Test, Trace, and Isolate: Covid-19 and the Canadian Constitution

Lisa M. Austin, University of Toronto Faculty of Law
Vincent Chiao, University of Toronto Faculty of Law
Beth Coleman, University of Toronto ICCIT/Faculty of Information
David Lie, University of Toronto, Department of Electrical and Computer Engineering
Martha Shaffer, University of Toronto Faculty of Law
Andrea Slane, Ontario Tech University, Faculty of Social Science and Humanities
François Tanguay-Renaud, Osgoode Hall Law School, York University

May 22, 2020

Summary

Contact tracing is essential to controlling the spread of infectious disease and plays a central role in plans to safely loosen Covid-19 physical distancing measures and begin to reopen the economy. Contact tracing apps, used in conjunction with established human contact tracing methods, could serve as part of Canada's "test, trace, and isolate" strategy. In this brief, we consider the potential benefits of using contract tracing apps to identify people who have been exposed to Covid-19, as well as the limitations of using this technology. We also consider the privacy implications of different app design choices. Finally, we consider how the privacy impacts of contact tracing apps could be evaluated under the Canadian *Charter of Rights and Freedoms*, which provides a framework for balancing competing rights and interests. We argue that so long as apps are carefully constructed and the information they reveal is appropriately safeguarded, tracing apps may have a role to play in the response of a free and democractic society to the Covid 19 pandemic.

1. **Improving the Efficiency of Human Contact Tracing:** The public health goal of a contact tracing app should be to integrate with human contact tracing and make it more efficient rather than replace it. We need to keep humans in the loop to ensure accuracy and to maintain the important social functions of contact tracing, which includes educating people about risks and helping them access social supports.

2. **Privacy Choices:** Currently, the most privacy-protective design for contact tracing apps makes use of proximity data (via Bluetooth) through a decentralized design. This method is receiving significant technical support from Apple and Google. However, this method fails to integrate with the human contact tracing system. Other options, such as the use of location logs or a centralized registration system, are more aligned with the public health goal of integration with human contact tracing but raise additional privacy questions.

In addition to the constitutional questions raised by these privacy choices, there are two important considerations. First, social trust is important. If individuals do not feel comfortable with using a particular contact tracing app there will not be the large-scale uptake needed to make these an effective addition to human contact tracing. Second, due to various technical challenges, it is difficult to make effective contact tracing apps utilizing proximity data unless one uses the method supported by Apple and Google. However, Google and Apple prohibit app developers both from utilizing centralized methods and from utilizing location data.

3. **Constitutional Balancing:** Our privacy commissioners have discussed the need to assess these privacy choices according to the principles of necessity and proportionality. The Canadian *Charter* provides an important framework for thinking about these principles as it provides us with a framework for how to balance rights and interests in a free and democratic society. The *Charter* requires that we choose the most privacy-protective app design that meets the public health goal, so long as the benefits of meeting this goal outweigh its deleterious effects on privacy. This requires a reasonable belief in the efficacy of such an app. It also requires an assessment of the nature of the benefits, which are not just the economic benefits of reopening the economy. The currently prevailing restrictions on movement and work are themselves limitations of basic rights and liberties. Individuals who self-isolate in situations of poverty, precarious housing, mental health challenges, abusive relationships, or other vulnerabilities face challenges that affect their security of the person. There are also broader effects on equality and human flourishing. If contact tracing, enhanced by an app, reduces the

need for restrictions in the form of self-isolation, it promotes other *Charter* rights and values (e.g., security of the person) which must be balanced against the potential infringement of privacy rights.

1. Introduction

As countries gradually move through the first wave of the COVID-19 pandemic, governments around the world are looking for ways to safely loosen physical distancing measures and to begin to reopen their economies. Contact tracing has long been an essential component of any plan to control an outbreak of infectious disease, and so forms a central part of re-opening strategies. Canada is no exception to this trend. On April 28, 2020, Canada's premiers released their "First Ministers' Statement on Shared Public Health Approach to Support Restarting the Economy."[1] The Statement contains a set of principles for lifting the physical distancing measures, informed by the experience in other countries, public health, and the "shared objective" of minimizing the "risk of another wave of COVID-19 that forces governments to re-impose severe restrictions." The Statement identifies the existence of sufficient public health capacity to "test, trace, and isolate all cases" as among the measures that need to be in place in order to safely lift physical distancing restrictions.

While the Statement is silent as to how "test/trace/isolate" measures are to be implemented, it is clear about the goal of these measures. Testing and contact tracing measures are to be in place

> so that suspected cases are detected quickly and all confirmed cases are effectively isolated, while *all close contacts are traced, quarantined, and monitored.*[2]

These different steps -- **identification** of close contacts, **quarantine** of those individuals, and **monitoring** of them -- all raise questions regarding the legitimate bounds of public health surveillance.

