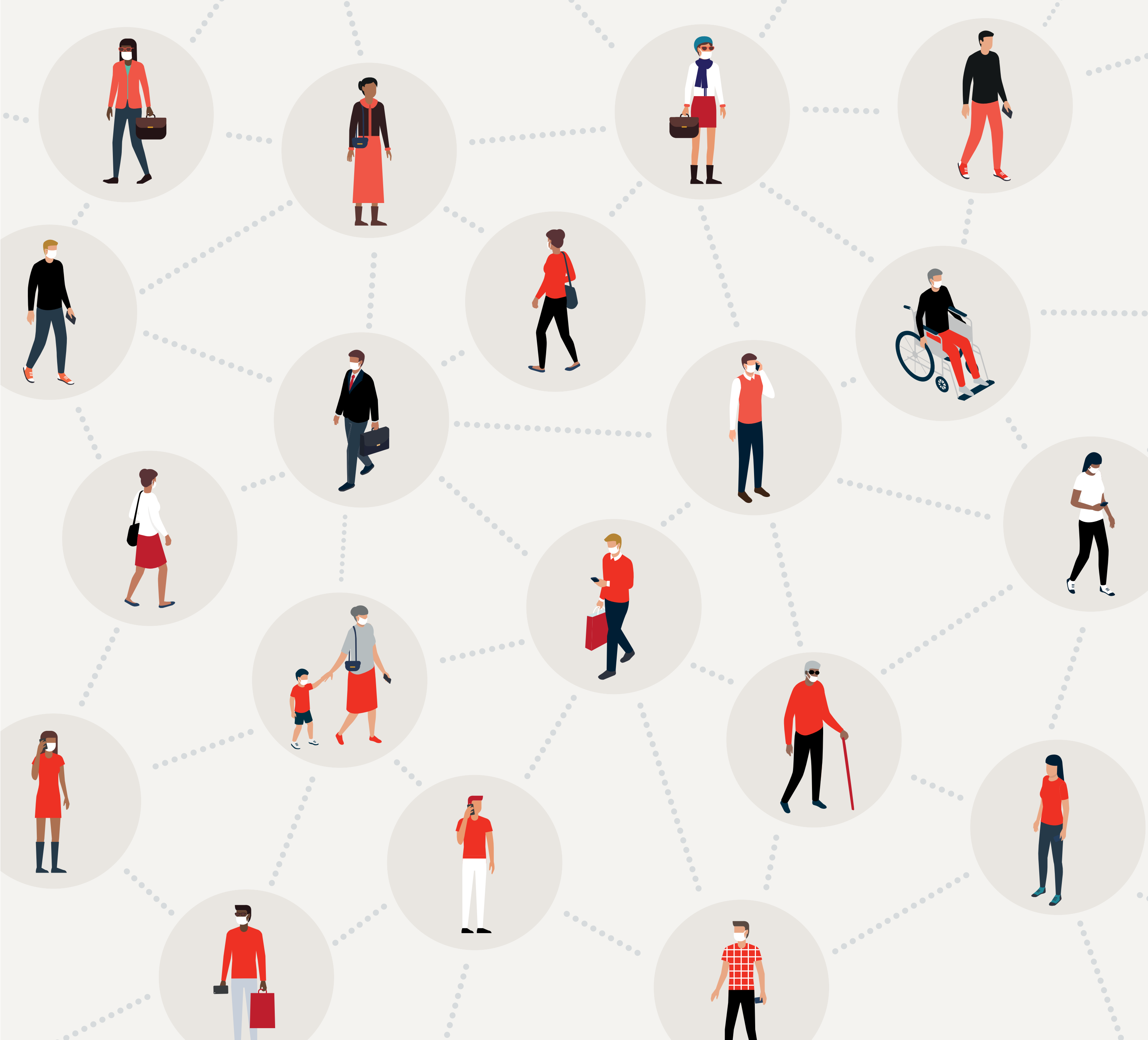


CIFAR

SOCIETY, TECHNOLOGY AND ETHICS IN A PANDEMIC

EXPERT ADVISORY GROUP REPORT

APRIL 30, 2020

TABLE OF CONTENTS

3 Executive Summary

5 Canadian Context

7 Overview of Contact/Proximity-Tracing Apps

10 Principles

12 Implementation Guidelines

14 Conclusion

15 Appendices

15 A. Society, Technology and Ethics in a Pandemic (STEP) Expert Advisory Group

17 B. International Roundtable Participants

17 C. CIFAR Contributors

18 D. Scan of Contact/Proximity-Tracing Apps in Use

22 E. Further Reading

ABOUT CIFAR

CIFAR is a Canadian-based global charitable organization that convenes extraordinary minds to address the most important questions facing science and humanity.

