Commissaire à la protection de la vie privée du Canada
Privacy Commissioner of Canada

BY EMAIL

23 January 2023

The Honourable Gwen Boniface
Joint Chair, Special Joint Committee on the Declaration of Emergency
40 Elgin Street
Chambers Building
The Senate of Canada
Ottawa ON K1A 0A4

Mr. Rhéal Éloi Fortin, M.P. and
Mr. Matthew Green, M.P.
Joint Chairs, Special Joint Committee on the Declaration of Emergency
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

Subject: Privacy during an Emergency

Dear Joint Chairs:

I am writing in response to an invitation received on December 22, 2022, from the Joint Clerk of the Special Joint Committee on the Declaration of Emergency (the "Committee"), to submit a brief for the Committee's consideration. I would like to thank the Committee for the invitation.

As the Privacy Commissioner of Canada, I am pleased to provide the Committee with an overview of the principles that government institutions should adhere to during an emergency to ensure that privacy rights are respected. I will also outline some issues raised in the context of my Office's work related to matters being examined by the Committee.

The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private-sector privacy law.

… /2

The OPC works independently from any other part of the government to investigate complaints from individuals with respect to the personal information-handling practices of both the federal public sector and the private sector. We focus on resolving complaints through negotiation and persuasion, using mediation and conciliation if appropriate.

In cases that remain unresolved, particularly under PIPEDA, I may take the matter to Federal Court and seek a court order to rectify the situation. Both the *Privacy Act* and PIPEDA prohibit me from disclosing any information that comes to my knowledge as a result of the performance or exercise of my duties or powers, including ongoing investigations and engagements with public sector institutions and private sector organizations, subject to certain limited exceptions.[1]

Another key part of my Office's mandate is to promote public awareness and understanding of privacy issues. In line with this, I would like to provide the Committee with an overview of the key privacy principles that should factor into any assessment of measures proposed to address a public order emergency that may have an impact on the privacy of Canadians.

During a 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. When reasonably and contextually interpreted, existing privacy legislation, norms and best practices ensure responsible data collection, use and sharing that can support public order. They also promote continued trust in the government and ensure that fundamental rights are respected. Privacy protection is not just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental rights and democratic values, even in exceptional circumstances.

I recognize that emergencies evolve rapidly and require swift and effective responses to address extraordinary public needs. However, even in an emergency, public institutions must continue to operate under lawful authority and act responsibly, particularly with respect to handling information that may be considered sensitive, such as information about individuals' finances, political opinions, travel, movements, and contacts or association. To achieve this, government institutions should ensure that the following key principles factor into any assessment of measures proposed during an emergency that may have an impact on the privacy of Canadians:

… /3

[1] *Privacy Act*, R.S.C., 1985, c. P-21, s.63; PIPEDA, S.C. 2000, c. 5, ss. 20(1).

- **Legal authority**: Government institutions should identify the legal authority that they are relying on to collect, use, and disclose personal information.

- **Necessity and proportionality:** Measures taken by institutions to address a public order emergency should be necessary and proportionate. This applies both within the context of existing measures and in deciding on new actions taken to address a crisis. Necessary means that measures are more than potentially useful. Although this does not require "absolute necessity" (i.e., that no other conceivable means are available, regardless of costs), measures should be more than potentially useful. They must be evidence-based and likely to be effective, although effectiveness must be assessed in context. Institutions should also ensure that measures are not overbroad, meaning that they are tailored in a way that is rationally connected to the specific purpose to be achieved.

- **Purpose limitation:** Institutions should ensure that personal information collected in the specific context of an emergency is not used or disclosed for any other reason. Individuals' reasonable expectation of privacy may decrease during a crisis, but individuals would not reasonably expect that sensitive information (such as their financial information or political opinions) would be available for other government or commercial purposes. Personal information collected in an emergency should also be disposed of when the emergency ends, except for narrow purposes such as research or ensuring accountability for decisions made during the crisis, particularly decisions about individuals.

- **De-identification and other safeguarding measures**: Institutions should ensure that personal information is protected by administrative, technical, and physical means, including enhanced safeguards for sensitive information. They should also consider whether directly identifiable information is required in the context, or if de-identified or aggregate data is sufficient. When using de-identified or aggregate data, institutions should be attentive to the risk of re-identification, which depends on case-specific contextual factors, including what data is used, in what form, with what other data it is combined, and with whom it will be shared.

- **Openness and transparency:** During an emergency, institutions should provide clear and detailed information to individuals about new and emerging measures on an ongoing basis. Transparency is a cornerstone of democratic governance as well as our privacy laws, and it is all the more vital in the midst of an emergency when extraordinary measures are being contemplated. The public, and wherever possible individuals, must be informed of the purpose of the collection of their personal information.