In this brief we address the use of contact tracing apps, used in conjunction with established human contact tracing methods, as part of the identification step of the "test, trace, and isolate" strategy. We do not discuss testing or quarantine but note that these are additional components to what must be a comprehensive strategy. For example, if Canada does not have sufficient testing capacity then this can call into question other components of the strategy.

There is a great deal of concern, nationally and internationally, that the use of contact tracing apps raises alarming privacy issues, which if unchecked could create a surveillance state that will be difficult to reign in after the pandemic. This brief contributes to this discussion in the Canadian context. Our privacy commissioners have stressed that governments need to apply the principles of necessity and proportionality to any proposed measures that impact upon

[1] The Council of the Federation, "First Ministers' statement on shared public health approach to support restarting the economy" (28 April 2020), online (pdf): <https://www.canadaspremiers.ca/wp-content/uploads/2020/04/FM_Joint_Statement_April_28_2020.pdf>.
[2] *Ibid* at 3.

privacy.[3] These principles must be understood within a broader legal framework than data protection law, specifically the Canadian *Charter of Rights and Freedoms*. We therefore seek to broaden the discussion by examining the *Charter* framework for understanding the rights at issue and when infringements of those rights can be justified in a free and democratic society.

This broader context is especially important when effective contact tracing is seen as an essential strategy for easing lockdown measures. Currently we are containing rates of infection through mandatory social distancing, and in some cases mandatory quarantine. These measures infringe liberty, and do so at a scale Canadians have never before experienced. They also engage a set of values that go beyond population health and economic activity: *Charter* values such as security of the person, equality, and broader ideas of human flourishing. Just as the current measures rest on a complex balancing of rights and interests, so too will whatever strategies are put in place as we transition out of lockdown.

We also seek to place digital contact tracing apps within the broader context of human contact tracing. Apps cannot replace human contact tracing but instead must be integrated into the overall system of human contact tracing, as a means to accurately and comprehensively identify people who have been exposed to COVID-19, and connect them to appropriate public health education and resources. When deciding whether some app functionality is necessary or not, we need to understand necessity in relation to this public health goal of making human contact tracing more efficient, and so more effective at containing the spread of the virus to the point where more freedoms can be safely exercised.

2. The Need to Make Human Contact Tracing More Efficient

Many states are pursuing the development of contact tracing apps, which could alert their users when they have been in close contact with someone who has been diagnosed with COVID-19. Both privacy advocates and public health professionals are largely skeptical of the utility of these apps to stem the current pandemic.[4] Those who are willing to entertain that a contact-tracing app may play some role typically stress that no technology will replace the

---

[3] Office of the Privacy Commissioner of Canada, "Commissioner issues guidance on privacy and the COVID-19 outbreak" (20 March 2020), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200320/>.

[4] See e.g. Fred Vogelstein & Will Knight, "Health Officials Say 'No Thanks' to Contact-Tracing Tech", *Wired* (8 May 2020), online: <https://www.wired.com/story/health-officials-no-thanks-contact-tracing-tech/>; Reed Albergotti & Drew Harwell, "Apple and Google are building a virus-tracking system. Health officials say it will be practically useless.", *Washington Post* (15 May 2020), online: <https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/>; Ashkan Soltani, Ryan Calo & Carl Bergstrom, "Contact-tracing apps are not a solution to the COVID-19 crisis", *BrookingsTechstream* (27 April 2020), online: <https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/>; Jay Stanley & Jennifer Stisa Granick, "ACLU White Paper: The Limits of Location Tracking in an Epidemic" (8 April 2020), online (pdf): <https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic>.

invaluable work of human contact tracing, nor should it.[5] If contact tracing apps are to supplement and support the work of human contact tracing, they need to be able to fill some of the gaps that human contact tracing is currently unable to effectively address while also ensuring that human contact tracing remains in the foreground, in order not to lose the vital social support components of the existing contact tracing system. We elaborate on these points in this section and then, in the following section, discuss some of the privacy-related design choices involved in contact tracing apps in more detail.

As described by Public Health Ontario, "Contact tracing is a process that is used to identify, educate and monitor individuals who have had close contact with someone who is infected with a virus… Contact tracing can help the individuals understand their risk and limit further spread of the virus."[6] Human contact tracing is done by public health staff – or in the case of a pandemic like COVID-19, by public health staff as supplemented by battalions of contract or volunteer contact tracers. The core component of contact-tracing is the interview with the newly diagnosed person, aiming to collect the names and contact information of everyone with whom the person has come into close contact: at present, this means coming within 6 feet for at least 15 minutes, starting 48 hours before the onset of symptoms.[7] In densely populated areas, strict adherence to social distancing helps reduce the problem of not knowing how to contact the people a newly diagnosed person came into contact with in this way – for instance, at a long line-up at a grocery store or on public transit. But as Ontario's chief medical officer Dr. David Williams recently lamented, newly diagnosed community transmissions in Ontario remain stubbornly constant at about 200 a day despite the current lock-down and social distancing measures, and the human contact tracing system has not been able to identify the source of many of these infections.[8]

