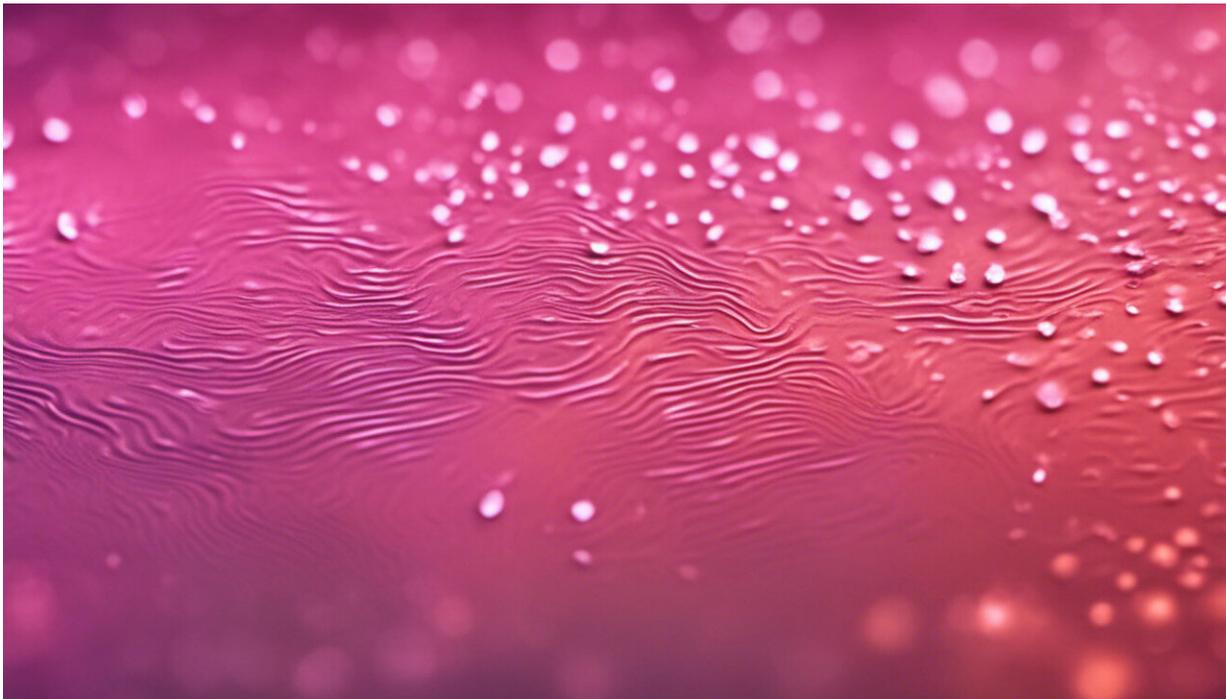


Coronavirus contact tracing poses serious threats to our privacy

May 11 2020, by Aaron Mauro



Credit: AI-generated image ([disclaimer](#))

We are all wondering how COVID-19 will end. We will not likely return to normal without a broadly distributed vaccine, which is a bracing proposition. It is also becoming increasingly clear that [we will have to find a way to trace transmission and maybe even enforce individual quarantines in the interim.](#)

I want to say that I am not an epidemiologist, nor am I a public health official. As a faculty member within the [Centre for Digital Humanities](#) at [Brock University](#), my role is to [communicate the social and cultural consequences of digital media](#), including potential privacy and security risks of software used to limit the effects of COVID-19.

In the coming weeks and months, I expect that [we will hear a lot](#) about "[contact tracing](#)." Contact tracing involves interviewing patients to collect information on all the people they have had sustained contact with and all the places they have been. It is laborious and error-prone because it is dependent on memory, interviews and detective work.

Because of the scale of [contact tracing](#) needed for COVID-19, using cellphones to detect and record proximity appears to be an ideal solution. The Canadian government is exploring contact tracing and Prime Minister Justin Trudeau expressed that "[all options are on the table](#)."

Civil liberties in crisis

Before the Canadian government makes decisions that infringe on [civil liberties](#) through widespread digital surveillance, we need to think about the concessions we make during a time of crisis. Crises have long been used as an opportunity by governments and corporations to infringe on civil liberties in the name of public safety.

