Intelligence MEMOS

From: Bryan Thomas, Colleen M. Flood, Vivek Krishnamurthy, Ryan Tanner and Kumanan Wilson

To: Canadians Concerned About Vaccine Passports

Date: July 12, 2021

Re: **Four Privacy Choices for Vaccine Passports**

There are at least four fundamental choices regarding the design of vaccine passport systems that bear upon their privacy impacts that we discuss in our forthcoming C.D. Howe Institute Working Paper.

The first relates to the information encoded. To be useful, vaccine passports obviously need information regarding an individual's vaccination status such as the date of vaccination, as well as details regarding the vaccines they received.

Most discussions of the privacy impacts of vaccine passports assume that they must contain at least some information regarding identity, such as name, date of birth or perhaps a unique identification number.

Such identifying information does not necessarily need to be encoded into the passports for them to be useful, however. One could imagine a system of vaccine passports that record the fact that the bearer has received certain vaccinations without recording any information about the bearer's identity. Not including any identifying information on a vaccine passport would reduce the privacy risk the system poses.

The trade-off for policymakers, however, is that omitting identification information makes the system more subject to fraud and abuse. Correspondingly, policymakers must weigh the public health benefits of incorporating more identity information into a vaccine passport versus the privacy drawbacks of doing so.

The second choice relates to what information is collected by the organization issuing the passport at the time of issuance. The default assumption is that issuing organizations will simply collect and retain whatever information is encoded into the passport, but they could choose to collect more or less personal information than appears on the face of the passport. For example, the issuer could collect information about an individual's risk factors for adverse reactions without encoding that information into the passport.

Here too, there are public health benefits to collecting more information that need to be weighed against privacy risks. There are inherent privacy risks in creating any new large databases of private information, such as the risk of data breaches or the possibility that the data will be reused for some other unforeseen purpose.

The third choice relates to who should be permitted to issue vaccine passports. Under our consent-based privacy regime, there is nothing to stop any private-sector entity from developing its own vaccine passport system, so long as those entities operate within the generally applicable laws that govern the collection, retention, use and sharing of personal information.

The modalities of Canada's current vaccine rollout make it likely that only governments have the capacity to issue vaccine passports. It is noteworthy, therefore, that Canada's federal, provincial, and territorial privacy commissioners recently issued a unanimous joint statement expressing the view that "for vaccine passports introduced by and for the use of public bodies, consent alone is not a sufficient basis upon which to proceed."

The fourth choice – which is really a set of choices – relates to the technological implementation of vaccine passports.

Most discussions presume passports will be digital, on the basis that they are cheaper and faster to deploy than analog systems. This is debatable, as most large bureaucracies have systems in place to produce vast quantities of personalized documents relatively quickly. It may well be simpler and easier for governments to issue vaccine passports on paper stock incorporating some physical security features (such as watermarks or embossing) than to create secure digital systems for the issuance and verification of vaccine passports.

Many different digital technologies have been discussed in relation to vaccine passports. For example, the European Union's "Digital Green Certificate" system is based on QR codes that can be printed on paper or stored on a smartphone, while South Korea has proposed a blockchain-based vaccine passport system to prevent counterfeiting. The devil of the privacy implications of these technological choices is in the details, but digital systems raise more serious privacy concerns than analog ones because digital technologies make it much easier to collect, store and analyze data. Consider how the use of a proximity-based ID card to enter a building creates a digital record of one's movements, whereas using a key or flashing one's ID badge to a security guard does not result in the creation of any such records.

The design characteristics of a vaccine passport system have an obvious impact upon the uses that can be made of them. Even so, there is a separate set of considerations regarding how such passports can be used that is germane to understanding their privacy impacts. The first relates to who can ask to see your vaccine passport. Under background privacy law principles, individuals can consent to showing their passports to any entity that has some legitimate reason to view the passport or to such entities collecting some information that is encoded into the passport (such as the bearer's name).

Preventing the spread of COVID-19 through the verification of vaccine passports would seem to be a legitimate purpose under Canadian privacy law, although this question has yet to be decided.

Bryan Thomas is Senior Research Associate & Adjunct Professor, Centre For Health Law, Policy & Ethics, University of Ottawa, where Colleen M. Flood is Research Chair in Health Law and Policy, and Vivek Krishnamurthy is Samuelson-Glushko Professor of Law. Ryan Tanner teaches at the Faculty of Law, and Kumanan Wilson is Senior Scientist, Clinical Epidemiology Program, Ottawa Hospital Research Institute and Professor, Faculty of Medicine, at the University of Ottawa.

To send a comment or leave feedback, email us at blog@cdhowe.org.

The views expressed here are those of the authors. The C.D. Howe Institute does not take corporate positions on policy matters.