The Race to Trace

Security and Privacy of COVID-19 Contact Tracing Apps

June 2020

cybersecure policy exchange

Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is a new initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

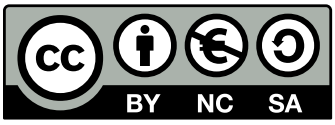
Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University that develops leaders and solutions to make progress on our most pressing civic challenges. Through research and policy activation, leadership development, and civic convening, the Leadership Lab is building a new generation of skilled and adaptive leaders, at all ages and stages, to build a more trustworthy, inclusive society.

This initiative is made possible by the generous contributions of **Royal Bank of Canada**, which enable our team to independently investigate pressing public policy issues related to cybersecurity and digital privacy. We are committed to publishing objective findings and ensuring transparency by declaring the sponsors of our work.

How to Cite this Report
Masoodi, M.J., Andrey, S., Bardeesy, K. & Choudhry, Z. (2020, June 8).
Race to Trace: Security and Privacy of COVID-19 Contact Tracing Apps.
Retrieved from https://www.cybersecurepolicy.ca/racetotrace

350 Victoria St, Toronto, ON M5B 2K3



Contributors
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Communications and Knowledge Mobilization, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Braelyn Guppy, Marketing and Communications Lead, Ryerson Leadership Lab
Mohammed (Joe) Masoodi, Policy Analyst, Ryerson Leadership Lab
Kate Pundyk, Policy and Research Assistant, Ryerson Leadership Lab
Yvonne Su, Policy Lead, Ryerson Leadership Lab

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange
For more information, visit: https://www.cybersecurepolicy.ca/

Executive Summary

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 are **contact tracing apps** — 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 contact tracing, provided that enough of the population uses the app.

Though a contact tracing app has yet to be deployed nation-wide, many Canadians seem ready to embrace this technology. A **survey of 2,000 Canadians** from mid-May 2020 finds that:

- Majorities of Canadians support making contact tracing apps mandatory for the use of public services, like public transit **(55%)** and in workplaces **(51%)**, though in both cases only one in four strongly support such an approach.
- Support is somewhat lower **(46%)** for retail or grocery stores making apps mandatory.
- In contrast, opposition to landlords or condominiums making contact tracing apps mandatory **(45%)** surpassed support **(30%).**

But there are critical considerations that need to be addressed to make certain this technology is deployed in a manner that protects the security and privacy of Canadians.

While there will be security and privacy vulnerabilities with any contact tracing app, Canadian governments and institutions should ensure that any app mitigates 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 Canadians' individual devices;

(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 deleting 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 Canadian households do not have a smartphone; and

(5) Being **transparent** and maintaining **trust**, in part through transparent procurement, publicly available source code, comprehensive independent reviews and ongoing oversight.

A review of contact tracing apps implemented in other jurisdictions indicates that no jurisdiction has yet to fully satisfy all these conditions, and should they choose to proceed, Canadian governments and institutions must ensure **the highest standards of privacy and security**. Canada must pay particular attention to maintaining the trust of the public through ongoing oversight of the contact tracing app's efficacy alongside parallel manual contact tracing, particularly given other jurisdictions' experiences, where negative risks to cybersecurity and digital privacy have outweighed apparent benefits to public health.

App-enabled contact tracing is only desirable if it feeds into a strong, 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.

Intent of this Report

Contact tracing is one of the most discussed and misunderstood policy issues as we grapple with COVID-19.

In this report, the first through the Cybersecure Policy Exchange, we explain what contact tracing is, its context, share our most up-to-date understanding of the issue, and reveal Canadians' attitudes toward the use of the technology. We give policy recommendations to help ensure that contact tracing is done responsibly, and in a way that builds public trust.

This report is in dialogue with work by policy-makers, technologists, academics and think tanks in Canada and internationally, and we look forward to informing and evolving the work with this community.

What is Contact Tracing?

Contact tracing is a process used by public health officials to identify individuals who have had close contact with someone who has an infectious disease; inform those individuals of their potential infection; and help prevent their infection of others. Contact tracing is used as a primary means of infectious disease control and has been used in past outbreaks, including severe acute respiratory syndrome (SARS), foot-and-mouth-disease, smallpox and avian influenza.[1]

Contact tracing has been used frequently in previous public health crises in Canada. In fact, contact tracing is required by law in most Canadian provinces in the case of HIV diagnoses.[2] Canadian public health officials have also used contact tracing in previous 21st century coronaviruses, with SARS (2003) and Middle East respiratory syndrome (2012).[3,4]

Contact tracing is typically conducted manually by public health staff.[5] Once an individual is confirmed as infected with a virus, they are interviewed about their past activities and the people they have come into contact with since they were infected. Efforts are then made to identify these potentially infected individuals to provide them with information, including how to prevent the disease and any other actions that they should take. This may include quarantine or isolation for high-risk contacts. Regular follow-ups are conducted with these potentially infected individuals to monitor symptoms and test for signs of infection.[6]

Contact Tracing During COVID-19

To control and further mitigate the spread of COVID-19, governments around the world have mainly relied on traditional public health measures such as: encouraging increased personal hygiene and social distancing; banning social gatherings; limiting travel; promoting and enforcing self-isolation; and increasing testing for the virus.[7]

Existing and new digital technologies capable of real-time monitoring at the individual and aggregate level have been proposed in tandem with traditional public health measures, followed by claims that they will improve their effectiveness.[8,9]

These technologies have included contact tracing using cell/smartphones or other mobile devices, such as wearables. The commonly-cited rationale behind mobile contact tracing is to increase the volume, accuracy and reach of manual contact tracing, which can be labour-intensive and relies on both an infected person's memory and the ability to identify and reach contacts who the infected person does not know personally, such as contacts from public transit or retail stores.[10]

Supplementing manual contact tracing with digital technology is not new. Reports as early as 2000 reveal public health authorities in California accessing the social networking sites of patients who were positively diagnosed with a sexually transmitted infection in order to notify their sexual partners who lacked contact information.[11,12] In the current COVID-19 pandemic, British Columbia is asking restaurants to collect and store the contact information of its customers, as well as using credit card and loyalty program data, to facilitate contact tracing.[13,14] However, mobile contact tracing that automatically tracks and records every interaction is a new approach that, prior to COVID-19, had yet to be tested or evaluated.

How Contact Tracing Apps Work

Contact tracing applications (apps) work by calculating the proximity of phones or other mobile devices, automatically tracing sustained intersections of individuals, including those who later test positive for COVID-19.[15]

Although there are a number of ways to calculate the proximity of mobile devices, many governments and organizations around the world have rolled out contact tracing apps that rely on Bluetooth technology and/or cellphone location data to do so.[16]

The contact tracing apps locate and keep a record of contact when a device that is running the same app gets close to another for a defined period of time. The apps then typically can alert or notify users if they have come close to someone who has a confirmed or presumed case of COVID-19.

