

Public Input on the Use of Contact Tracing Apps for Pandemic Management

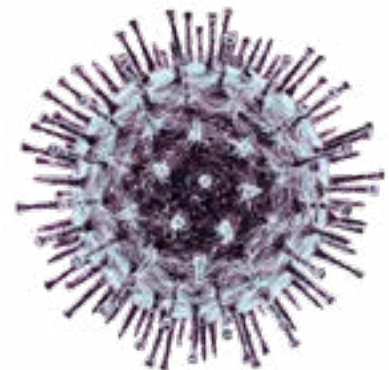
Deliberating trade-offs in COVID-19 policy making

Summary Report

July 2020
British Columbia

Colene Bentley
Michael Burgess
Kimberlyn McGrail
Kieran O'Doherty
Stuart Peacock

Vancouver, British Columbia, Canada



About this report

On May 25, 2020 three online public consultation sessions were held in British Columbia (BC) on the topic of using smart phone technology (an app) for the purpose of pandemic management. The purpose of these sessions was to seek direction from British Columbians on what values should underpin policy decisions related to the design features, data management, and uptake of a contact tracking app, should one be implemented in BC. The sessions were conducted as a pilot to determine the feasibility of holding public consultations online using Zoom technology (rather than in person) in adherence to physical distancing requirements during COVID-19, and to provide rapid, meaningful public input to decision makers on emerging pandemic policies.

This summary report provides a high-level analysis of the results of the pilot public consultation, including key findings and limitations of the data. It has been prepared as part of the Public Input into Pandemic Policy research project.

Background

The COVID-19 pandemic has led to many unprecedented public health measures, including business restrictions and closures, and physical distancing requirements. The success of these measures in managing the population spread of the virus means there are now ongoing conversations about how those restrictions might be relaxed. In BC and elsewhere, contemplating changes in policy requires first understanding the full scope of their effects, which can extend from public health to social and economic effects, and then contemplate the trade-offs that need to be considered for the next phase of policy.

Understanding the trade-offs involved in pandemic policy decisions requires relevant input from scientists, public health officials, social and business leaders, and the public. Input from the public can help outline the values at stake—such as privacy, safety, and freedom of movement—when considering the next steps in managing COVID-19, and what values trade-offs British Columbians are willing to accept as reasonable.

In May 2020 the Public Input into Pandemic Planning project consulted British Columbians to understand what is important to them as BC moves from the crisis to the management phase of the COVID-19 pandemic. The consultations were held online using Zoom technology, and involved 21 British Columbians across three consultation sessions of 90 minutes each. Participants were recruited using a strategy that leveraged the University of British Columbia's communication networks, social media platforms (Facebook, Twitter), media interviews, and targeted outreach to groups that may be uniquely affected by policy decisions (e.g. seniors organizations, anti-poverty groups). Those interested in participating in the consultations were directed to the project website (<http://chspr.ubc.ca/covid19/>) and asked to complete a brief demographic survey and indicate their availability to participate. People were also encouraged to hold their own consultations with neighbours, friends or family. Supports for these self-directed consultations were provided on the project website.

During the consultation sessions, participants were asked to consider three questions about the use of contact tracing apps for pandemic management. The questions were developed by the research team in collaboration with decision makers in BC and at the Public Health Agency of Canada. The questions were:

Question 1	If the government decides to endorse apps for pandemic management, is it also okay to use the data generated to assess or study group behaviour?
Question 2	If apps are used to support pandemic management, how should the data be managed?
Question 3	If apps are used to support pandemic management, who should be responsible for their implementation and management?

All consultation sessions were conducted by a trained facilitator and notetaker. The notetaker captured participants' feedback during the session, which participants could review online as it was documented in real time. Participants were supported in their discussions by an information booklet and the project website, which provided background information on the project and consultation questions.

Key messages

The following points represent a synthesis of the key messages from participants across the three consultation sessions. They summarize what was most important to the participants. Participants were mostly female, with higher income and education levels, and resided in BC's Lower Mainland and Interior regions. See graphs below for detailed participant characteristics. Not all groups discussed all three policy questions due to time constraints; this limitation is noted below as it applies.

Participants across all three groups strongly supported implementing a contact tracing app that could provide aggregate-level data to health professionals to help reduce the spread of COVID-19.

- They considered apps designed solely to track an infected person's contacts as too limited to be of value for pandemic management. There was broad support for using data generated from apps to identify clusters of COVID-19 cases. Some participants raised concerns about governmental surveillance if app data were used to assess crowd formation.

Participants in all groups were cognizant of the success of any contact tracking app depending upon its widespread adoption and use across the population.

