April 15, 2020

Joint statement: Digital surveillance technologies and COVID-19 in Canada

As the Canadian government seeks to respond to the COVID-19 pandemic, the possibility of using smartphone tracking or other mass public data collection to track infections or ensure compliance with rules has been raised.

The pressure to adopt extraordinary measures in response to extraordinary situations is understandably high. But we must make sure to carefully consider the cost to our privacy, values and human rights. We must emphasize that any measures that amount to mass warrantless surveillance of identifiable people in Canada would not be a proportionate or reasonable response, even in these difficult times.

People in Canada are concerned about the possibility of invasive emergency measures, and for their potential to continue undermining our rights after the current crisis is over. Even in times of crisis, mass digital surveillance tools pose a unique and insidious threat to our fundamental values. No data set fully represents the world, and biases and flaws in data and the algorithms applied to it have been shown to disproportionately impact already marginalized communities in our society. There is also a real risk that they undermine public health measures by providing a false sense of security, or undermine trust in and disclosure to public institutions. It is therefore crucial that all discussions about enhanced surveillance take place transparently and openly, before any new measures are put in place.

We, the undersigned organizations and experts, urge the government of Canada to follow these seven principles when considering any kind of enhanced digital surveillance or data collection:

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 other data, and subject to 'ongoing' consent - ie, 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.

Sincerely,

OpenMedia
B.C. Civil Liberties Association (BCCLA)
BC Freedom of Information and Privacy Association (FIPA)
International Civil Liberties Monitoring Group (ICLMG)
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)