Other COVID-19 Mobile Technologies

Contact tracing apps have features that make them distinct from other mobile technologies that have been developed or proposed to assist with the spread of COVID-19, including:

Self-Diagnosis: These apps ask users a series of questions related to the most common COVID-19 symptoms. Those answers evaluate the user's risk of having contracted COVID-19 and provide recommendations to self-isolate or get tested. This functionality has also been included in some contact tracing apps, such as the UK's NHS app.[17]

Aggregated Data Analytics: This approach uses the data collected from mobile devices' location data in aggregate to understand movement patterns and how they have changed over time, to assess the effectiveness of public health interventions. Hot spots can also be tracked to inform people to avoid certain areas due to apparent clusters of infections.[18] Some contact tracing apps also map hot spots, including for example the contact tracing app developed by the Quebec-based Mila.[19]

Quarantine Enforcement: Some governments and private institutions have used mobile devices' location data to monitor compliance with imposed isolation or quarantine by requiring people to install an app, for instance in China and South Korea.[20,21]

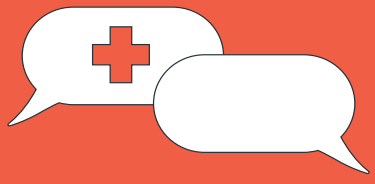
Manual Contact Tracing

Person confirmed positive for COVID-19

Public health provides guidance on next steps (e.g., self-isolation)

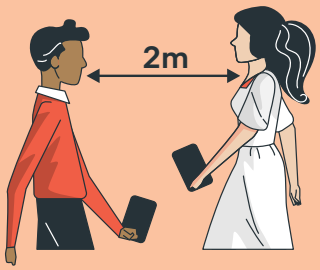
Public health interviews person on recent activities and contacts

Public health identifies and reaches out to contacts with guidance

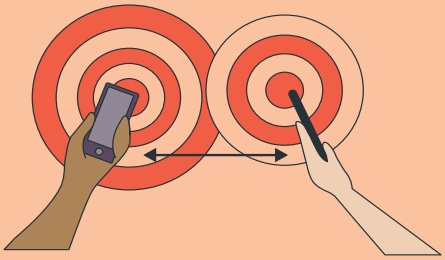


Regular follow-ups are conducted with contacts to monitor symptoms

App-Enabled Contact Tracing



Person 1 and Person 2 come within two metres for 15 minutes



Their apps exchange an anonymous key to log their interaction

Person 1 becomes COVID-19 positive

Person 1 enters they are COVID-19 positive into the app, triggering an alert to all phones Person 1 has exchanged keys with

Person 2's phone receives an alert, notifying them and to contact public health

Security And Privacy Considerations for Contact Tracing Apps

As with any digital technology, the security and privacy of its users must be protected. The stakes are greater for digital technology endorsed and encouraged by governments and institutions, and even more so when that encouragement is under the premise of protecting people's health.

When building contact tracing apps, it is important to consider what potential harms and vulnerabilities users could be exposed to. The most top-of-mind issue is the potential for a data breach of personal information, particularly considering the elevated level of cybercrime targeting health organizations during the pandemic.[22]
A positive COVID-19 diagnosis can result in social stigma and harassment, particularly for those from otherwise vulnerable groups.[23]

Beyond the individual risk, businesses and organizations risk reputational and financial damage as a result of being identified as a place where individuals became infected. For these reasons, contact tracing apps need to be built to minimize such harms, by making privacy and security central to their design.

The Cybersecurity and Digital Privacy Concerns with Contact Tracing Apps can be broadly grouped into five categories:

1. Technology Design
2. Data Governance
3. Data Minimization and Retention
4. Voluntary Use
5. Transparency and Trust

Given the risks of deploying new technology of this nature, governments and public health authorities need to publicly address each of these concerns in the development, deployment and ongoing use of this technology.

Technology Design

Contact tracing apps have primarily been designed to calculate the proximity of mobile devices using:

- Bluetooth technology;
- location data; or
- a combination of these features.

Apps that rely on location data, such as satellite-based GPS and/or triangulation of cell towers, have been subject to significant criticism, as the technology can be used to expose sensitive and personally-identifiable information, such as users' home addresses, workplaces and routines.[24] Although developers have proposed apps that anonymize users' data, past research has shown that it is possible to reverse engineer anonymized datasets to reveal individual identities through a process of combining other data sources.[25, 26, 27]

The use of individual location data by contact tracing apps increases risks for users in the event of a cyberattack or data leak.[28] It is worth noting that awareness of the importance of limiting mobile location data collection is rising, with opt-in rates falling significantly last year.[29] Furthermore, research suggests that location data is unlikely to be precise enough to track close and sustained contact, and to meaningfully predict the risk of COVID-19 transmission.[30]

Bluetooth, on the other hand, does not calculate location but rather communicates directly with other devices using signals through standards-based technology, making it less likely for apps using this technology to reveal sensitive and personal information of users often tied to location data.[31] Bluetooth technology can also achieve significantly more accurate distance measurements (usually within a range that is less than 100 feet), though the accuracy of Bluetooth signals can still degrade amid high levels of signal interference, which can occur in high-density buildings or streets. In addition, no technology design can prevent some false positives in the COVID-19 context, such as picking up sustained close contact through walls or cars, or not taking into consideration the use of masks.[32]

Bluetooth-based apps, however, are not without cybersecurity and privacy risks. Because Bluetooth signals are broadcast openly, security experts warn about potential for wrongful surveillance of users' devices.[33] There is a risk of bad actors actively monitoring and intercepting the signals of app users to identify those who are COVID-19-positive. It is then possible to reveal individual identities, for example on social media, to 'name and shame' individuals.[34]

Bluetooth technology is also vulnerable to spoofing and duping.[35] In such cases, threat actors intercept the signals for the purpose of either omitting or falsifying data. For instance, someone could capture a user's signals and broadcast them to another location, making the user appear to be in two different places at once.[36] Researchers have also found ways to intercept Bluetooth signals and either block or send bogus notifications, including false alerts

telling users they have been in contact with an infected person.[37]

Recommendation: While there are still security and privacy risks, contact tracing apps should follow privacy-by-design principles using Bluetooth technology only, as location-based apps pose significantly greater risk for personal identification.

Data Governance

There are two data governance approaches to contact tracing apps, and governments are split on which model to adopt.[38]

Under the first centralized model, collected anonymized data on users' interactions is regularly uploaded to a remote server. The server analyzes the data and determines which devices interacted with a COVID-19-positive case and should be contacted.[39] Depending on the design, the server may also be able to tie that data to individual identities,[40] as is the case with the national contact tracing apps in Australia,[41] Norway[42] and Singapore,[43] which require users to share their phone numbers.

The centralized model has been favoured by some governments and public health authorities (e.g., France and the UK) who argue that the approach provides more control to the authority in question over notification and follow-up with contacts, as well as additional insight into the spread of the virus and how well the app is performing.[44]

Security and privacy experts have raised concerns over the centralized model, arguing that it expands government access to intimate details about users, including their relationships and links with others, potentially leading to future misuse and abuse.[45, 46] Under this model, the central government authority is entrusted to properly handle and secure device-linked personal data, including keeping the data inside the country and safe from cyberattacks.[47]

By contrast, a decentralized model gives users more control over their contact data by keeping it on their mobile device. In this model, the mobile device downloads information on only those individuals who have been identified as COVID-19-positive and processes whether the users, represented by unique codes, have interacted in the past. If the mobile device finds a unique code that matches any codes that are periodically downloaded from the server, the user receives a notification through the app with further instructions. Thus, while the model still uses a server, that server has no access to contact interactions and is not responsible for processing or informing clients of contact. Among the supporters of this approach is the privacy-focused consortium of European academics, DP-3T, who argue for contact tracing apps to follow a decentralized approach.[48]

Mostly notably, Apple and Google – which together run operating systems on 99% of Canada's smartphones[49] – have also favoured a decentralized approach in jointly developing an application programming interface (API) for approved apps run by government health agencies (which it calls 'exposure notification'

rather than contact tracing), allowing for improved Bluetooth interoperability between their operating systems.

In addition to using Bluetooth technology only, the current Apple/Google-proposed design does not upload any data from users who are not diagnosed with an infection and also does not collect specific location data from users.[50] It is worth noting that experts observe the proposed design may still collect some general location data in order for users to have periodic downloads of infected users filtered to their region, rather than downloading the entire world's database of positive cases.[51, 52]

Some countries that developed apps earlier on — relying on a centralized model — have chosen or are considering switching to a decentralized model, which may be due to an awareness of their increased security and privacy vulnerabilities,[53] as well as technical issues involving interoperability on some models of the iPhone and battery consumption.[54]

Recommendation: Contact tracing apps should use a decentralized approach to reduce the security and privacy risks created by a central database.