Partly this is a problem with the pace of human contract tracing, which is a labour-intensive process in the best of times and which the COVID-19 pandemic requires at an unprecedented scale. A delay of a day or more in the face of an easily transmissible disease means that infections potentially proliferate with every hour that a contagious person comes into contact

---

[5] See e.g. Ada Lovelace Institute, "Exit Through the App Store: A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis" (20 April 2020) at 11, online (pdf): <https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf>; Patrick Howell O'Neill, "Five things we need to do to make contact tracing really work", *MIT Technology Review* (28 April 2020), online: <https://www.technologyreview.com/2020/04/28/1000714/five-things-to-make-contact-tracing-work-covid-pandemic-apple-google/>; Centers for Disease Control and Prevention, "Digital Contact Tracing Tools of COVID-19" (20 April 2020), online (pdf): <https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contact-tracing.pdf>; Fred Vogelstein & Will Knight, *supra* note 4.

[6] Public Health Ontario, "COVID-19 Contact Tracing Initiative" (last modified 11 May 2020), online: <https://www.publichealthontario.ca/en/diseases-and-conditions/infectious-diseases/respiratory-diseases/novel-coronavirus/contact-tracing-initiative>.

[7] Centers for Disease Control and Prevention, "Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic" (29 April 2020), online: <https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html>.

[8] Rob Ferguson, "Community spread of COVID-19 remains stubbornly high, Ontario's top doctor says", *Toronto Star* (8 May 2020), online: <https://www.thestar.com/politics/provincial/2020/05/08/ontario-records-another-459-covid-19-cases-44-deaths.html>.

with others. A contact-tracing app that is able to alert a person that they have come into close contact with a newly diagnosed person within the timeframe where the illness is likely contagious could potentially help to eliminate that lag that is still costing avoidable new infections, if people receiving an alert self-isolate until they can be tested for the virus.

So far at least, the 15 minutes of close contact guideline for possible transmission means that casually passing someone on the sidewalk is not something an app would need to track and log. However, it is possible that clusters could be associated with, say, a store facing the challenge of how to inform customers of an outbreak among employees[9]; notification would also help inform employees of a workplace experiencing an outbreak, without having to wait for management to inform them.[10] Being able to identify possible clusters – new infections linked to the same store or the same workplace for instance – could also be app-assisted, although here too it is mainly the specialized skills of the human contact tracers that will likely reveal these sorts of contact hot spots. As Dr. Williams stated, "We need to get to that kind of granularity"[11], whether we get there with the assistance of an app or not.

Human contact tracers do not tell the people they call who exposed them to infection, as their job is really to support each individual in their efforts to reduce the likelihood of exposing others. As a medical officer and contact tracer with Alberta Health Services, Dr. Grace Salvo, recently stated, "Some people at first, they're surprised. Other people are actually expecting it because maybe the person who came back positive was able to call them [before] we were," but "[o]ften, in the end, they're very grateful to know and to have been informed that they were in contact."[12] Notification of exposure to an infected person is only the very beginning of a person's relationship to public health supports: as Dr Tom Friedan, former director of the CDC in the United States stated, "Some of the best practices [of contact tracing] include ensuring that people have food in their home, that they have security, that they have the ability to care for elders or children who may need to be removed from the house," which means that "Public

---

[9] Muriel Draaisma, "Loblaws closes west-end store after 'several team members' test positive for COVID-19", *CBC News* (9 May 2020), online: <https://www.cbc.ca/news/canada/toronto/loblaws-several-staff-members-test-positive-covid-19-dupont-christie-1.5563319>.

[10] Andrew Russell, "After failing to publicly reveal COVID-19 outbreak, Ontario meat plant now has 24 confirmed cases", *Global News* (7 May 2020), online: <https://globalnews.ca/news/6913049/coronavirus-ontario-meat-packing-plant/>.

[11] Ferguson, *supra* note 8. The ethics of publicly revealing this level of granularity again requires that the social supports provided by human contact tracers be foregrounded. At present, local data revealed to the public at large is only at the public health unit scale, which may cover a large geographic area or a large population: See e.g. Chris Brackley, "What are maps really saying about COVID-19 in Canada?", *Canadian Geographic* (1 April 2020), online: <https://www.canadiangeographic.ca/article/what-are-maps-really-saying-about-covid-19-canada>. See also Public Health Ontario, "Ontario COVID-19 Data Tool", online: <https://www.publichealthontario.ca/en/data-and-analysis/infectious-disease/covid-19-data-surveillance/covid-19-data-tool>.