By supporting long-term interdisciplinary collaboration, CIFAR provides researchers with an unparalleled environment of trust, transparency and knowledge sharing. Our time-tested model inspires new directions of inquiry, accelerates discovery and yields breakthroughs across borders and academic disciplines. Through knowledge mobilization, we are catalysts for change in industry, government and society.

CIFAR's community of fellows includes 20 Nobel laureates and more than 400 researchers from 22 countries. In 2017, the Government of Canada appointed CIFAR to develop and lead the Pan-Canadian Artificial Intelligence Strategy, the world's first national AI strategy.

EXECUTIVE SUMMARY

COVID-19 has created unprecedented challenges for Canada and the world. Major scientific efforts are focused on understanding the virus, developing vaccines, and finding treatment options. At the same time, many in the scientific community have turned their energies toward developing novel digital and biological technologies in response to the pandemic.

At the request of Canada's Chief Science Advisor, Dr. Mona Nemer, CIFAR established an Expert Advisory Group (EAG) on Society, Technology and Ethics in a Pandemic (STEP) to advise on the technical, social, legal, and ethical considerations for deploying novel technologies in response to COVID-19. This independent group includes leading Canadian experts in law, regulatory innovation, artificial intelligence, epidemiology, clinical care, philosophy, ethics, and public policy. Their advice has informed this report. It is intended to be a clear reference document to inform government actions and decision making.

NOVEL TECHNOLOGIES IN A PANDEMIC

In recent weeks, several novel technologies have been discussed and developed to address different aspects of the COVID-19 response. These technologies include applications that trace a user's location to provide information about the user's potential exposure to the virus (contact-tracing apps); apps that alert the user after potentially encountering someone diagnosed with COVID-19 (proximity-tracing apps); apps for reporting symptoms and modelling health scores; or a combination of the three. Even more recently, a focus on improving serological tests that detect COVID-19 antibodies has resulted in speculation that some governments will reopen the economy by issuing "immunity certificates" to workers considered to be safe from exposure. The STEP EAG discussed these options and consulted with international experts to inform a framework of guiding principles and specific implementation advice, focusing on the deployment of contact- and proximity-tracing apps.

RECOMMENDED PRINCIPLES

When considering novel technologies during a pandemic, governments should take a principled approach that includes a commitment to:

- Transparency and Accountability
- Privacy
- Equity and Diversity
- Cooperation and Mobility
- Necessity and Proportionality
- Quality, Security, and Efficacy

Public trust must be a focal consideration for the deployment of even time-limited technologies. Leadership is imperative and technology is not a surrogate for policy.

ADVICE ON CONTACT/ PROXIMITY-TRACING APPS

- Consideration of contact/proximity-tracing apps should occur only in support of broader, evidence-based public health measures, such as increased testing and manual contact tracing.
- Governments should work together, as Canadians expect harmonized standards and interoperable systems to ensure equity, security, and mobility.
- A legal framework and independent oversight mechanisms that can report in real time on the effectiveness and impacts of technology are required. These should provide clarity on the types of data that can be collected and for what purposes; who will have access to the data and penalties for unauthorized use; security provisions; and a requirement to delete data at a specified time, or after specified criteria are met.

- Privacy principles set out in the Privacy Commissioner of Canada's framework should be followed and governments, in collaboration with oversight bodies, should interrogate developers' claims of privacy preservation.
- The offices of privacy commissioners should be empowered to provide oversight and auditing for the deployment of these technologies.
- Apps should only be deployed when the underlying technology has been tested for efficacy. Governments should be transparent about their limitations, with open-source code available for public scrutiny.
- Governments should consider creating a pan-Canadian independent advisory group to examine the ethical, legal, and social issues arising from the deployment of digital technologies and develop and recommend policies to the government.
- Governments are cautioned against making the use of apps mandatory by all residents and citizens because of the technical, social, legal, and ethical issues identified to date.