Data Minimization & Retention

A number of important considerations for security and privacy have been raised with respect to how contact tracing apps collect, store and retain data. Any data collection and retention beyond what is necessary, whether by governments, private institutions or individual devices, adds additional vulnerabilities for misuse and cybercrime.

First, the data collected should be minimized to what is necessary to carry out effective contact tracing. Anonymous data stored in a server from users with a positive diagnosis, for example, could still include IP addresses or other metadata that can allow for personal or location identification. For instance, while the Apple/Google project indicates that IP addresses should not be stored, it is up to app developers to follow this policy.[55]

Second, the data should only be retained for as long as it is epidemiologically useful for contact tracing. That means data on devices should only be stored for the period of time that COVID-19 can be contagious, in addition to a feasible window to allow for testing and notification. Our understanding is that deleting data after no more than 30 days would be appropriate, based on the current evidence on COVID-19 transmission. Any data stored on servers, such as positive diagnoses, should be deleted after its use for contact tracing. While time of contact is a data variable that should be stored to allow for effective data deletion, the app should also not provide an exact time that users came into contact with a positive case, to reduce the risks of personal identification.

The app itself and all linked data should also be removed and permanently deleted when the COVID-19 pandemic has been adequately contained. Governments and public health authorities should provide a clear and public

explanation of how this sunset point will be determined, including for example its connection to rates of community spread and/or vaccine deployment. If implementation is successful, it could be tempting for public health authorities to keep the app in place for future pandemic outbreaks or other diseases. A clear sunset methodology ahead of deployment, which could include users having to periodically renew their informed consent, will help to keep decision-makers accountable.

Third, the use of the data should be limited to the purpose for which it was collected. Concerns have been raised about the risk of function creep and increased state surveillance.[56, 57, 58] Function creep is the use of technology beyond that for which it was originally intended. An example of function creep for contact tracing is the collected data being used by other agencies, including law enforcement. Given that Ontario has already embraced sharing the personal information of COVID-19-positive cases with police, this is not a speculative concern.[59] If there are data-sharing agreements with other entities, governments must be transparent about their existence, rationale and conditions.

Recommendation: Contact tracing apps should only collect, store and use data that is necessary, including built-in functionality to automatically and permanently delete mobile data after no more than 30 days. The apps and their data should be limited to public health uses only, with a clear expiration date that ensures all data are permanently deleted when the pandemic is adequately contained.

Voluntary Use

Most Western countries, including Canada, have proposed that the use of contact tracing apps be voluntary, fully "opt-in" (meaning that residents must choose to use the apps) and require the informed consent of users. Other countries, including China and India, have made downloading contact tracing apps mandatory for their citizens.[60,61]

Despite Canada's assurances that these apps will be voluntary, there is potential for coercive approaches that challenge informed, voluntary consent. Some governments, businesses and organizations are considering requiring the use of a contact tracing app for individuals to gain entry to specific locations or to allow employees to come to work.[62]

Singapore, for example, now requires check-ins at all workplaces, educational and health care institutions, shopping malls, grocery stores and hairdressers.[63] When asked, the UK's National Health Service did not rule out the potential for data from its contact tracing app being shared with employers.[64] A recent survey of U.S. businesses found nearly a quarter planned to evaluate contact tracing technology as part of their office reopening strategy.[65]

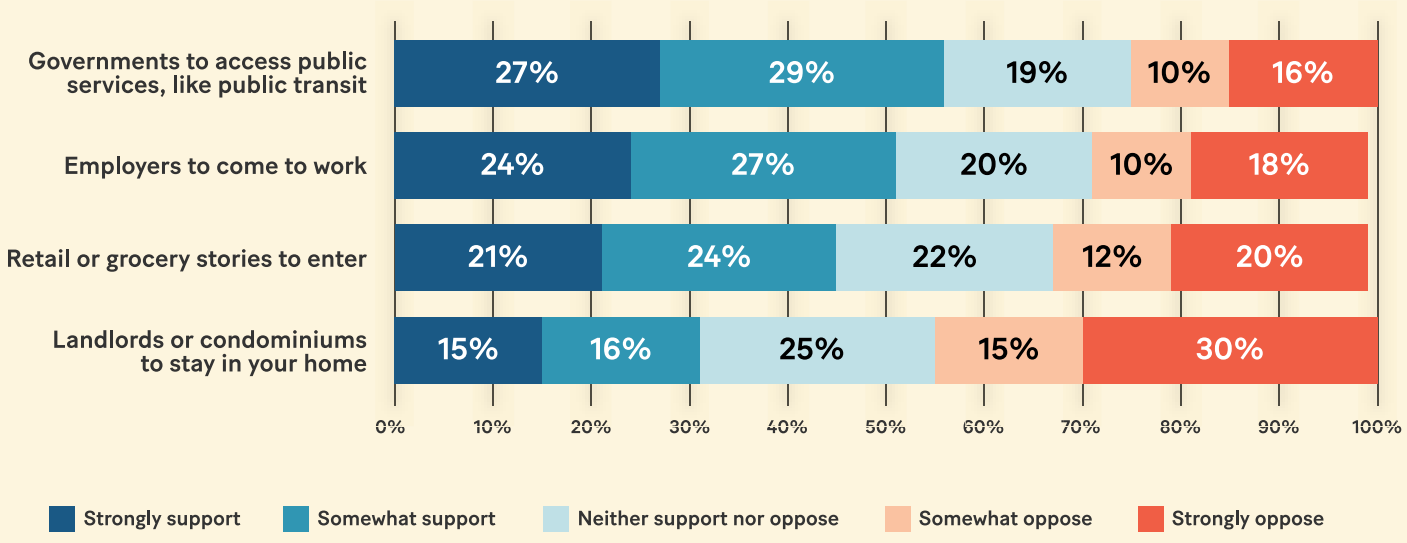
We conducted a representative survey of Canadians in mid-May 2020 to gauge their views on different organizations making contact tracing apps mandatory. We found support for such an approach varied significantly, depending on the organization in question:

- Majorities of Canadians supported making contact tracing apps mandatory for the use of public services, like public transit (55%) and in workplaces (51%), though in both cases only one in four Canadians strongly supported such an approach.
- Support was somewhat lower (46%) for retail or grocery stores making apps mandatory.
- In contrast, opposition to landlords or condominiums making contact tracing apps mandatory (45%) surpassed support (30%).
- Between 19% and 25% of Canadians neither supported nor opposed the different scenarios, representing a significant lack of certainty about this approach.
- Support and opposition for mandatory apps were remarkably consistent across regions, age groups, education levels and gender (see Table 1). There was less consistent support across income, which we explore more below.

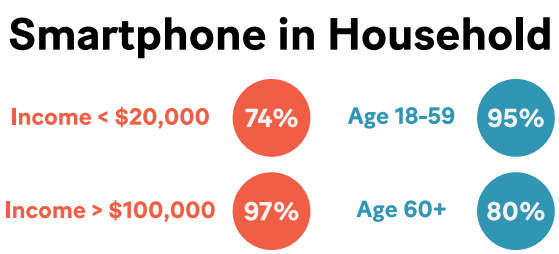
Requiring access to a mobile device for mobility, employment, education, services or housing has high potential to reinforce and exacerbate existing inequalities. Implicit coercion to use the app, particularly by those in a position of power such as an employer or landlord, will result in unequal treatment and negative consequences for those who cannot, which will likely be already disadvantaged groups.