- They noted the diminished utility of any app in rural areas with poor wi-fi reception, and when individuals can turn off location tracking features or simply leave their phones at home. Public education on the need for contact tracing apps was seen as a way to mitigate, in part, the problem of obtaining sufficient public uptake. Participants did not think contact tracing apps should be mandatory, however.

The two groups (14 individuals) that considered Question 2 strongly endorsed using app data for approved health research (i.e., research vetted by a research ethics board) and pandemic management.

- Participants wanted identifiable data stored for contact tracing purposes only (e.g., 14 days), and data intended for research purposes to be de-identified for longer term storage. A few participants expressed concern about data security and privacy should a centralized database be used.

Participants were concerned about who would have access to data from the app.

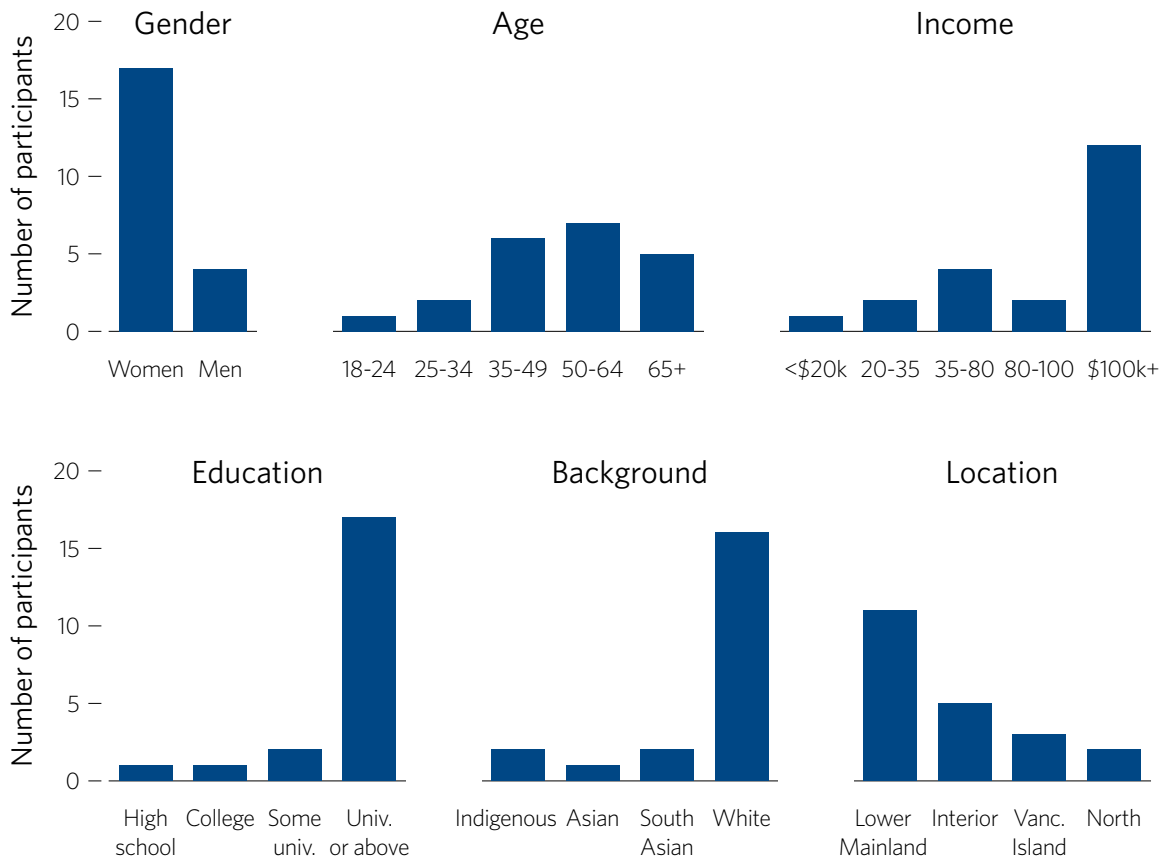
- They wanted assurances that only scientists, the government and “health authorities,” and researchers who had signed conflict of interest declarations would have access to the data. They did not want the data shared with law enforcement.

The two groups (13 individuals) that considered Question 3 did not support having the private sector implement and manage a contact tracing app, raising concerns about whether a private company would sell the data.

- However, they supported private-public partnerships that leveraged the expertise of private companies to develop the app, but the government or a non-profit entity would own and manage the data. It was important to participants that the data are owned and used by individuals they consider trustworthy. In this instance, participants specified health authorities and the BC Centre for Disease Control as acceptable government entities, and physicians and information technologists as appropriate professionals in a non-profit entity.

Participant characteristics

Twenty-one British Columbians participated in the deliberations.



