

Vaccine passports can be used for surveillance under the guise of public health measures

February 23 2022, by Sze-Fung Lee, Benjamin C. M. Fung



Credit: Unsplash/CC0 Public Domain

The COVID-19 pandemic has sparked heated and passionate debates about the introduction of vaccine passports. The use of digital

vaccination certificates is becoming increasingly common in cities around the globe. Whether they would become a prerequisite for international travel is yet to be determined.

In September 2021, proof of vaccination became mandatory for individuals in [Ontario](#), [Québec](#) and [British Columbia](#) to enter "non-essential locations" such as gyms, restaurants, cinemas and exhibition centers.

Canada is experiencing a wave of protests against vaccine mandates organized by the so-called "freedom convoy." The protests were sparked by the federal government's decision to require vaccines to cross the United States-Canada border.

Should vaccine passports become mandatory, it is crucial for the public to distinguish between how these documents can be used to ensure public [health](#) and how they may violate an individual's privacy and threaten their security. While details on vaccine passports may vary in different jurisdictions, we should be asking what kind of data is being collected. How and where will the data be stored? How will data be encrypted and protected from misuse or crime?

Liberal democracies and data collection

When pressed, governments may indicate that vaccine passports only contain the information necessary to verify someone's identity and vaccine status. How a government defines "necessity" is one of the best indicators of whether the country is adopting [public health policies](#) that primarily deal with COVID-19, or if they are expanding [mass surveillance](#) and further restricting movement and activities under the guise of public health.

A vaccine passport does not need to include [health information](#) that is

unrelated to vaccination status, such as health card number or additional personal data like an address or phone number. For example, [the SMART Health Card](#), widely used in New York and California, displays only the holder's legal name, date of birth and COVID-19-related information—test and vaccine dates and locations and test manufacturer or vaccine type.

In less liberal jurisdictions, additional information is often required. For example, [Health Code](#)—an online platform introduced in Hong Kong last year—collects identity document numbers, phone numbers and addresses, as well as travel history and sites visited (including restaurants and other entertainment venues). Individual privacy is compromised.

Perhaps what is more alarming is that Health Code is a less intrusive version of other apps, such as the Chinese COVID-19 tracking app. In contrast to Ontario's public health policy that only requires proof of vaccination for non-essential locations, the Chinese app is required for some public transportation and residential areas.

The Chinese app also has a GPS-tracking function, [which sends users' location and an identification code to the police](#). The app uses color coding—red, yellow and green—to indicate a person's status, and whether they are qualified to enter public areas. Some people's health code turned yellow or red without a seemingly apparent reason, implying [the potential for Chinese authorities use the pretext of public health policy to restrict people's activities](#).

Such practices indicates a new level of digital mass surveillance in the name of public health. As Human Rights Watch researcher Maya Wang noted, this is "[one of those landmarks in the history of the spread of mass surveillance in China](#)."

Convenience versus regulation

It may make sense for to trade a certain amount of privacy for the greater good of [public health](#). But this is not as simple for those not living in a democratic country where the public can hold the government accountable. Vaccine passports can and have been developing into a new tool for mass surveillance and crackdown on its opposition in totalitarian regimes.

A system designed to indicate health status can be used as a device for restricting people's freedoms because of their political beliefs or professions. Even in more liberal democracies, the line between freedom and the public good could be easily crossed if not cautiously managed.

To ensure the Canadian government doesn't walk on the same path, public policy needs to be transparent and in compliance with existing privacy laws. No additional information such as location data should be collected or shared, and any personal data must be encrypted and kept no longer than 14 days. Last and most importantly, the use of vaccine [passport](#) "[must not be required as a condition of service](#)."

[As COVID-19 becomes endemic](#), [vaccine](#) passports may become part of monitoring and managing outbreaks. Vaccine passports have the potential for mass surveillance, and the threat to individual security is real, especially in totalitarian states. But for more [liberal democracies](#), prudent foresight will help protect the privacy rights of civilians.

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

Provided by The Conversation

Citation: Vaccine passports can be used for surveillance under the guise of public health measures (2022, February 23) retrieved 24 April 2024 from

<https://medicalxpress.com/news/2022-02-vaccine-passports-surveillance-guise-health.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.