Support for Organizations Making Contact Tracing Apps Mandatory

A smartphone app has been proposed that would anonymously notify you if you have been physically close to someone who has been diagnosed with COVID-19. To what extent would you support the following organizations making it mandatory to download this smartphone app:



According to Statistics Canada's Survey of Household Spending, 73% of households in the lowest income quintile had a mobile phone in 2017, compared to 89% overall and 97% in the highest income quintile.[66,67] Our survey found this had not changed significantly in 2020, with 74% of households with incomes under $20,000 indicating they own a smartphone, compared to 91% overall and 97% of households with incomes above $100,000. Significant gaps were also observed by age, with 80% of those aged 60+ having a smartphone, compared to 95% of those aged under 60 (see Table 2). Moreover, access to a device does not guarantee it is connected to a data plan or home internet to make a contact tracing app operable.[68]



The level of public support for making contact tracing apps mandatory underlines why government action is needed to prevent discriminatory outcomes. In fact, support for mandatory contact tracing apps drops among low-income Canadians, with average support for the four scenarios at 38% for those with household incomes under $30,000, compared to 48% average support for household incomes above that threshold (see Table 1).

For low-income households without a device, or where one device is shared among multiple members of the household, there are currently limited options available to acquire a mobile device to participate equitably in contact tracing. Programs established in response to COVID-19 to loan or provide mobile devices to those in need have, to date, been targeted at school-aged children. There are calls to offer a similar program to workers and small businesses.[69] For a regime of contact tracing using apps (with appropriate safeguards) to be taken up widely, such programs will indeed need to be made much more widely available.

Other jurisdictions have already made advancements to prevent such a need. American legislators, for instance, have drafted a bill aimed at regulating contact tracing apps, including making it illegal for any person or entity to discriminate against or make unavailable goods, services and accommodations to individuals choosing not to use an app. Australia passed legislation in May 2020, making it illegal to require individuals to download their contact tracing app in order to enter a premises, or to receive or provide any goods or services. The legislation also bans any person outside of public health authorities from collecting, using or disclosing data from their contact tracing app.[70] A group of academics from the University of Newcastle has drafted a similar bill that would ensure no one in the UK is penalized for not having a phone or other device, including leaving the house without it or failing to charge it.[71]

Recommendation: Contact tracing apps should be voluntary, fully opt-in and require informed consent. The federal, provincial and territorial governments should pass legislation to ensure public and private entities cannot make it mandatory to have access to the app in order to access goods, services, employment or housing.

Transparency & Trust

Developing mobile applications for contact tracing purposes is new, and it remains unclear whether the technologies will prove effective against the spread of COVID-19. Those jurisdictions that have deployed contact tracing apps to date have not reported them being particularly helpful, and what success they do have appears to depend in large part on the availability and timeliness of testing capacity and continued investment in parallel manual contact tracing.[72,73,74]

Before proceeding, governments should transparently and comprehensively assess all issues and risks with contact tracing apps — including legal, technical and practical concerns — as well as broader societal issues of equity, and the immediate and long-term impacts of these apps on civil liberties.[75,76,77,78] While recognizing the need for urgent action to protect public health, this is not a time for privacy and security considerations to be set-aside — not least because maintaining the trust of the population is critical to successful adoption of this technology.

To be most effective against the spread of COVID-19, reports suggest that close to 60% of a population need to use the contact tracing app.[79] No jurisdiction that has released an app, with a voluntary adoption policy, has seen a download rate approaching this level. For context, the most downloaded app in the U.S., Facebook, has an adoption rate of 69%.[80]

If governments plan to proceed with a contact tracing app deployment, they should provide a clear and unambiguous explanation for how the apps will be implemented and operate, including how misuse and discrimination will be prevented and privacy rights will be minimally impaired on an ongoing basis.[81] This should include full transparency to the public in how the apps are procured, evaluated, developed and maintained on an ongoing basis, including the role of third party technology providers.

Independent assessments of the apps by both privacy commissioners and cybersecurity experts, as well as releasing open source code, can play an important role in identifying potential flaws and should be considered before governments or institutions deploy apps. Federal, provincial and territorial privacy commissioners issued a joint statement outlining considerations to be addressed during app development.[82] The National Cybersecurity Consortium and universities from across Canada have also released a detailed set of guidelines to reference for these reviews.[83]

Independent reviews, as well as clear and robust complaints mechanisms and ongoing and transparent review of efficacy and effectiveness, can enhance trust and acceptance by the population. With new and untested technology of this nature, it is critical that an ongoing mechanism is available to identify and mitigate issues as they arise, including legal mechanisms for enforcement in instances of non-compliance.

Regardless of the technical design of contact tracing apps, the consensus is that security and privacy risks will exist regardless of scenario.[84, 85] As experts begin to converge around Bluetooth-based decentralized models of contact tracing apps, supported by likes of Apple/Google and DP-3T, it needs to be understood that, despite their privacy-focused framework, these are not perfect systems without security and privacy risks to continuously prevent, mitigate and monitor.

As an example, depending on the design of the app, individuals could use contact tracing apps to intentionally generate false positives of COVID-19 infection, particularly since there is no verification of user identity.[86] This would undoubtedly result in lost trust in the app, and individuals potentially ignoring genuine notifications. One possible safeguard to prevent this includes designing the app such that only registered health care providers or public health officials can verify positive diagnoses.[87]

Systems of contact tracing may roll out by province, potentially guided by a pan-Canadian framework. The principles in this section should form the basis of a more lasting framework of technological co-operation. Federal, provincial, municipal and Indigenous governments, informed by regulators, public health and technology policy advice, should institutionalize and codify the practices of a well-regulated contact tracing regime. A standing secretariat that sits at the intersection of technology and public health could help oversee this regime. It could also help co-ordinate ongoing research, so that app-driven contact tracing regimes, and other matters related to the intersection of technology and public health, can be further improved.

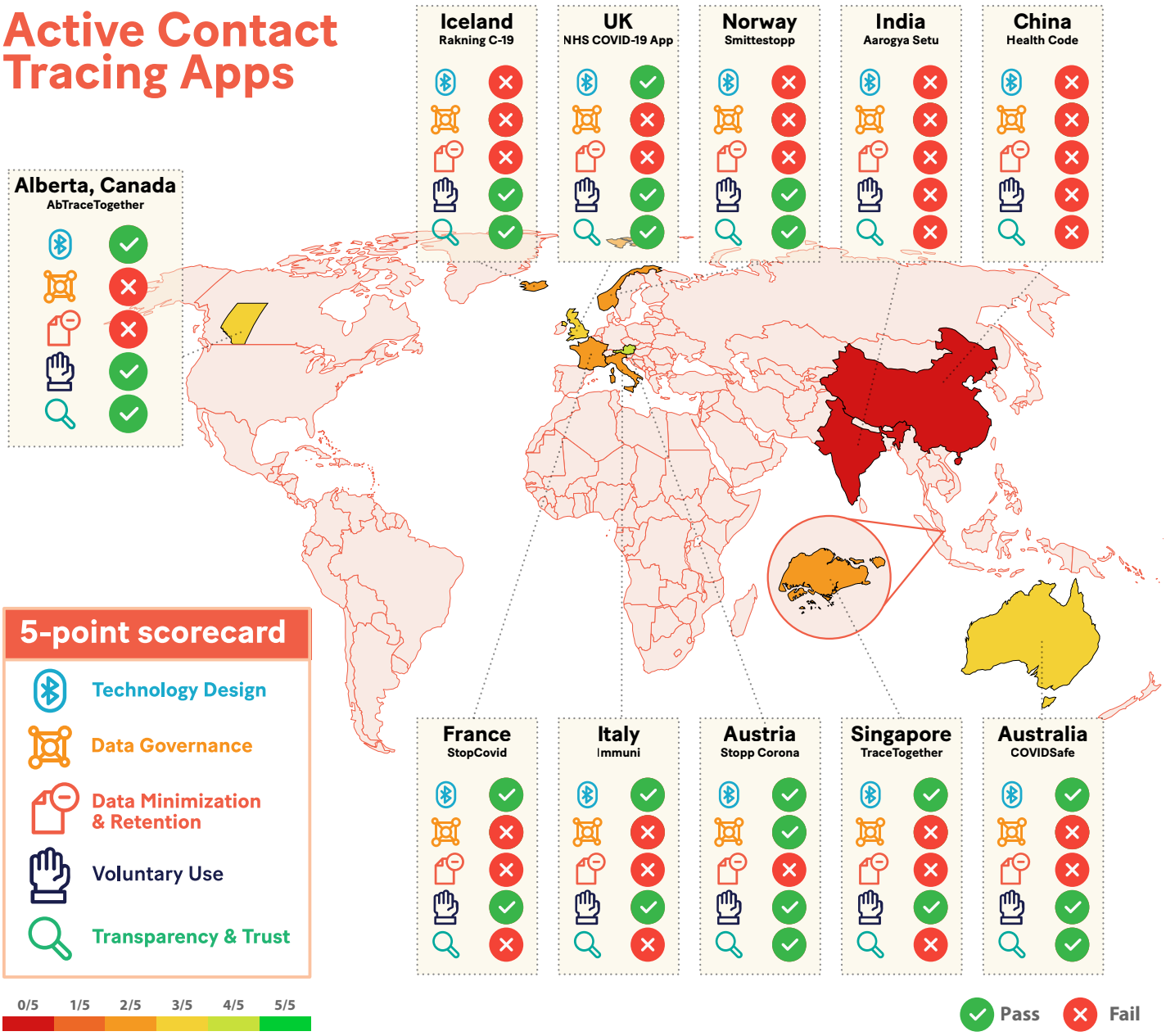
Recommendation: Contact tracing apps should be transparent through a transparent procurement process, publicly available code and comprehensive independent review, as well as maintain trust of the population, including through medical verification of positive diagnoses and ongoing oversight and review of the app and its efficacy. Transparent procurement, review and oversight should ultimately be co-ordinated by a standing secretariat dedicated to developing learnings around app-based contact tracing, and related issues at the intersection of technology and public health.