Detailed results

Participants’ input is synthesized across the three groups by question. All groups deliberated at least two questions and one group deliberated all three questions in the allotted 90 minute session. One group created their own recommendation (see Question 3, below).

For each question, participants were asked to consider the options provided and give their reasons for and against each option. Then, in light of their deliberations and reasons, they were asked to vote in support of the option they deemed to be the best policy option for the people of BC. Their reasons and votes, as well as any changed perspectives as a consequence of deliberation, are reported below.

Question 1: Use of data

Apps can be used to help with pandemic management. They can track self-reported symptoms, allow self-reporting of information, and provide real-time alerts. They can also be used to track and store information on location (e.g., where you have been with your phone over the last week) and information on other phones you were near for more than a few minutes. This means that combining data from many app users could help show travel patterns, crowd formation, and general movement of people.

If the government decides to endorse apps for pandemic management, is it also okay to use the data generated to assess or study group behaviour?	
Options	<p>A. Only to help the professionals who are tracing people who have been infected by COVID-19.</p> <p>B. For contact tracing and to identify new potential clusters of cases.</p> <p>C. All of that plus to assess public movement and congregation (crowds, etc).</p>

Reasons for and against Option A: Only to help the professionals who are tracing people who have been infected by COVID-19.

- Because the data set will be incomplete (from partial uptake of the app), any decisions made on the basis of the data will be based on faulty/incomplete data, which is just as bad as not using data at all.
- Need more information on who’s monitoring real time data collection between human interactions to make a decision, and need real people to look over the data.
- Clarifying that monitoring/accessing the data is with health professionals and not law enforcement.
- Would be a good tool to help me remember where I’ve been if I need to report. Might turn it on if on a bus, but not have it on at home.
- Downfall to using app in rural areas—may not always have signal.

Question 1: Use of data

- Unequal motivation for people to opt-in to receive information, without willingness to share their own data (ex: people might want to be notified, but not be willing to contribute with their own information).
- More information for the public on how this option will enhance the system that's currently in place.
- Concerns with carrying out this app in a centralized system and the potential for data breaches, as opposed to a decentralized system with less risk.
- What kind of information is traded using Bluetooth?

Reasons for and against Option B: For contact tracing and to identify new potential clusters of cases

- Could allow contact tracing without being too permissive (i.e., Option C is being too permissive or invasive).
- Probably more public buy-in than Option C.
- Less privacy and confidentiality concerns than with Option C; also, more likely to have 60% of the population using it.
- Turn it on when in community—if there was a case, might be alerted.
- Protecting me and others (if I'm a carrier and don't know it).
- There should be an option in the app to submit your information if you want it to be used—policy folks can be clear this is an "opt in" data set.

Reasons for and against Option C: All of that plus to assess public movement and congregation (crowds, etc).

- Need more information to clarify the importance of including this as part of a contact tracing app.
- The data collection proposed in C is already done by third party apps (e.g., Google Maps) and it would be almost negligent to not use that data (or their own) if it could be used to prevent harm to people
- See people being disrespectful—not honoring 6 feet, kids playing together, etc.—app could help

- Don't have much of a problem with C while we're in an active pandemic state— as long as data are secure, private and there is an END time/date. Don't want the data being left out there or used for other purposes once the pandemic ends.
- Because this is a novel virus, it is important to use data to study how the virus is being spread, but need to set out careful rules/regulations/boundaries to ensure data is used in a safe way. Only let health authorities or scientists use data.
- Would feel empowered and more confident to go back to a little more normal life. Will also help economy.
- Concerns about privacy—Where does it end? What would we do if we knew people were congregating? C sounds too Big Brother.
- Worried about government having all that data.

Reasons cited for change of mind or as important

- Don't think you can mandate enough of the population to use the app to actually do B or C. But IF we can gather the data sets for B or C and get enough people to use the app, then Option C. But don't think we should mandate use of the app.
- We will have second wave, so C could be helpful here.
- Will have good data sets from other countries already running with C.
- If we had countries that were able to provide info on clustering—would that change your mind? It might.
- Shift from C to B: Option C already exists (the existence of other crowd congregation apps like Google Maps for traffic congestion, and restaurant apps).
- Between A and C: Initial misunderstanding of the meaning of Options A and C. Option C now seems more invasive than Option A.

Question 1: Votes per group	Option A	Option B	Option C
Group 1 (8 participants)	1	7	0
Group 2 (7 participants)	0	3	4
Group 3 (6 participants)	1	3	2

Question 1: Use of data

Question 2: Storage of data

Apps can be used to record your location and other phones your phone is near for more than a few minutes. The data that are generated can be stored on your phone, they can be automatically transferred and stored in a central database, or you can have the choice of whether the data are transferred to a centralized database.

