



## BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

The Right Honourable Justin Trudeau, P.C., M.P.  
Office of the Prime Minister  
80 Wellington Street  
Ottawa, ON K1A 0A2

June 24, 2020

Prime Minister:

The Canadian government has announced that it has chosen a digital contact tracing application to recommend across the country, putting forward a call for residents to accept a new reality of digital surveillance. However, this call has come far too early, as the requisite privacy assessments are yet to be completed. The Federal government has announced the app will be available in July, and will be “tested” in Ontario, although the nature of that testing remains unclear.

We, the undersigned, write to call attention to our serious concerns with the application’s implementation and operation at a regional and national level.

Privacy Commissioners across Canada have issued guidance for the prospective development and deployment of this technology. The Prime Minister indicated in his press conference on June 18, 2020 that the government has “worked with” the federal Privacy Commissioner on this application, but the Privacy Commissioner’s office has not yet received the necessary information to analyze and provide recommendations on the application, nor has a Privacy Impact Assessment been completed or submitted to that office for review. In fact, from our understanding, the Office of the Privacy Commissioner has yet to have had access to the app in order to analyze it.

If a contact tracing application is to earn the trust of Canadians, then privacy must be of paramount importance. It is concerning that a deployment date has been publicly announced before the federal Privacy Commissioner has been given the opportunity to comprehensively review the application and its privacy impacts.

In addition, privacy rights and civil liberties organizations across the country have issued principles to protect the privacy and rights of people in Canada in regard to digital surveillance tools, but the government has not demonstrated how these principles have been met or considered.

In a context where, internationally, contact tracing apps have yet to prove their effectiveness, it is of particular importance to ensure that an appropriate balance is struck between the degree of invasiveness of information collection, and the public health benefit that might derive from its use. There is jeopardy, for personal information, for public trust, and for our rights, in recommending a tool for national deployment without a publicly available and fully transparent assessment of its privacy impacts.



## BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

For these reasons, we are calling on the federal government to provide the Privacy Commissioner of Canada and their provincial and territorial counterparts with the time necessary to fully analyze the application and release an assessment *before*, not *after* the application is released to the public. To ensure public confidence and adequate rights protections, a decision of whether to release the application to the public should only be made once any privacy concerns associated it are addressed. Additionally, the privacy policy for the application must be clear, detailed, and understandable so users can provide informed and meaningful consent, as well as understand their privacy rights and protections. Finally, all elements of the application's source code (including any code developed for its implementation) must be released to the public so that the privacy and security of the initiative can be assessed.

While some of the concerns expressed in the general principles below have been met, others have not.

### **1. Prioritize approaches which do not require any surveillance or data gathering to encourage people to stay at home**

Make full use of public education, financial assistance, and other options and support which will allow people in Canada to practice social distancing, and avoid infection, as well as testing at scale to identify people who have been infected. Any surveillance-based measures must only be relied on where demonstrably necessary and as a last resort.

### **2. Due process for adopting any new powers. Any new powers must be adopted through a legislative process, following transparent and open public debate.**

Invasive measures must be referred to the courts and the privacy commissioner for an assessment of their legality, effectiveness and proportionality. As the federal Privacy Act remains an inadequate and outdated instrument, data gathering must be accompanied by binding rules to ensure data minimization, strict necessity and proportionality. Such measures must be temporary, with a defined end date and review periods regularly scheduled. Ongoing reviews must be public and transparent, and must consider the impact and effectiveness of any new measures as well as their continued necessity

### **3. Favour consent in any data sharing initiatives**

In any government use of mass data technologies to address the pandemic, options that allow people the choice to volunteer their data must be strongly preferred to non-voluntary data collection. Voluntary measures must be truly voluntary, and free from coercion of any kind. Neither leaving location services on nor an agreement signed with their mobile provider on registration can be understood as providing this voluntary consent. Any voluntarily provided data must be subject to the same limitations and considerations of proportionality and use as all



## BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

other data, and subject to 'ongoing' consent – i.e., subject to withdrawal by the provider at a later date.

### **4. Put strict limits on data collection and retention**

Any adopted measure must ensure that data collection is minimized, limited to collecting data that is strictly necessary for established public health considerations directly relating to the declared emergency, and proportionate, keeping in mind the sensitivity of the data being collected. Any data collected must be fully and promptly deleted as soon as it is no longer necessary to contain the pandemic.

### **5. Put strict limits on use and disclosure**

The intended use of any collected data must be specifically and clearly defined, and that data should only be used for its intended purpose. All data must be de-identified and anonymized. Any data gathered must only be used for the public health purposes that justified its collection, and may only be disclosed to public health bodies. No data gathered through these measures can be used to achieve law enforcement or immigration objectives, or for commercial purposes, including in de-identified format.

### **6. Oversight, transparency and accountability**

Any new rules or technology adopted during this period must have independent oversight, must be transparent to the public, and must provide options for recourse with regards to breaches, misuse, or other violations of rights. This independent oversight must be additionally empowered to remedy any inaccuracy or bias in any adopted measures, as many digital surveillance and analytic tools have been found to be deeply biased, particularly against marginalized groups.

### **7. Any surveillance efforts related to COVID-19 must not fall under the domain of security, law enforcement or intelligence agencies**

The current pandemic situation is a public health crisis, not a matter of national security. Security, law enforcement and intelligence agencies must not be involved in any form of public health surveillance or data collection. Moreover, the line between the data held by Canada's health and security establishments must be maintained throughout.

Commissioner's Guidance on contact tracing apps

[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c\\_200507/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200507/)



## BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

Sincerely,



BC Freedom of Information and Privacy Association

**Jason Woywada**  
Executive Director  
P: (604) 739-9788  
E: [fipa@fipa.bc.ca](mailto:fipa@fipa.bc.ca)



BC Civil Liberties Association

**Harsha Walia**  
Executive Director  
P: (604) 630-9752  
E: [harsha@bccla.org](mailto:harsha@bccla.org)

CANADIAN  
CIVIL LIBERTIES  
ASSOCIATION



ASSOCIATION  
CANADIENNE DES  
LIBERTES CIVILES

Canadian Civil Liberties Association

**Brenda McPhail**  
*Director, Privacy, Technology &  
Surveillance Project*  
P: (416) 646-1406  
E: [bmcphail@ccla.org](mailto:bmcphail@ccla.org)



OpenMedia

**Laura Tribe**  
Executive Director  
P: (1 888) 441-2640 ext. 2  
E: [laura@openmedia.org](mailto:laura@openmedia.org)



Samuelson-Glushko Canadian Internet Policy & Public  
Interest Clinic (CIPPIC)

**Tamir Israel**  
Staff Lawyer  
P: (613) 562-5800 ext. 2914  
E: [tisrael@cippic.ca](mailto:tisrael@cippic.ca)



International Civil Liberties Monitoring Group

**Tim McSorley**  
National Coordinator  
P: (613) 241-5298  
E: [nationalcoordination@iclmg.ca](mailto:nationalcoordination@iclmg.ca)

CC: Premiers