Review Of Active Contact Tracing Apps

To date, there have been innumerable contact tracing apps proposed or developed around the world, though many of these are without the backing of government or public health.[88,89] A reported 22 jurisdictions are now choosing to adapt to, or plan to introduce, apps using Apple/Google's API, including Canada.[90, 91 ,92] Switzerland is now testing the first app built using the API as part of the DP-3T project.

This is a rapidly changing landscape — but as of the end of May 2020, 29 apps have been introduced that are backed by national governments and are already or soon-to-be used by the public.[93] We have performed a review of some of these apps, in addition to Canada's only active app in Alberta, to illustrate our five recommendations for security and privacy.

Active Contact Tracing Apps



Notes: This scorecard is based on a review of publicly available information as of the end of May 2020, with inspiration from the MIT Technology Review's Covid Tracing Tracker. The methodology for receiving a passing assessment for each category is as follows:

1. Technology Design: The app uses only Bluetooth technology and does not track location data.
2. Data Governance: The app uses a decentralized approach, keeping contact interactions on the device.
3. Data Minimization and Retention: The app only collects, stores and uses data that is necessary, including built-in functionality to automatically and permanently delete mobile data after no more than 30 days, limiting its use to only public health, with a clear expiration date ensuring all data is permanently deleted after the pandemic is adequately contained.
4. Voluntary: Government has not made use of the app mandatory by all residents/citizens.
5. Transparency and Trust: At least three of the following are in place: an independent security or privacy impact assessment; open source code; positive diagnoses are verified by a health authority; and process in place for ongoing oversight/monitoring.

Conclusion

Since COVID-19 has spread across the world, governments and institutions are increasingly looking at proposed technology to help mitigate its impact. Technologies capable of real-time mass monitoring at the individual and aggregate level are gaining traction, accompanied by arguments that they will improve the effectiveness of traditional public health measures against this unprecedented challenge.

Though a contact tracing app has yet to be deployed nation-wide, federal and provincial governments have expressed interest and intent in doing so, with Alberta already having implemented its own app. There are a number of critical security and privacy risks and considerations to this type of technology, and we stress that these must be addressed in a transparent manner before it is implemented — not least because public trust in the app is critical to sufficient take-up for the technology to provide meaningful assistance to public health efforts. In fact, the effectiveness of this technology to control the spread of COVID-19 remains unclear, with several jurisdictions claiming no positive effect.

It should be understood that, even with the most privacy and security-focused approach, contact tracing apps are not perfect systems, and that vulnerabilities and risks will be intrinsically a part of any networked technology. That said, our recommendations are meant to mitigate these risks to the extent possible, including:

1. While there are still security and privacy risks, contact tracing apps should follow privacy-by-design principles using **Bluetooth technology only,** as location-based apps pose significantly greater risks for personal identification.
2. Contact tracing apps should use a **decentralized approach** to reduce the security and privacy risks created by a central database.
3. Contact tracing apps should **only collect, store and use data that is necessary,** including built-in functionality to automatically and permanently delete mobile data after no more than 30 days. The apps and their data should be limited to public health uses only, with a clear expiration date that ensures all data are permanently deleted when the pandemic is adequately contained.
4. Contact tracing apps should be **voluntary, fully opt-in and require informed consent.** The federal, provincial and territorial governments should pass legislation to ensure public and private entities cannot make it mandatory to have the app in order to access goods, services, employment or housing.
5. Contact tracing apps should be **transparent** through a transparent procurement process, publicly available source code and comprehensive independent review, as well as maintain **trust** of the population, including through medical verification of positive diagnoses and ongoing oversight and review of the app and its efficacy. Transparent

procurement, review and oversight should ultimately be co-ordinated by a standing secretariat dedicated to developing learnings around app-based contact tracing, and related issues at the intersection of technology and public health.

As our review indicates, no national app has yet to fully satisfy all of these conditions; and should they choose to proceed, Canadian governments have an opportunity to lead by example in this regard, in deploying the highest standards of privacy and security. Canada, though, must pay particular attention to the last recommendation and maintain the trust of the public through ongoing review of the contact tracing app's efficacy alongside parallel manual contact tracing, particularly given other jurisdictions' experience, where negative risks to security and privacy have outweighed apparent benefits.

It is presumed that app-enabled contact tracing will work best in support of public health objectives if it is implemented at scale. There are ample civil liberties, equity and public policy reasons to reject a mandatory regime required to get scale. That said, a well-governed technology with some coverage, and feeding into a strong manual tracing, testing, and health system, may still be better than manual tracing alone.

Hand-washing, mask-wearing, physical distancing — these are some of the tactics that are recommended by public health officials to governments, institutions, and people and their families to help contain the pandemic.

To that, public health could add a mobile technology solution: app-enabled contact tracing.

If it is well-designed and governed, it may be one more enabler of the strategy. In an age where technology platforms can help amplify mistrust and division, successfully building a regime with these robust protections may help prove out a larger point: that well-designed and -governed technology, developed and used transparently and responsibly in the public interest, can build trust, and protect our democracy.

About the Authors

Mohammed (Joe) Masoodi is a Policy Analyst at the Cybersecure Policy Exchange and the Ryerson Leadership Lab. Joe has been conducting research and policy analysis on the intersections of surveillance, digital technologies, security and human rights for over six years. He has conducted research at the Surveillance Studies Centre at Queen's University and the Canadian Forces College. He holds an MA in war studies from the Royal Military College of Canada, an MA in sociology from Queen's University, and has studied sociology as a PhD candidate from Queen's University, specializing in digital media, information and surveillance.

Sam Andrey is the Director of Policy & Research at the Ryerson Leadership Lab. He also teaches about public leadership and advocacy at Ryerson University and George Brown College. He has led the design, execution and knowledge mobilization of multiple applied research projects, including surveys, focus groups, interviews, randomized controlled trials and cross-sectional observational studies. He previously served as Chief of Staff and Director of Policy to Ontario's Minister of Education, in the Ontario Public Service and in not-for-profit organizations advancing equity in education.