If apps are used to support pandemic management, how should the data be managed?	
Options	<p>A. Data should remain on phones and fully private. Data should be shared only when the phone's owner chooses to do so.</p> <p>B. Data should be stored in a central database, but only accessed for contact tracing (if the phone's owner is diagnosed or has been in close contact with a diagnosed person).</p> <p>C. Data should be stored in a central database and should be available for use by health professionals for pandemic management and related approved health research.</p>

Reasons for and against Option A: Data should remain on phones and fully private. Data should be shared only when the phone's owner chooses to do so.

- Like the opt-in option—only share when owner chooses to do so. BUT if the data gets transferred to the central data base with the owner's permission, then C—use it to the best ability we can (need ethics approval).
- A is too limited—negates the exercise. If someone around you has had COVID-19, you should know.
- A is too limited because it doesn't help the science.

Reasons for and against Option B: Data should be stored in a central database, but only accessed for contact tracing (if the phone's owner is diagnosed or has been in close contact with a diagnosed person).

- Support B, but want to do everything possible to stop this pandemic. I think about the second wave and the possibility of another pandemic, so I'm leaning towards Option C.
- More inclined to support this option if data are stored for a short but sufficient storage time to (such as two weeks for individual data).

Reasons for and against Option C: Data should be stored in a central database and should be available for use by health professionals for pandemic management and related approved health research.

- Need to empower scientists to do the work they can in the most available way. Confidence with the ethics board will depend on putting strong rules in place.
- Concerned about abuse of privilege with C. I'd rather not have the data out there for a long time.
- The only way for us to surface from this is to use that data for more research. We don't have this under control on a worldwide scale or even in Canada. Right now we're lucky in BC, but don't know what is going to happen. Need to get all the data we can at this point.
- Need to explore other non-traditional policy alternatives with a focus on reducing long-term social harm by mitigating the risks of accessing identifiable data. Start with a short-term storage (such as two weeks for tracing purposes) of identifiable data and shift to long-term de-identified data for long-term research purposes.
- In addition to the above, the need to be coupled with proper public education and awareness on the long-term benefits.

Reasons cited for change of mind or as important

- Originally B, but after listening to comments, changed to C. Want this data to be useful for future decision making, so need to make it available.
- Said no to C because don't know what "related health research" is. Agreed with C until the last part of that sentence, which is too vague.
- What stopped me from voting for C is that it isn't clear what "health research" is or which health professionals will have access to the data.

Question 2: Storage of data

Question 2: Votes per group	Option A	Option B	Option C	Abstain
Group 1 (8 participants)	0	1	6	1
Group 2 (7 participants)*	-	-	-	-
Group 3 (6 participants)	1	2	3	-

*Group 2 did not deliberate Question 2.

Question 3: App implementation and management

Apps can be developed by private companies or by non-profit groups, governments or universities, or a combination of those groups. There are many apps already in use for contact tracing, and some are being adopted in multiple jurisdictions. Analysis of the data from the apps can be done by government and health system people, or by a company on a contract.

If apps are used to support pandemic management, who should be responsible for their implementation and management?	
Options	<p>A. A private company which has full access to and ownership of all aspects of the app, including the data generated.</p> <p>B. A private company, but the app functions and data are managed and controlled by government.</p> <p>C. A non-profit group that owns and controls the app functions and data (i.e., the data are not held by the government or a private company).</p>

Reasons for and against Option A: A private company which has full access to and ownership of all aspects of the app, including the data generated.

- Lack of trust—would they be willing to sell the data?

Reasons for and against Option B: A private company, but the app functions and data are managed and controlled by government

- More comfortable with the government having the data, health authorities and experts directly involved.

Reasons for and against Option C: A non-profit group that owns and controls the app functions and data (i.e., the data are not held by the government or a private company).

- Hopefully run by physicians and information technologists.

Question 3: App implementation and management

Reasons for and against a recommendation developed by Group 2:

Non-profit/private partnership where the data is owned by the government (e.g., Centre for Disease Control) and bound/protected by current personal health information laws.

- We need the resources of the private sector.
- Would like to see the government level up in the right way via a public/private partnership.
- When the province privatized seniors care, there was a lot of destruction because it became heavily focused on profit—when it’s private, the first thing to be cut is safety.

Reasons cited for change of mind or as important

- None.

Question 3: Votes per group	Option A	Option B	Option C	Option D*
Group 1 (8 participants)**	-	-	-	-
Group 2 (7 participants)	0	0	0	7
Group 3 (6 participants)***	1	2	3	-

*Independent recommendation developed by Group 2.

**Group 1 did not deliberate Question 3.

***One participant, whose session was terminated by Zoom, was unable to rejoin the session to vote.