[12] Caley Ramsay, "How does COVID-19 contact tracing work? Alberta doctor explains", *Global News* (22 April 2020), online: <https://globalnews.ca/news/6854518/alberta-covid-19-coronavirus-contact-tracing/>.

health works by making the patient the VIP of the program, and that's what we need to do here.[13]

Although contact tracing apps could make some components of contact tracing more efficient, they cannot replace human contact tracing and so need to be integrated into the human contact tracing process. For example, human contact tracing involves educating people about risks and helping them access social supports as they self-isolate and monitor themselves for symptoms, and ideally are given access to testing even if asymptomatic -- this vital component cannot be done via contact-tracing apps. By having a human reach out to potential contacts, public health authorities also gain some insight into whether people are acting upon their knowledge of exposure and taking steps to get tested or self-isolate.

Another reason why the adoption of digital contact tracing cannot replace the need for human contact tracing is that the contact tracing apps do not have the coverage necessary for achieving public health goals. Not everyone has a smartphone and voluntary adoption rates in other countries continue to be low. This leaves gaps in coverage and these gaps will have a disproportionate effect on individuals who either do not have smartphones (such as the elderly or people of lower socio-economic status) or have reason to distrust government surveillance and so not use the apps (such as members of communities traditionally overly surveilled).

Integrating human contact tracing with digital tracing could increase the accuracy of both methods. First, this would allow for digital tracing methods to fill in some of the gaps and delays outlined regarding human contact tracing. Second, having a human-in-the-loop can help address the problem of false positives and false negatives associated with the contact tracing apps, since a human contact tracer could discuss the level of exposure a person is likely to have actually had. One of the main developers of Singapore's TraceTogether app explains this in the following way:

> *Encounters between individuals can be classified into close, casual and transient contacts for epidemiological purposes, based on proximity and duration of contact. However, these classifications depend on factors such as location/environment. For example, short-duration encounters in enclosed spaces without fresh ventilation often constitute close contact, even if encounter proximity and duration do not meet algorithmic thresholds.*
>
> *Since Bluetooth-based contact tracing solutions do not, by themselves, record location/environment data, this information needs to be obtained through other means — a human-led contact tracing interview.*
>
> *A human-in-the-loop system is also necessary to allow judgment to be applied, given the high likelihood of pre-symptomatic transmission of the SARS-CoV-2 virus. Since time is*

[13] Casey Ross, "5 burning questions about tech efforts to track Covid-19 cases", *STAT* (15 April 2020), online: <https://www.statnews.com/2020/04/15/coronavirus-digital-contact-tracing-tech-questions/>.

of the essence, contact tracers may preemptively wish to trace selected second-degree close contacts of a COVID-19 patient, in cases where there is a high likelihood of exposure and infection, even if the first-degree close contact has yet to test positive. For example, there may be epidemiological value in tracing close contacts of a close relative of an infected person.

A human-out-of-the-loop system will certainly yield better results than having no system at all, but where a competent human-in-the-loop system with sufficient capacity exists, we caution against an over-reliance on technology.[14]

Appreciating the role of human contact tracing allows us to see that the public health goal of contact tracing apps should be framed in terms of supporting and supplementing human contact tracing. In the following section we will outline some of the design choices of contact tracing apps and what some of the trade-offs between this public health goal and privacy look like.

3. Privacy Choices

There are various types of data that can be used to help understand who is a close contact of someone who is diagnosed with COVID-19. Some of this is location data. In human contact tracing, individuals are asked to provide details of where they have been in order to help contact tracers identify who might have been exposed. But other sources of location data can assist with this, such as mobile data (for e.g., from your cell phone communicating with cell towers), transaction data held by financial institutions (recording location of transactions), and GPS data on your phone. Similarly, some locations can track who uses their services, such as airlines with their passenger logs. Recently Washington State asked restaurants to keep logs of their customers in order to assist contact tracing, although this was quickly changed from a requirement to a request for customers to voluntarily comply.[15]

Location data is considered highly sensitive from a privacy perspective, which is why there has been a lot of attention to using "proximity" data instead. Bluetooth signals can be exchanged between two cell phones and an anonymous record of this encounter created. Contact tracing apps can use these records to determine who has been in "proximity" to a known COVID-19 case. Proximity data does not reveal location but, like all methods of contact tracing, it does potentially reveal one's social contacts.

There are privacy issues associated with using both location data and proximity data to do contact tracing. One set of issues is to limit the identifiable information collected, shared, and

---

[14] Jason Bay, "Automated contact tracing is not a coronavirus panacea" (10 April 2020), online (blog): <https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98>.