Karim Bardeesy is the Co-Founder and Executive Director of the Ryerson Leadership Lab. Karim is a public service leader who has worked in progressively senior roles in public policy, politics, journalism and academia in Toronto and the United States since 2001. Karim was previously Deputy Principal Secretary for the Premier of Ontario, the Honourable Kathleen Wynne, and served as Executive Director of Policy for Premiers Wynne and Dalton McGuinty. He has worked as a journalist, an editorial writer at *The Globe and Mail*, and as an editorial assistant at *Slate* magazine. Karim holds a Master in Public Policy from Harvard's John F. Kennedy School of Government.

Zaynab Choudhry is the Design Lead at the Ryerson Leadership Lab. She has been working as a designer, illustrator and marketer in the realm of public service by helping organizations rebrand, simplify communication and solve problems for over four years. Zaynab believes good design stimulates and motivates much of our everyday decisions; and through her design journey has developed skills in visual communication to accomplish just that. Zaynab is a recent graduate with a BTech in Graphic Communications Management, with double minors in marketing and sociology from Ryerson University.

Methodology

This report was informed by: a literature review; interviews with Canadian cybersecurity, privacy and technology experts; and two video town halls on April 14 and May 19, 2020 with 646 participants, featuring:

- Murad Hemmadi, Reporter for *The Logic*
- Dr. Richard Lachman, Associate Professor, RTA School of Media, Ryerson University
- Gregory Smolynec, Deputy Commissioner of Policy and Promotion, Office of the Privacy Commissioner of Canada
- Bianca Wylie, Co-Founder of Digital Public and Senior Fellow, Centre for International Governance Innovation

An anonymous survey was conducted by Pollara Strategic Insights online with 2,000 Canadian residents over the age of 18 from May 14 to 22, 2020. A random sample of Canadian residents who have opted-in to the AskingCanadians panel were invited to complete the voluntary survey. As a guideline, a probability sample of this size would yield results accurate to +/- 2 percentage points, 19 times out of 20 (95%). Totals may not sum or add to 100 due to rounding.

The data were weighted by region, gender and age, based on the most recent Canadian census figures to ensure that the sample matched Canada's population.

Table 1: Support for Organizations Making Contact Tracing Apps Mandatory

"A smartphone app has been proposed that would anonymously notify you if you have been physically close to someone who has been diagnosed with COVID-19. To what extent would you support the following organizations making it mandatory to download this smartphone app":

Summary of "Strongly support" and "Somewhat support"

		Region						Age					Gender		
	Total	BC	AB	MB/ SK	ON	QC	ATL	18-29	30-39	40-49	50-59	60+	Female	Male	Other/ Did not say
All Respondents	2,000	269	264	201	669	397	200	405	344	321	369	561	1,014	978	8
Weighted Respondents	2,000	272	227	130	766	468	138	380	351	334	371	564	1,025	968	8**
Employers to come to work	1,021	148	111	60	426	211	65	193	177	142	189	321	537	479	5
	51%	54%	49%	46%	56%	45%	47%	51%	50%	42%	51%	57%	52%	49%	62%
Governments to access public services, like public transit	1,110	151	121	70	455	245	68	202	191	152	205	359	571	532	6
	55%	56%	53%	54%	59%	52%	50%	53%	54%	46%	55%	64%	56%	55%	75%
Retail or grocery stories to enter	910	129	100	60	380	180	61	168	151	133	167	292	474	431	5
	46%	47%	44%	46%	50%	39%	45%	44%	43%	40%	45%	52%	46%	45%	62%
Landlords or condominiums to stay in your home	609	83	52	40	259	135	40	111	109	85	116	188	318	288	3
	30%	31%	23%	31%	34%	29%	29%	29%	31%	25%	31%	33%	31%	30%	37%
Average	46%	47%	42%	44%	50%	41%	43%	44%	45%	38%	46%	52%	46%	45%	59%

Table 1: Support for Organizations Making Contact Tracing Apps Mandatory cont.

		Education					Income						
	Total	High School or Less	College	Technical /Trade	Undergraduate	Graduate /Professional Degree	Under $20,000	$20,000 - Less than $30,000	$30,000 - Less than $50,000	$50,000 - Less than $80,000	$80,000 - Less than $100,000	$100,000 - Less than $150,000	$150,000 or More
All Respondents	2,000	329	357	215	606	470	82	118	264	363	279	409	279
Weighted Respondents	2,000	314	364	197	623	479	79*	116	263	357	282	410	287
Employers to come to work	1,021	168	180	109	309	249	34	48	136	190	152	223	157
	51%	53%	50%	56%	50%	52%	43%	42%	52%	53%	54%	54%	55%
Governments to access public services, like public transit	1,110	169	206	108	343	276	35	55	144	211	168	237	171
	55%	54%	57%	55%	55%	58%	45%	47%	55%	59%	60%	58%	60%
Retail or grocery stories to enter	910	151	171	96	276	209	34	46	122	180	130	193	134
	46%	48%	47%	49%	44%	44%	44%	39%	46%	50%	46%	47%	46%
Landlords or condominiums to stay in your home	609	93	113	69	178	151	18	28	88	111	86	136	95
	30%	29%	31%	35%	29%	31%	23%	25%	34%	31%	30%	33%	33%
Average	46%	46%	46%	49%	45%	46%	39%	38%	47%	48%	48%	48%	49%

Table 2: Smartphone Ownership

"How many of the following devices do you currently have in your household?"
Smartphone = 0

		Age					Income						
	Total	18-29	30-39	40-49	50-59	60+	Under $20,000	$20,000 - Less than $30,000	$30,000 - Less than $50,000	$50,000 - Less than $80,000	$80,000 - Less than $100,000	$100,000 - Less than $150,000	$150,000 or More
All Respondents	2,000	405	344	321	369	561	82	118	264	363	279	409	279
Weighted Respondents	2,000	380	351	334	371	564	79*	116	263	357	282	410	287
0	179	3	10	17	37	111	21	15	49	30	21	10	9
	9%	1%	3%	5%	10%	20%	26%	13%	19%	8%	7%	2%	3%

*small base
**very small base; ineligible for significance testing

References

[1]Armbruster, B., & Brandeau, M. L. (2007). Contact tracing to control infectious disease: when enough is enough. Health Care Management Science, 10(4), 341–355. doi: 10.1007/s10729-007-9027-6

[2]Broeckaert L. & Haworth-Brockman, M. (2014). HIV Contact Tracing in Canada. Retrieved from: https://www.catie.ca/en/pif/fall-2014/you-may-have-come-contact-hiv-contact-tracing-canada

[3]Health Canada. (2003, October). Learning from SARS: Renewal of Public Health in Canada. Retrieved from: https://www.canada.ca/content/dam/phac-aspc/migration/phac-aspc/publicat/sars-sras/pdf/sars-e.pdf

[4]Public Health agency of Canada. (2013). Public Health management of human illness associated with Middle East Respiratory Syndrome Coronavirus (MERS-CoV): Interim guidance for containment when imported cases are suspected/confirmed in Canada. Retrieved from: https://www.canada.ca/en/public-health/services/emerging-respiratory-pathogens/coronavirus/public-health-management-human-illness-associated-middle-east-respiratory-syndrome-coronavirus-mers-interim-guidance-containment-when-imported-cases.html

[5]Tian, Y., Osgood, N. D., Al-Azem, A., & Hoeppner, V. H. (2013). Evaluating the Effectiveness of Contact Tracing on Tuberculosis Outcomes in Saskatchewan Using Individual-Based Modeling. Health Education & Behavior, 40(1_suppl). doi: 10.1177/1090198113493910

[6]World Health Organization. (2020, May 10). Contact tracing in the context of COVID-19. Retrieved from https://www.who.int/publications-detail/contact-tracing-in-the-context-of-covid-19

