under the Privacy Act, the following conditions must be met: (i) robust contractual and physical protections are in place and (ii) acceptable data aggregation levels and access controls exist.

67. In light of the above, the accepted practices in this field and the measures taken against the risk of PHAC identifying any individual, we find that there is not a serious possibility that the information PHAC collected could be used to identify any individual. Therefore, the complaints are **not well-founded**.

Other

68. OPC is generally supportive of the use of anonymization and de-identification as a privacy enhancing technique to glean insights from data while reducing privacy risks. Indeed, our Office issued in April 2020 a Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19. Said framework encouraged organizations to use de-identified and aggregated data whenever possible, while cautioning of the existence of a residual risk of re-identification.

69. However, de-identification is an active research field and no method has yet been found that eliminates re-identification risks, and the resulting privacy risks to individuals. This highlights the importance of privacy laws that are modernized to expressly deal with de-identified personal information.

70. The Privacy Act treats personal information as a binary concept, and therefore does not fully capture the nuances associated with de-identified personal information. As a technique in information management, de-identification is often motivated by a desire to strike the right balance between, on one hand, preserving the utility of data derived from personal information, and reducing privacy risks associated with that data on the other.

71. Consequently, the more we increase the utility of de-identified data, the more we add information deduced from personal information and the more we move away from anonymity and vice versa. Needless to say, removing *all* personal data elements from a dataset would render that data useless. However, even de-identified information presents at least some risk to privacy. Generally speaking, the more data elements that remain, the greater the risk to privacy. This nuance is not captured by the binary approach in the current legal framework, especially since the assessment of the risk associated with re-identification is not static, but rather can evolve over time.

International benchmarking

72. Our benchmarking against privacy legislations in other jurisdictions regarding the use of de-identified information highlighted a certain heterogeneity with respect to the definition of de-identified information and on whether to consider it personal information subject to the provisions of national laws or, on the contrary, as anonymized data that is outside of the scope of law. The benchmark exercise, although not exhaustive, did not identify any country that chose to include in its law, provisions that are customized to, and specific to, this category of information.

73. Regarding the use of mobility data to combat the pandemic, the benchmark illustrated that most countries have integrated this measure into their response to the COVID-19 pandemic.

74. In the European Union, recital 26 of the GDPR states that pseudonymized[14] data should be considered as personal data whereas anonymized data should not. Consequently, the principles enshrined in the European regulation apply to pseudonymized data, which can be assimilated to de-identified data at the device level mentioned above, and not to anonymized data. On another note, the opinion 05/2014 on Anonymization Techniques adopted on April 10, 2014 by the Article 29 Data Protection Working Party, the predecessor of the European Data Protection Board ("EDPB") states that "*Anonymisation constitutes a further processing of personal data; as such, it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing*".

75. In the United States, the Health Insurance Portability and Accountability Act ("HIPAA") includes two methods: 'expert determination' and 'safe harbor', that covered entities under HIPAA can use to de-identify protected health information. Once de-identified, said information is no longer protected under HIPAA and can be used freely to glean valuable

[14] Processed personal data by replacing identifiers with artificial ones in such a manner that personal data can no longer be attributed to a specific individual without the use of additional information.

insights about population health. Similarly, the California Consumer Privacy Act ("CCPA") does not restrict businesses from collecting, using, retaining, selling, or disclosing consumer information that has been de-identified or aggregated as it does not consider these categories of data as personal data. Conversely, pseudonymized consumer information is considered under the statute as personal data.

76. In the United Kingdom, the Information Commissioner's Office ("ICO") is of the view that "Generalised location data trend analysis is helping to tackle the coronavirus crisis. Where this data is properly anonymised and aggregated, it does not fall under data protection law because no individual is identified".

77. In Australia, the Office of the Australian Information Commissioner ("OAIC") published guidance on the subject matter that considers de-identification as a privacy-enhancing tool and advised that information that has undergone an appropriate and robust de-identification process is not personal information and is therefore not subject to the Australian Privacy Act. Said guidance added that: "*whether information is personal or de-identified will depend on the context. Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment). Put another way, information will be de-identified where there is no reasonable likelihood of re-identification occurring*".

78. In its "ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS", the Personal Data Protection Commission ("PDPC") in Singapore considers data that has been properly anonymized as no longer being personal data and therefore not subject to the provisions of the Singaporean Personal Data Protection Act. The PDPC also clarifies that it does not assimilate de-identified data to anonymized information.

79. On another note, the use of mobility data to analyze human mobility dynamics to inform decision making in many topics, such as transportation and disease surveillance, is not novel. De-identified and aggregated mobility data have been used in the past to fight Ebola in Africa, Zika in Brazil, and swine flu in Mexico.

80. Regarding the current pandemic, health authorities, researchers and NGOs in many foreign regions worldwide leveraged this type of information to shape their policies aiming to curb the spread of COVID-19. Examples include Argentina, Austria, Brazil, Chile, China, Colombia, Curaçao, Democratic Republic of Congo, Ecuador, European Union, Germany, Ghana, Greece, Haiti, Italy, Japan, New York, Spain, Sweden, Poland, Portugal, United Kingdom, etc.