[15] King 5 Staff, "Gov. Inslee says businesses no longer required to keep daily customer log but it's encouraged", *King 5* (15 May 2020), online: <https://www.king5.com/article/news/health/coronavirus/washington-state-contact-tracing-daily-customer-log-governor-inslee/281-1f2579bc-38ce-4275-b39f-8de66c50807c>.

disclosed, to only what is necessary to fulfil the purposes of contact tracing. Privacy protection of any of this data can be accomplished to various degrees and through various means including encryption, anonymization, and decentralized storage. The Office of the Privacy Commissioner of Canada has a helpful framework that outlines these considerations.[16] In general, it is easier to manage privacy risks with proximity data than with location data. However, the more general question is which type of data -- proximity data, location data, or some combination -- is more likely to meet the public health goal of making human contact tracing more efficient. Proximity data typically only registers that a device enabled with the bluetooth app came within a set range of another device that has been associated with a person who has tested positive for the virus. Whether the app is able to determine the duration of the contact is variable, and it typically does not record the environment or location within which that contact occurred, which reduces the granularity of the information and likely leads to many more notifications than would present a real risk of infection. Retaining a log of location data, whether associated with the proximity data or not, could help with this more granular analysis. Location logs, even if only stored locally on a device, could be used as an aid in a human contact tracing interview, helping a person remember where they have been, which may provide a more accurate assessment of risk of infection to others. This information currently exists on many smartphone mapping apps, such as Google Maps, which passively track daily movement. Such logs are already on our phones (and in the cloud); but it would be up to the user to share this information with health authorities, as it would not be bundled into the existing Apple-Google contact-tracing paradigm (discussed below).

Another set of privacy issues are concerns about the potential abuse of this data if held by the state, or by a corporation. Human contact tracing involves public health officials gathering data about both known COVID-19 cases as well as their contacts. However, it starts from a known case and then, in a targeted manner, learns about other particular individuals. Digital contact tracing apps utilize a “bulk surveillance” technique -- they depend on the collection of either the proximity data or location data (or both) of *all* app users and then use this information to match against known COVID-19 cases in order to identify close contacts; the more users the better this method works. Because of this difference with human contact tracing, digital methods are more privacy invasive. If this data is held and managed centrally by public health authorities then those authorities will have more information about more people than they would through human contact tracing methods.

There are different methods for addressing the concerns about the potential abuse of this data. Legal responses include passing legislation that would require that the data is only used for contact tracing purposes, that imposes strict sunset clauses, and that provides for forms of oversight. Technological responses include “decentralized” models for contact tracing apps. The difference between the apps that utilize a “centralized” or “decentralized” model may refer to one or both of: 1) whether the data is held in a central database or on individual devices, and 2)

[16] Office of the Privacy Commissioner of Canada, “A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19” (April 2020), online: <https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid>.

whether disclosure of any such data is initiated centrally or by individuals. This choice, in turn, affects how much information is available to public health authorities.

In early April, Apple and Google announced that they would collaborate to create the technological infrastructure to better enable the use of bluetooth signals to engage in decentralized proximity tracing, and make this interoperable as between Android and IOS devices.[17] Although Apple and Google are not directly creating contact-tracing apps, they are effectively setting the terms of how those apps will operate if they are to make use of the Apple-Google API. The basic idea is that phone users exchange Bluetooth beacons with random rotating identifiers. When an individual tests positive they can choose to upload their "keys" to the app's server. These keys, and the keys of anyone else who has tested positive in that area, are regularly downloaded by other app users and matched against the data on their phone. If there is a match, the app user gets a notification. Although Apple and Google contemplate that public health authorities will develop these apps, these health authorities will only get to access a limited amount of data: 1) if someone chooses to report their positive diagnosis their keys get added to those that are broadcast to other users; 2) if a match occurs a user gets notified through the app but does not receive information about the infected person apart from the day of the contact, its length, and the Bluetooth signal strength (in order to deduce distance from the contact).[18] What this ultimately means is that although individual app users get notification about their exposure, a human contact tracer working with a confirmed COVID-19 case cannot use these apps to learn about the contacts of that person. It is a system that would largely operate in parallel with human contact tracing, rather than be closely integrated with it. This is likely why Apple and Google now refer to this as "exposure notification" rather than contact tracing.

A number of countries have opted to create a centralized, rather than decentralized app. For example, Australia's COVIDSafe app uses the bluetooth method of proximity tracing but adopts a centralized model in order to integrate it with manual contact tracing.[19] When an individual downloads the app, they are asked for their name, cell phone number, postcode, and age (within a range). This is then used to create a unique reference code, which is encrypted. When two people who use the COVIDSafe app come into proximity with one another the app notes the date, time, Bluetooth signal strength (an approximation of distance between contacts), duration and reference code of the other app user. If an individual comes into contact with a person who has tested positive and has uploaded that information to the data store, public health staff gain access to that person's registration information. This information is then used to support human contact tracing rather than to automatically alert other users about their potential exposure, and

[17] Apple, Press Release, "Apple and Google partner on COVID-19 contact tracing technology" (10 April 2020), online: <https://www.apple.com/ca/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>.
[18] Apple & Google, "Exposure Notification – Frequently Asked Questions, v1.1" (May 2020) at 5-6, online (pdf): <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf>.
[19] Australian Government Department of Health, "COVIDSafe app" (last modified 13 May 2020), online: <https://www.health.gov.au/resources/apps-and-tools/covidsafe-app>.