- **Oversight and accountability:** New measures specific to the emergency should also provide specific provisions for oversight and accountability. Institutional safeguards become more, and not less, important during times of crisis.

- **Time limitation**: Privacy invasive measures taken during an emergency should be time-limited, with obligations to clearly end when they are no longer needed. There should be strict time and other limits on measures implemented in response to the emergency (e.g. the type and range of personal data being collected, used and shared). Time limits should be short, with the option to extend, if necessary.

Such principles have helped inform our work in three files related to concerns raised in the context of the disruptions, blockades, and occupation in February 2022.

First, after concerns were raised about the privacy implications of the use of the *Emergencies Act*,[2] the OPC engaged with the Canadian Security and Intelligence Service (CSIS), the Financial Transactions and Reports Analysis Centre (FINTRAC), and the Royal Canadian Mounted Police (RCMP). The goal of this engagement was to better understand and assess against the *Privacy Act* how the institutions handled personal information within the context of the *Emergencies Act* and the temporary powers granted as a result of the *Emergency Economic Measures Order* ("the Order").[3]

… /5

[2] *Emergencies Act*, R.S.C., 1985, c. 22 (4th Supp.).
[3] *Emergency Economic Measures Order*, SOR/2022-22.

The Order allowed 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. 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 RCMP or CSIS.

These measures included a requirement for certain financial entities to determine whether they had in their possession or control property that is owned, held or controlled by or on behalf of a designated person,[4] and to disclose this information to the RCMP or CSIS, as well as temporary authority for federal, provincial and territorial government institutions to share relevant information with financial entities if the disclosing institution was satisfied that the disclosure would contribute to the application of the Order. The Order also created a requirement for certain entities to register and report certain financial transactions to FINTRAC.

While our examination of these issues remains ongoing, key issues that we have been considering in this context include:

- The scope and nature of the personal information received and disclosed within the context of the *Emergencies Act* and related Order;
- Whether reasonable steps were taken to ensure the accuracy of the personal information;
- Whether reasonable steps were taken to limit the sharing of personal information;
- Whether personal information was used or disclosed for other purposes beyond the purpose of collection; and
- Whether consideration was given to the publication of a new or modified Personal Information Bank to describe the 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*.

… /6

[4] Designated person means any individual or entity that is engaged, directly or indirectly, in an activity prohibited by sections 2-5 of the *Emergency Measures Regulations*.

We are currently finalizing our report and plan to publish our findings and observations in the Spring of 2023.

Second, the OPC's Government Advisory Directorate, which provides advice and recommendations to federal public sector institutions in relation to specific programs and initiatives, received notification from a law enforcement agency about their use of an internet monitoring tool they were implementing due to concerns about officer and public safety related to the disruptions, blockades and occupation. The agency followed up by submitting a Privacy Impact Assessment to my Office. However, as the use of this tool was within the scope of an ongoing investigation by my Office, we advised the institution that we would pause our review but may engage in further consultation and review at the conclusion of the investigation. Our investigation remains ongoing though we expect it to be completed in the Spring/Summer of 2023. I would be happy to provide our conclusions to the Committee once it is completed.

Third, on March 15, 2022, the OPC received a complaint from Mr. James Bezan, Member of Parliament for Selkirk–Interlake–Eastman, related to a series of breaches at a crowdfunding site that resulted in the exfiltration and partial publication of Canadians' personal information.[5] We are currently investigating the breach, including whether the site had adequate safeguards in place and whether breach reporting requirements were met. We expect to complete the investigation in the Spring of 2023, and I would be happy to provide our conclusions to the Committee once it is completed.

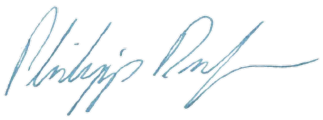
In conclusion, privacy is fundamental, and ensuring that it is protected builds necessary trust and supports the achievement of important public interest goals. In the context of any emergency, it is important for a clear privacy governance framework to be developed and implemented to ensure that government institutions and private sector entities can effectively meet their obligations under both the *Privacy Act* and PIPEDA.

… /7

[5] MP Bezan pens letter to Privacy Commissioner on leaked data (March 9, 2022).

I hope that this information is of assistance to the Committee, and I look forward to reviewing the Committee's report. Please do not hesitate to contact me should you have any questions or require further information.

Sincerely,



Philippe Dufresne
Commissioner

c. c. Miriam Burke, Joint Clerk of the Committee
Mark Palmer, Joint Clerk of the Committee
E-mail: DEDC@parl.gc.ca