[7]Kitchin, R. (2020, April 21) Using Digital Technologies to Tackle the Spread of the Coronavirus: Panacea or Folly?, The Programmable City, Maynooth University. http://progcity.maynoothuniversity.ie/wp-content/uploads/2020/04/Digital-tech-spread-of-coronavirus-Rob-Kitchin-PC-WP44.pdf

[8]Ibid

[9]Romm, T., Dwoskin, E., & Timberg, C. (2020, March 17). U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus. *The Washington Post*, Retrieved from https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/

[10]Kitchin (2020)

[11]Public Health Ontario (2019). Case and Contact Management for STIs: Internet-Based Contact Tracing. Retrieved from https://www.publichealthontario.ca/-/media/documents/E/2019/eb-internet-contact-tracing.pdf?la=en

[12]Pennise, M., Inscho, R., Herpin, K., Owens, J., Jr, Bedard, B. A., Weimer, A. C., Kennedy, B. S., & Younge, M. (2015). Using smartphone apps in STD interviews to find sexual partners. *Public health reports*, 130(3), 245–252. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4388222/

[13]WorkSafeBC. (2020, May). Restaurants, cafés, and pubs: Protocols for returning to operation. Retrieved from: https://www.worksafebc.com/en/about-us/covid-19-updates/covid-19-returning-safe-operation/restaurant-cafes-pubs

[14]Daflos, P. (2020, May 22). Credit Cards, loyalty programs quietly used in BC contact tracing. *CTV News*, Retrieved from: https://bc.ctvnews.ca/credit-cards-loyalty-programs-quietly-used-in-b-c-contact-tracing-1.4951402

[15]Kitchin (2020)

[16]In addition to these methods, the ACLU provides a list of others that can calculate phone proximity, including Wi-Fi: Stanley, J., & Granick, J. S. (2020, April 8). The Limits of Location Tracking in an Epidemic. Retrieved from https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic

[17]Chowdhury , H., Field, M., & Murphy, M. (2020, June 2). NHS track and trace app: how will it work and when can you download it? *The Telegraph*, Retrieved from https://www.telegraph.co.uk/technology/2020/06/02/nhs-app-track-trace-coronavirus-when-how-download-uk/

[18]Dave, P. (2020, April 3). Google data shines light on whether coronavirus lockdowns worldwide are working. *CBC News*, Retrieved from https://www.cbc.ca/news/technology/google-coronavirus-data-1.5520194

[19]Patriquin, M. (2020, April 9). Montreal computer scientists expect to launch contact-tracing app in less than a week. *The Logic*, Retrieved from https://thelogic.co/news/montreal-computer-scientists-expect-to-launch-contact-tracing-app-in-less-than-a-week/

[20]Harwell, D., & Timberg, C. (2020, March 19). Government efforts to track virus through phone location data complicated by privacy concerns. *The Washington Post*, Retrieved from https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

[21]Stupp, C. (2020, March 27). Europe Tracks Residents' Phones for Coronavirus Research. *The Wall Street Journal,* Retrieved from https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401

[22]Canadian Centre for Cyber Security. (2020, March 20). Alert: Cyber threats to Canadian health organizations. Retrieved from https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations

[23]*The Japan Times*. (2020, May 13). Social stigma and harassment undermine COVID-19 testing efforts across Asia. Retrieved from: https://www.japantimes.co.jp/news/2020/05/13/asia-pacific/stigma-harassment-coronavirus-testing-asia/#.XtX2YxNKiAw

[24]O'Neill, P. H., Ryan-Mosley, T., & Johnson, B. (2020, May 7). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*, Retrieved from https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker

[25]Kitchin (2020)

[26]Montjoye, Y.-A. D., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, 3(1). doi:10.1038/srep01376

[27]Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "Personally Identifiable Information". Communications of the ACM, 53(6), 24–26. doi:10.1145/1743546.1743558

[28]Angwin, J. (2020, April 14). Will Google's and Apple's COVID Tracking Plan Protect Privacy? *The Markup*. Retrieved from https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy

[29]Airship. (2019, May 2019). Airship's Data Study Reveals the State of Global Mobile Permissions One Year into GDPR. Retrieved from https://www.businesswire.com/news/home/20190522005486/en/Airship%E2%80%99s-Data-Study-Reveals-State-Global-Mobile

[30]Landau, S. (2020, March 25). Location Surveillance to Counter COVID-19: Efficacy Is What Matters. Lawfare. Retrieved from https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters

[31]Gebhart, G. (2020, April 30). COVID-19 and Technology: Commonly Used Terms. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2020/04/covid-19-and-technology-commonly-used-terms

[32]Newton, C. (2020, April 10). Why Bluetooth apps are bad at discovering new cases of COVID-19. *The Verge*, Retrieved from https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health

[33]Angwin (2020)

[34]Greenberg, A. (2020, April 17). Is Apple and Google's Covid-19 Contact Tracing a Privacy Risk? *Wired*, Retrieved from https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses

[35]Kitchin (2020)

[36]Angwin (2020)

[37]Hamilton, I. A. (2020, May 20). Cybersecurity experts found seven flaws in the UK's contact-tracing app. *Business Insider,* Retrieved from https://www.businessinsider.com/cybersecurity-experts-find-security-flaws-in-nhs-contact-tracing-app-2020-5

[38]Criddle, C. & Kelion, L. (2020, May 7). Coronavirus contact-tracing: World split between two types of app. *BBC*, Retrieved from https://www.bbc.com/news/technology-52355028

[39]Zastrow, M. (2020, May 19). Coronavirus contact-tracing apps: can they slow the spread of COVID-19? *Nature*, Retrieved from https://www.nature.com/articles/d41586-020-01514-2

[40]Gebhart (2020)

[41]Australian Government Department of Health. (2020, April 24). COVIDSafe Application Privacy Impact Assessment. Retrieved from https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf

[42]Helsenorge.no. (last updated 2020, April 28). Together we can fight coronavirus. Retrieved from https://helsenorge.no/coronavirus/smittestopp?redirect=false

[43]Asghar, H., Farokhi, F., Kaafar, D., & Rubinstein, B. (2020, April 6). On the privacy of TraceTogether, the Singaporean COVID-19 contact tracing mobile app, and recommendations for Australia. Retrieved from https://eng.unimelb.edu.au/ingenium/technology-and-society/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia

[44]Holmes, A. (2020, April 27). Governments have to decide whether to scrap their own COVID-19 contact tracing apps in favor of tech built by Apple and Google. Here's what's at stake. *Business Insider*, Retrieved from https://www.businessinsider.com/coronavirus-contact-tracing-government-apps-vs-apple-google-covid-19-2020-4

[45]Ball, K., Haggerty, K. D., & Lyon, D. (2014). *Routledge handbook of surveillance studies*. (pp.377-385). London: Routledge

[46]Davidson, A., & Erwin, M. (2020, April 29). Contact Tracing, Governments, and Data. Mozilla. Retrieved from https://blog.mozilla.org/blog/2020/04/29/contact-tracing-governments-and-data

[47]Lomas, N. (2020, May 15). How will Europe's coronavirus contact-tracing apps work across borders? *Tech Crunch*, Retrieved from https://techcrunch.com/2020/05/15/how-will-europes-coronavirus-contacts-tracing-apps-work-across-borders

[48]DP-3T Project (2020, May 25). Decentralized Privacy-Preserving Proximity Tracing. Github. Retrieved from: https://github.com/DP-3T documents/blob/master/DP3T%20White%20Paper.pdf

[49]Mobile Operating System Market Share Canada. (2020, April). StatCounter. Retrieved May 28, 2020, from https://gs.statcounter.com/os-market-share/mobile/canada

[50]Greenberg (2020)

[51]Ibid

[52]Angwin (2020)

[53]*BBC News.* (2020, May 19). Coronavirus: Security flaws found in NHS contact-tracing app. Retrieved from https://www.bbc.com/news/technology-52725810