so as with contact tracing interviews generally, is able to take into account a fuller range of factors that affect risk.[20]

In order to support the privacy of information that is not expressly needed for human contact tracing, COVIDSafe encrypts the proximity data collected, making it inaccessible even to the app user, and then destroys this data after 21 days if no contact with another user flagged as testing positive occurs. Further, because of the centralized design, the Australian government has committed to not using this information for additional purposes (including law enforcement), to ensuring that the data remains within Australia, and to destroying it at the end of the pandemic. In addition, Australia is going to make it a crime for anyone to require an individual to download the app as a condition of employment or service. However, the legislation needed to support these promises is still in draft form.

There are many choices, therefore, in terms of types of data collected and models for implementation, that affect the trade-offs between privacy and utility. Although some states reportedly have used mobile data,[21] and have even matched this with other types of location data,[22] there is increasing convergence on the use of apps utilizing bluetooth technology, although some make use of this and location (GPS) data. As we have outlined, there are good public health reasons for adopting a centralized approach as well as to utilize both proximity data and location data, although these choices are less privacy-protective than a decentralized approach utilizing proximity data alone. In the following section we outline how the Canadian *Charter* would frame these trade-offs.

There are two additional sets of general considerations. First, if individuals do not feel comfortable with using a particular contact tracing app there will not be the large-scale uptake needed to make these an effective addition to human contact tracing. Therefore, even if a centralized design with strong safeguards is constitutionally permissible it might not be effective if citizens do not actually trust it and therefore do not use it.

Second, it is difficult to make effective contact tracing apps utilizing proximity data unless one uses the Google/Apple API, due to various technical challenges. However, Google and Apple prohibit app developers both from utilizing centralized methods and from utilizing location data. Several states have announced that they will make use of the Apple-Google API, including Austria, Germany, Ireland, Italy, Malaysia, the Netherlands, and Switzerland.[23] Some of these countries, like Germany, had been pursuing a centralized version before announcing a switch in

---

[20] *Ibid.*

[21] Natasha Lomas, “Israel passes emergency law to use mobile data for COVID-19 contact tracing”, *TechCrunch* (18 March 2020), online: <https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/>.

[22] Some states also used banking records and video footage to track people: Justin Fendos, "How surveillance technology powered South Korea’s COVID-19 response", *BrookingsTechStream* (29 April 2020), online: <https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/>

[23] See chart in Patrick Howell O’Neill, Tate Ryan-Mosley & Bobbie Johnson, “A flood of coronavirus apps are tracking us. Now it’s time to keep track of them.”, *MIT Technology Review* (7 May 2020), online: <https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/>.

strategy. Other countries, like Singapore, Australia, the UK, and France, have pursued a centralized strategy although some -- like Singapore and Australia -- have recently indicated that they might switch to the Apple-Google model because it is difficult to get the Bluetooth technology to work effectively without making use of the Apple-Google API.

4. Constitutional Balancing

The Office of the Privacy Commissioner recently released a framework for assessing the privacy impacts of COVID-19 initiatives.[24] Much of the framework draws upon the fair information practice principles (FIPPs) that underpin many Canadian privacy laws, both provincially and federally, and in the private and public sectors. These principles include ideas of lawful authority, purpose limitation, safeguards, openness, accountability and oversight, and limited data retention. The framework also discusses the need for measures to comply with the principles of "necessity and proportionality." These principles do not stem directly from FIPPs but are rooted in constitutional requirements and international human rights norms and, in particular, how these provide strict justification tests for limitations on rights.[25] In this section we outline what the privacy issues look like from an explicitly *Charter* lens, as well as how the questions of necessity and proportionality would be framed from a *Charter* perspective. One of the benefits of doing so is that it brings into focus the complex set of *Charter* rights and values that are at issue in trying to create an effective contact tracing regime, in circumstances of considerable uncertainty, in order to ease up on our current "lockdown" measures.

Section 8 of the *Charter* states that "[e]veryone has the right to be secure against unreasonable search or seizure." The Supreme Court of Canada has understood s.8 to protect privacy in a variety of overlapping forms. The most traditional form of privacy protection afforded by s.8 is "territorial" privacy, essentially privacy in one's home. Section 8 also protects "personal" privacy, for instance with regard to extraction of bodily samples. Finally, and most broadly, s.8 protects "informational" privacy, which includes efforts to secure information about individuals that do not otherwise engage territorial or personal privacy.[26] Tracking a person's movements in public spaces, for instance, could give rise to an informational privacy claim.[27]

Contact tracing engages a person's interests in informational privacy, as the information requested would be highly likely to reveal "core biographical information" about a person's life. Indeed, obtaining such information (presence in churches, schools or other congregating points; social contacts) is precisely the point of contact tracing. In other words, the kind of information captured by contact tracing -- whether conducted by a human or by an app -- is likely to attract a

[24] Office of the Privacy Commissioner of Canada, *supra* note 16.