We need only think of the legislative overreach in the wake of the 9/11 terrorist attacks. In the United States, the extraordinary powers granted by the [Patriot Act](#) were revealed by whistleblower Edward Snowden when he disclosed [NSA and CIA surveillance. Those disclosures shook the country to the core](#). In Canada, the omnibus Bill C-36 was passed, which contained the [Anti-Terrorism Act](#).

During the post-9/11 period, Canadians learned a lot about phone

tracking. In 2017, the Canadian government introduced [Bill C-59](#), which amended the earlier [Anti-terrorism Act and acknowledged past legislative overreach](#).

Contact tracing using [digital technology](#) represents an opportunity to battle COVID-19 and reopen the economy, but its application will create unprecedented surveillance infrastructure beyond anything we have seen before.

There is an app for that

In recent days, the federal government has indicated that the provinces will be responsible for managing their plans to reopen their economies, which will result in a [patchwork of contact tracing apps across the country](#). There are risks that such a network of policies, laws and collection techniques will muddy the data about COVID-19 nationally.

By contrast, many countries have turned to nationally mandated mobile applications to automate contact tracing. [South Korea](#), [Singapore](#), [Germany](#) and [China](#) have all implemented their own digital tools to assist public health officials and trace the spread of COVID-19.

There are several models that Canadians can think about with regard to contact tracing apps. China dealt with this problem first, and chose some rather [extraordinary methods](#). Citizens were allowed to travel between checkpoints based on an app embedded in online payment systems like Alibaba's Alipay or Tencent's WeChat. Without a green QR code, citizens were not allowed to travel and could face detention for violations.

Currently, the [Canada COVID-19 app](#)—a partnership between private health-care software company Thrive Health and Health Canada—allows you to volunteer your [location data and self-report symptoms](#). This

volunteer approach was led by Singapore's [TraceTogether](#) app, which goes a step further by accessing the Bluetooth radio in smartphones to detect proximity.

The limitations of the TraceTogether app include the difficulty of running an app 24 hours a day, which depletes battery life and results in less reliable data.

The Alberta provincial government has recently released the [ABTraceTogether app](#); it is [unclear how effective this system will be](#) in the province.

Because the use of digital contact tracing was meant to correct for the errors of human interviews and memory, the [partnership between Google and Apple](#) has drawn a [tremendous amount of attention](#). In this case, our phones would eventually detect proximity and duration using a low level operating system process that would allow for 24/7 tracking.

The security and privacy implications are profound.

Regardless of the [optimism of the technology news observers](#), these systems are too complex and lacking in the transparency necessary for legislators to make adequately informed decisions on their implementation.

There is no reason [the general public should trust these corporations](#) to not monetize this system and maintain this surveillance infrastructure after the crisis has passed. While the need for digital contact tracing is clear, Canadians must take steps to protect their personal data.

Non-technical recommendations

It will be important for Canadians to discuss these systems before plans

are put in place and laws are passed that may violate the [Canadian Charter of Rights and Freedoms](#), particularly with regard to the security of the person. With any luck, the conversation held by Canadians with their provincial leaders and federal counterparts will include the following:

- A sunset clause to define when surveillance ends.
- A chain of custody agreement for data passed between government, industry and researchers, which includes a process to delete data.
- A plan to protect data sovereignty, which ensures that data are subject to Canadian laws and governance structures.
- A public use of judicial oversight of government, industry and researchers to ensure the laws we choose as Canadians are followed.
- A commitment to corporate accountability if our data are misused, stolen or sold.

Digital contact tracing will likely become central to the government's approach to stifling the resurgence of the virus and reopening the economy.

The complexity of these systems is a risk for the general public who may agree to something that is not well understood. It is critical to inform the public about these risks before governments take extraordinary powers and infringe on our civil liberties.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Coronavirus contact tracing poses serious threats to our privacy (2020, May 11)
retrieved 16 April 2024 from
<https://techxplore.com/news/2020-05-coronavirus-contact-poses-threats-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.