[54]Nellis, S., & Dave, P. (2020, May 4). Apple, Google ban use of location tracking in contact tracing apps. Retrieved from https://www.reuters.com/article/us-health-coronavirus-usa-apps/apple-google-ban-use-of-location-tracking-in-contact-tracing-apps-idUSKBN22G28W

[55]Greenberg (2020)

[56]Davidson & Erwin (2020)

[57]Lomas, N. (2020, April 27). Germany ditches centralized approach to app for COVID-19 contacts tracing. *Tech Crunch*, Retrieved from https://techcrunch.com/2020/04/27/germany-ditches-centralized-approach-to-app-for-covid-19-contacts

[58]NS Tech. (2020, April 24). PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear. Retrieved from https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear/

[59]Davidson, S. (2020, April 24). Ontario takes 'extraordinary step' to give police list of all COVID-19 patients. *CTV News*, Retrieved from https://toronto.ctvnews.ca/ontario-takes-extraordinary-step-to-give-police-list-of-all-covid-19-patients-1.4910950

[60]Law, E. (2020, April 24). Coronavirus: China's contact tracing app touted as helping to contain outbreak. *The Straits Times,* Retrieved from https://www.straitstimes.com/asia/east-asia/coronavirus-chinas-contact-tracing-app-touted-as-helping-to-contain-outbreak

[61]Phartiyal, S. (2020, May 14). India follows China's lead to widen use of coronavirus tracing app. *The Guardian*. Retrieved from https://www.theguardian.pe.ca/business/reuters/india-follows-chinas-lead-to-widen-use-of-coronavirus-tracing-app-449536/

[62]Leswing, K. (2020, May 6). Companies could require employees to install coronavirus-tracing apps like this one from PwC before coming back to work. *CNBC*, Retrieved from https://www.cnbc.com/2020/05/06/pwc-is-building-coronavirus-contact-tracing-software-for-companies.html

[63]Yu, E. (2020, May 10). Singapore turns to businesses to bolster contact tracing efforts. *ZDNet,* Retrieved from https://www.zdnet.com/article/singapore-turns-to-businesses-to-bolster-contact-tracing-efforts

[64]Lomas, N. (2020, May 4). UK's coronavirus tracing app strategy faces fresh questions over transparency and interoperability. *Tech Crunch,* Retrieved from https://techcrunch.com/2020/05/04/uks-coronavirus-tracing-app-strategy-faces-fresh-questions-over-transparency-and-interoperability/

[65]PwC United States. (2020, May 11). PwC's COVID-19 CFO Pulse Survey Results. Retrieved from https://www.pwc.com/us/en/library/covid-19/pwc-covid-19-cfo-pulse-survey.html

[66]Medow, J., & Sheldrick, O. (2020, April 9). COVID-19 Places the Right to Internet Access in Stark Relief. *First Policy Response*, Retrieved from http://policyresponse.ca/only-connect

[67]Government of Canada, Canadian Radio-television and Telecommunications Commission. (2019). Communications Monitoring Report 2019. Retrieved from https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/cmr1.htm#a2.1.1

[68]Ibid

[69]Rushowy, K. (2020, May 25). Have libraries provide wifi, devices to workers, small businesses, Liberal MPPs urge. *Toronto Star*, Retrieved from https://www.thestar.com/politics/provincial/2020/05/25/have-libraries-provide-wifi-devices-to-workers-small-businesses-liberal-mpps-urge.html

[70]Commonwealth Parliament, & Parliament House. (2020). Privacy Amendment (Public Health Contact Information) Bill 2020. Retrieved May 29, 2020, from https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6556

[71]Edwards, L., Veale, M., Lynskey, O., Coldicutt, R., Loideain, N. N., Kaltheuner, F., ... Bietti, E. (2020, April 13). The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates. Retrieved May 29, 2020 from https://osf.io/preprints/lawarxiv/yc6xu/

[72]Bay, J. (2020, April 10). Automated contact tracing is not a coronavirus panacea. Retrieved from https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98

[73]Hamilton, I. A. (2020, May 12). Iceland had the most-downloaded contact-tracing app for its population size. Authorities there say it hasn't made much difference. *Business Insider,* Retrieved from https://www.businessinsider.com/iceland-contact-tracing-not-gamechanger-2020-5

[74]McDonald, S., & Wylie, B. (2020, May 21). Hard questions for policy-makers about digital contact tracing. *First Policy Response*, Retrieved from http://policyresponse.ca/hard-questions-for-policy-makers-about-digital-contact-tracing

[75]Kitchin (2020)

[76]Lyon, D. (2020, May 24). The coronavirus pandemic highlights the need for a surveillance debate beyond 'privacy'. *The Conversation,* Retrieved from https://theconversation.com/the-coronavirus-pandemic-highlights-the-need-for-a-surveillance-debate-beyond-privacy-137060

[77]Scassa, T. (2020, March 24). Private sector data, privacy, and the pandemic. Retrieved from https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=322:private-sector-data-privacy-and-the-pandemic&Itemid=80

[78]Parsons, C. (2020 April, 30) Contact tracing apps must not compound historical discrimination. *Policy Options,* Retrieved from https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/

[79]Wright, M. (2020, April 26). Contact tracing app could halt spread of Covid-19 if downloaded by 60 per cent of the population. *The Telegraph,* Retrieved from https://www.telegraph.co.uk/news/2020/04/26/contact-tracing-app-could-halt-spread-covid-19-downloaded-60/

[80]Jackson, B. (2020, June 2). Contact tracing mobile apps hold potential to stop COVID-19 – but governments have missed the mark so far. *IT World Canada,* Retrieved from https://www.itworldcanada.com/article/contact-tracing-mobile-apps-hold-potential-to-stop-covid-19-but-governments-have-missed-the-mark-so-far/431625

[81]CIFAR. (2020, April 30). Society, Technology and Ethics in a Pandemic (STEP): Expert Advisory Group Report. Retrieved from https://www.cifar.ca/docs/default-source/all-reports/ai-step-report-eng-10-f.pdf

[82]Office of the Privacy Commissioner of Canada. (2020, May 7). Joint Statement by Federal, Provincial and Territorial Privacy Commissioners. Retrieved from: https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

[83]National Cybersecurity Consortium. (2020, May 22). Statement on Privacy-respecting and Trust-worthy COVID-19 Tracing Apps. Retrieved from https://www.ryerson.ca/cybersecure-catalyst/news/Covid-19-news-update/

[84]European Data Protection Board. (2020, April). Guidelines 04/2020 on the use of location data and contact tracing tools in the contexts of the COVID-19 outbreak. Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

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

[86]European Data Protection Board 2020

[87]Greenberg (2020)

[88]Editorial. (2020, April 29). Show evidence that apps for COVID-19 contact-tracing are secure and effective. *Nature,* Retrieved from https://www.nature.com/articles/d41586-020-01264-1

[89]Lomas, N. (2020, April 6). EU privacy experts push a decentralized approach to COVID-19 contacts tracing. *Tech Crunch,* Retrieved from https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/

[90]Kelion, L. (2020, May 20). Apple and Google release marks 'watershed moment' for contact-tracing apps. *BBC,* Retrieved from https://www.bbc.com/news/technology-52740131

[91]O'Brien, M. (2020, May 20). Apple, Google release their joint technology for pandemic-tracking apps. *CBC News,* Retrieved May 29, 2020, from https://www.cbc.ca/news/technology/apple-google-covid-app-1.5577166

[92]Scherer, S. (2020, May 22). Canada to ramp up COVID-19 testing and tracing, recommend digital app. *Reuters,* Retrieved from https://www.reuters.com/article/us-health-coronavirus-canada/canada-to-ramp-up-covid-19-testing-and-tracing-recommend-digital-app-idUSKBN22Y2H5

[93]O'Neill (2020)


cybersecure
policy
exchange
Powered by
RBC