[25] For example, the federal *Privacy Act* that regulates the federal government's data practices has no requirement that data collection be either necessary or proportionate, only that it "relates directly to an operating program or activity of the institution" (s.4). Other legislation incorporates some aspects of these principles but not as robustly as we find in the *Charter* framework.

[26] *R v Tessling,* 2004 SCC 67 at paras 20-23.

[27] *R v Wise,* [1992] 1 SCR 527, [1992] SCJ No. 16.

"reasonable expectation of privacy." It can also engage a person's privacy interest in anonymity, which is also included in informational privacy.[28] Location data and proximity data can reveal details of movements and social interactions that would otherwise remain anonymous.

There are two main consequences. First, any power to compel someone to reveal that kind of information must be authorized by law, with both the terms of the enabling law as well as particular exercises of power under it subject to reasonableness review.[29] While the Supreme Court has authorized search powers on a post-hoc, common law basis, a more secure foundation would be to ground the power to compel release of contact and location information in legislation. Any authorizing legislation would, of course, need to provide safeguards to ensure that the information is collected, stored and used in an appropriate manner.

Second, in the more likely case in which suspected infectious individuals are asked to voluntarily agree to turn over such information, any such consent must be adequately informed. Primarily, this is a matter of ensuring that those giving consent are apprised of the specific purposes for which their information will be used.[30] Information regarding data retention, use of identifying information and similar concerns (e.g., the risk that third parties will be able to infer the person's identity) should also be conveyed in a clear and concise manner. Increasingly, an analysis of the reasonableness of state action under s.8 also involves looking at questions of safeguards, including tailoring information use to specifically enumerated purposes and having accountability mechanisms in place.[31] This suggests the need for authorizing legislation that would put in place such protections.

The *Charter*, of course, contemplates the possibility that a government may justifiably infringe a person's *Charter*-protected rights. Given that we are focused on voluntary disclosure of information to public health officials, s.8 of the *Charter* is likely to be fairly easily satisfied, essentially just requiring adequately informed consent with respect to information over which individuals have a reasonable expectation of privacy and reasonable safeguards to protect against unconsented-to uses. Privacy rights are held by individuals, and individuals may waive them if they so choose.[32] However, *Charter* rights can still be at issue when the state collects personal information voluntarily through an app. Although the case law remains undeveloped, numerous courts have indicated that s.7 also protects privacy as an aspect of liberty or security of the person.[33] A government-sponsored app that collects more information than it needs, operates with a high level of inaccuracy, or fails to protect it through adequate safeguards can

[28] *R v Spencer*, 2014 SCC 43 at paras 41-44.
[29] *R v Collins*, [1987] 1 SCR 265 at 278, [1987] 3 WWR 699.
[30] *R v Borden*, [1994] 3 SCR 145, [1994] SCJ No. 82.
[31] See *R v Fearon*, 2014 SCC 77; *United States of America v Wakeling*, 2014 SCC 72 [*Wakeling*].
[32] There is a slight complication in that the Supreme Court has taken the view that one person may not "waive" another person's privacy rights, and there is a colourable argument that asking an infectious individual to reveal information about his or her contacts would be analogized to the former unilaterally waiving the privacy rights of the latter. See *R v Marakah*, 2017 SCC 59 at para 41. If the Supreme Court is disinclined to revisit this issue, then this may become an occasion for a s.1 justification.
[33] B.(R.) v. Children's Aid Society of Metropolitan Toronto, [1995] 1 S.C.R. 315, 122 DLR (4th) 1; Cheskes v. Ontario (Attorney General) (2007), 87 OR (3d) 581, 288 DLR (4th) 449.

affect an individual's liberty and security of the person through potentially exposing sensitive information to parties or for purposes not consented to, or because inaccuracies lead to improper actions regarding testing or quarantine. Even if the use of such apps is voluntary, if the state strongly encourages their use as a condition of easing other social restrictions, there remains an element of state pressure that heightens state obligations to safeguard the information. Because properly safeguarding information has also been held to be part of the "reasonableness" analysis under s.8 of the *Charter* it would likely, under s.7, affect the analysis regarding whether a particular violation of life, liberty, or security of the person was consistent with the principles of fundamental justice.[34]

If privacy rights are infringed, the *Charter* framework then shifts to balancing competing rights and interests under section 1. Section 1 of the *Charter* "guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society". To flesh out what these "reasonable limits" mean, the Supreme Court of Canada developed what has come to be known as the "Oakes test".[35] More generally, this provides the basis for understanding how the *Charter* frames questions regarding necessity and proportionality, which, as noted above, are also increasingly understood to be key tenets of data protection. There are two main branches of the *Oakes* test: 1) is there a "pressing and substantial" objective that can justify an infringement of rights; and 2) are the means proportional to the achievement of that objective? The second branch has three steps: a) rational connection (that the means is rationally connected to the objective); b) minimal impairment (that there are no less rights-impairing means of reasonably achieving the objective); and c) final balancing (that the beneficial effects outweigh the deleterious impacts).[36]

