The Race to Trace: Ensuring the Security and Privacy of COVID-19 Exposure Notifications Apps

Position Statement on Responsible Uses of Technology and Health Data During Times of Crisis

Authors (who collectively contribute to the Cybersecure Policy Exchange and authors of accompanying paper):

Mohammed (Joe) Masoodi
Policy Analyst, Ryerson Leadership Lab
joe.masoodi@ryerson.ca

Sam Andrey
Director of Policy & Research, Ryerson Leadership Lab
sam.andrey@ryerson.ca

Karim Bardeesy
Executive Director, Ryerson Leadership Lab
kbardeesy@ryerson.ca

Yuan Stevens
Policy Lead, Ryerson Leadership Lab
yuan.stevens@ryerson.ca

As governments around the world scramble to control the spread of COVID-19, leaders and policy-makers are urgently considering new technologies that might help. Chief among these technologies is exposure notification or contact tracing software — mobile device applications that track the proximity of other mobile devices and alert users if they have come close to someone infected with COVID-19. Proponents of these apps argue they can increase the volume, accuracy and reach of manual exposure notification, provided that enough of the population uses the software.

Before Canada deployed its exposure notification app, we conducted a representative survey of Canadian residents in May 2020 for the Cybersecure Policy Exchange that found many were ready to embrace this technology:

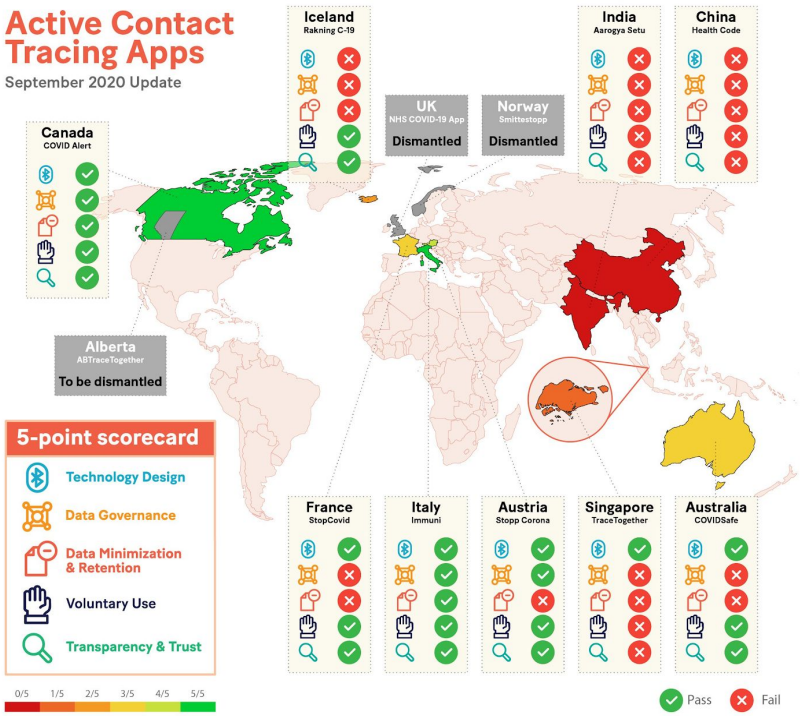
- A majority of Canadians supported making exposure notification apps mandatory for the use of public services, such as public transit (**55%**) and in workplaces (**51%**).
- Support was somewhat lower (**46%**) for retail or grocery stores making apps mandatory.
- In contrast, opposition to landlords or condominiums making exposure notification apps mandatory (**45%**) surpassed support (**30%**).

But there are critical considerations that need to be addressed that move beyond techno-solutionism. To make certain this technology is deployed in a manner that protects users, we assessed the security and privacy vulnerabilities of contact tracing/exposure notification apps. Realizing the potential appeal of digital technologies particularly during times of crises among leaders and policymakers, we offer recommendations to governments and institutions around the world to ensure that any deployed app mitigate these risks to the greatest extent possible by:

1. Following privacy-by-design principles and using only **Bluetooth technology**, not location data;
2. Using a **decentralized approach** by keeping contact data on the individual devices of the application's users;
3. Only **collecting, storing and using data that is necessary**, including deleting data after no more than 30 days, limiting data use to public health uses only, and decommissioning the app after the pandemic is adequately contained;
4. Ensuring the app is used on a **voluntary basis only**, and passing legislation to ensure that no public or private entities can make the app mandatory to access goods, services, employment or housing, especially considering one in four low-income households do not have a smartphone; and

5. **Ensuring transparency and maintaining trust**, through transparent procurement processes, publicly available source code, comprehensive independent reviews, and ongoing oversight related to the privacy impact of the software.

Our review in June 2020 of exposure notification apps around the world indicated that **no jurisdiction had yet to fully satisfy all these conditions**, and the Canadian government had the opportunity to lead and ensure the highest standards of privacy and security.



Since then, Canada deployed its COVID Alert exposure notification app on July 31, 2020, which meets our five recommended criteria. We join Canada's privacy authorities in saying that Canadians can opt to use this technology with confidence in its privacy and security protections. We believe the app's development has been done transparently, including through engagement with the research and policy community like ourselves. However, we continue to bring to light the potential impacts of such technology on disparities and equity. We therefore continue to urge governments to pass legislation to prevent individuals from being implicitly coerced into downloading the app by institutions or entities that demand it as a requisite to provide goods, services, employment or housing.

All countries deploying exposure notification software must pay particular attention to maintaining the trust of the public through ongoing oversight of the application's efficacy alongside parallel manual exposure notification, particularly given other jurisdictions' experiences where negative risks to cybersecurity and digital privacy have outweighed apparent benefits to public health.

App-enabled exposure notification is only desirable if it feeds into a robust, people-powered public health tracing, testing and treatment system. It should not be mandatory, but a well-governed regime guided by these five principles, may support the fight against COVID-19.