Transparency

81. Concerns were raised by Canadians regarding the lack of transparency in PHAC's collection and use of mobility data. This raises the important question as to whether PHAC was sufficiently transparent to the public on its use of mobility data, notwithstanding the fact that it was de-identified and aggregated.

82. The Privacy Act does not impose any transparency obligations on PHAC as it did not collect personal information as defined under the Act. Nevertheless, we understand Health Canada's position to be that the government took concrete actions to inform Canadians about PHAC's use of mobility data. Two specific examples were cited :1-the prime Minister's news release[15] on March 23, 2020 that announced support to BlueDot and 2- the COVIDTrends webpage which included an indicator about Canadians' mobility change over a week. The COVIDTrends page was accessed by at least 1.7 million visitors.

83. These measures were not sufficient to adequately inform Canadians about how their mobility data was being used. In fact, both measures required Canadians to proactively consult specific websites to inform themselves of the program(s). Further, the news release regarding the support to BlueDot did not mention that BlueDot would use and rely on Canadians' mobility data to produce its disease analytics. In the future, we recommend that more efficient, targeted, and accessible communication channels be used in order to achieve better transparency. Examples of such channels include press releases or press conferences properly relayed via the media that explain how personal information would be used in government programs.

84. OPC's Commissioner at the time, Mr. Daniel Therrien, nuanced that "most Canadians whose data was used did not know their data was used." and he opined that "both the government and the private sector, could have done more to inform users that their data was used for these purposes." He added in a statement following the release of the ETHI report that "greater flexibility to use personal information for the public good, including public health purposes, should come with greater transparency and accountability"

85. By way of comparison, other projects that also used de-identified and aggregated data in support of COVID-19 research opted for different channels. For example, partnership between TELUS and the Natural Sciences and Engineering Research Council of Canada (NSERC) was announced through a news release at TELUS' website.

[15] "Support for BlueDot, a Toronto-based digital health firm, with a first-of-its-kind global early warning technology for infectious diseases. The company was one of the first in the world to identify the spread of COVID-19. The Government of Canada, through the Public Health Agency of Canada, will use its disease analytics platform to support modelling and monitoring of the spread of COVID 19, and to inform government decision-making as the situation evolves".

Conclusion

86. We take this opportunity to highlight and remind public and private organizations that use and/or procure de-identified data of several principles that should be considered. Most of the following are consistent with recommendations of ETHI's study report.

87. There is a broad consensus that all de-identification techniques entail a residual risk to privacy that may increase over time, and that anonymization is an evolving area. With this in mind, organization that produce or collect de-identified data should continually assess the appropriateness of any de-identification techniques and related safeguards against identification. They should employ de-identification as a privacy enhancing technique, not only as a manner to achieve compliance with legislative requirements.

88. Although we did not examine the issue in this Report, it is incumbent upon data-holders to ensure that any third parties from which they source data have themselves collected data and personal information in a manner that respects privacy law obligations of collection and informed consent. Organizations that procure de-identified data are therefore accountable and should conduct their due diligence beyond ensuring that data is anonymized and falls outside the scope of privacy laws.

89. Public organizations, such as PHAC, should be transparent with regards to the use of de-identified information and make every effort to publicize such uses and to inform concerned individuals of its purposes, the sources of data, and safeguards implemented to protect it and maintain its anonymity.

90. We also recommend that the federal privacy laws be amended to include a clear legal framework that defines the different types of de-identified data and that specifies the rules that should govern the production, retention, use, disclosure, and collection of each type.

91. Any new legal framework should consider the specificity of de-identified data and draw the lesson from the limits of the current binary system that can be either suboptimal with regards to privacy protection or be a hurdle to realizing the public benefits of big data. The framework can for instance be tailored to the degree of anonymity of data and balance the benefits of using de-identified data against the residual risk to privacy. It would also ideally include clear rules on how to quantify residual risks to privacy and define acceptable thresholds to compare them with.

92. PHAC accepted our recommendations and shared the following measures that it took or plans to take, in order to implement OPC's recommendations:

    - PHAC established an internal working group, that includes the PMD, to improve transparency with the public about what PHAC does with the data it collects;
    - PMD has developed an internal tool to assess the risks of de-identified data and to determine whether it is within the threshold of "serious possibility" of re-identification. PMD provides advice to PHAC and HC programs and makes

recommendations towards mitigating these risks and ensuring compliance with the Privacy Act and Treasury Board privacy policies;

- PHAC is working with partners to improve transparency and public trust, and to enhance privacy protections. This work includes publishing sample and open data sets and algorithms used to de-identify, anonymize and aggregate data, using and developing synthetic datasets, ensuring the capacity to test privacy guarantees; and enhancing in-house technical skill to efficiently execute this work.
- PHAC and HC are ensuring due diligence when entering into agreements with third parties from whom data is sourced by including appropriate privacy clauses and measures to safeguard both personal information and de-identified information, where appropriate.