We are not in a position to speculate about what an adequate s.1 justification would look like at this point given that such analysis relies heavily upon specific facts. However, a few points are worth emphasizing here. First, even if contact tracing is deemed to infringe s.8 rights in some manner, the currently prevailing restrictions on movement and work are themselves limitations of basic rights and liberties. Hence, if widespread contact tracing is practically required as a condition of lifting those restrictions, then policy makers face a conflict between vindicating section 7 and 8 rights to privacy and other s.7 rights to life, liberty and security of the person. This should weigh heavily in the first step of the analysis, as to whether there is a "pressing and substantial" reason to adopt a system of contact tracing.

Second, much of the public discussion of contact tracing apps has focused on what, in *Charter* terms, would fall under the minimal impairment step of the second branch. This includes many of the technical considerations regarding how much personal information an app collects, what information public health learns, etc. It is important to note that the minimal impairment test

---

[34] *Wakeling*, *supra* note 31; See also *R v Mills*, [1999] 3 S.C.R. 668 at para 88, addressing the overlap between s.8 and the principles of fundamental justice.
[35] *R. v. Oakes*, [1986] 1 S.C.R. 103, 26 DLR (4th) 200.
[36] For an overview, see generally: Department of Justice Canada, "Section 1 – Reasonable limits" (last modified 17 June 2019), online: *Charterpedia* <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art1.html>

does not require that the state choose the most privacy-protective design of a contact tracing app -- what it requires is that the state choose the most privacy-protective design that meets the public health objective. As outlined in the previous section, there are some important questions regarding whether the decentralized bluetooth strategy meets public health objectives or sacrifices them to a degree in order to provide stronger privacy protections.

Third, when analysing the third step of the balancing, which asks whether beneficial effects outweigh deleterious impacts, the general context of using contact tracing to move to a post lockdown world is important. Individuals who self-isolate in situations of poverty, precarious housing, mental health challenges, abusive relationships, or other vulnerabilities face challenges that affect their security of the person. If state action in the form of contact tracing reduces the need for restrictions in the form of self-isolation, then it promotes *Charter* values even as it potentially infringes other *Charter* rights. Another set of issues are those associated with broader ideas of human flourishing. This would include ideas of social justice and equality, economic considerations, jobs, education and the role these play in our lives and in the sustainability of our society. Although things like economic prosperity might seem divorced from questions of freedom and democracy, we now have many examples of how widening social inequality and instability can lead to the rise of authoritarian threats to democracy. The promotion of *Charter* values and the furtherance of social justice goals can be factored into the beneficial effects.

Fourth, policy makers are acting under conditions of great uncertainty, along a great many dimensions: biological, medical, epidemiological, social and economic. This should weigh heavily in the second step of the analysis. It is unreasonable to expect policy makers to be able to definitively show that contact tracing is minimally impairing relative to the other available options when the policy space is so fluid and uncertain: it is difficult to determine what the other *technological* alternatives are, much less secure adequate information to enable reliable prediction of their expected rate of success relative to each other. This does not mean that the state can introduce contact tracing methods based upon speculation, but it does require sensitivity to context.

5. Conclusions

Contact tracing apps cannot replace human contact tracing. Alone, they are not accurate enough and these problems of accuracy would have disproportionate impacts on vulnerable groups. They also cannot replace the social functions of human contact tracers, who educate individuals about risks and help them to access needed social supports. Given this, the public health goal of contact tracing apps must be to supplement human contact tracing and make it more effective.

Of the many different general app designs in circulation, those that make use of proximity data (using Bluetooth signals) and a decentralized design are the most privacy protective. However,

they do not integrate with human contact tracing as effectively as apps that use a centralized design and/or additional location data. There are two additional considerations that also weigh heavily in deciding upon a contacting tracing app. The first is social trust: an effective app needs widespread adoption and so people need to trust its design. The second is technical: apps that make use of proximity data through Bluetooth signals will be more effective if they use the Apple/Google API and these companies restrict centralized designs for apps using this API as well as the collection of location data.

When assessing whether departures from the more privacy-protective design are necessary and proportional, we should use the *Charter* as our framework for thinking about rights and their justified limits. Government sponsored apps, even if voluntary, can infringe privacy rights if proper safeguards for the data are not in place. However, important *Charter* rights and values are also at stake in remaining within a state of “lockdown” and an assessment of post-lockdown strategies must be assessed against this complex array of constitutional values with consideration given to the great conditions of uncertainty that policy makers are operating under.