Tackling the COVID-19 pandemic will require a complex strategy with many concurrent tactics. In addition to ramping up public health capacity for rapid COVID-19 diagnostic testing, new technological approaches may provide some of the necessary data for monitoring and controlling the pandemic, and potentially help to create the conditions for an exit from lockdown and physical-distancing policies. However, there are significant technical, social, legal, and ethical considerations that need to be well understood by governments before moving forward. Most importantly, governments must work to build public trust in any proposed technological response, engaging the public with informed dialogue and transparent communication.

CANADIAN CONTEXT

As of April 30th, 2020, there have been[1] over 50,000 confirmed and probable cases of COVID-19 reported in Canada, and more than 3,000 people have died from the virus. The speed and severity of this pandemic have prompted an unprecedented public health response across the country, with massive disruptions to human health, the health system, social well-being, and the economy. All 13 provinces and territories have declared states of emergency, which allows governments to impose certain restrictions on personal and collective rights, such as banning large gatherings, enforcing the closure of schools and nonessential businesses, issuing stay-at-home orders, and even restricting entry or implementing screening at some provincial/territorial boundaries. The federal government has restricted travel into Canada since mid-March, and has invoked the Quarantine Act to enforce 14-day isolation for anyone entering the country.

More than 750,000 Canadians have been tested for COVID-19[2] (specifically, with PCR-based tests that detect for the presence of genetic material of the SARS-CoV-2 virus, a proxy for active infection). At this level of testing, Canada has achieved a relatively high rate[3] of testing per capita (around 20 tests per 1,000 people), though at a lower rate of testing per confirmed case (around 15 tests per confirmed case) than some other countries that have the pandemic under better control at this stage, such as South Korea, Taiwan, and New Zealand[4]. In addition, the level of testing is not uniform across the country. Achieving a higher rate of testing is important for obtaining a more accurate picture of the spread of the disease in the population, and will require broader testing beyond individuals with severe symptoms.

Effectively fighting this pandemic requires widespread diagnostic testing to quickly and effectively identify and isolate individuals infected with the virus, while protecting those who are not infected. Diagnostic testing and manual contact tracing are two important components of the public health strategy to contain and end this pandemic. The more we know about how COVID-19 affects all groups of people living in Canada, the more we will be able to plan our way out of the pandemic, for the benefit of all.

As the number of infections begins to plateau in different regions of the country, governments across Canada are making plans for the gradual lifting of restrictions. Together, the first ministers have agreed on a shared public health approach[5] to restart the economy.

From diagnostic testing and mathematical modelling to drug and vaccine development, science and technology are central to ending this pandemic. However, there are questions about the effectiveness, quality, and safety of some of these technologies. There are also concerns about whether the rights and freedoms of citizens may be affected. How do democracies, such as Canada, ensure that new technologies optimize individual well-being, including health and economic well-being and personal rights and liberties, while still achieving their goal of limiting viral transmission through the community?

1 https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection.html
2 https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection.html
3 https://ourworldindata.org/covid-testing
4 With 57, 145 and 114 tests per confirmed case, respectively. https://ourworldindata.org/covid-testing
5 https://pm.gc.ca/en/news/statements/2020/04/28/first-ministers-statement-shared-public-health-approach-support

STEP EXPERT ADVISORY GROUP

At the request of Canada's Chief Science Advisor, Dr. Mona Nemer, CIFAR established an Expert Advisory Group (EAG) on Society, Technology, and Ethics in a Pandemic (STEP) to advise on the technical, social, legal, and ethical considerations of deploying novel technologies in response to COVID-19. This independent group is made up of leading Canadian experts in law, regulatory innovation, artificial intelligence, epidemiology, clinical care, philosophy, ethics, and public policy (see Appendix A).

To inform the work of the STEP EAG, CIFAR convened an international, interdisciplinary roundtable with experts from Denmark, Israel, Singapore, South Korea, Switzerland, the United Kingdom, and the United States. Discussion topics included governance, regulation, and levels of citizen adoption of novel technologies, as well as privacy, public trust, equity, and accessibility. The perspectives provided by both the Canadian and international experts have informed this report. The international experts are listed in Appendix B, while Appendix D includes a jurisdictional scan of technologies that have been deployed internationally.

In its discussions, the STEP EAG considered several novel technologies, including "immunity certificates"[6], apps for reporting/modelling health scores, and contact/proximity-tracing apps. We believe the guiding principles below serve as a useful framework in considering many, if not all, of these novel technologies. However, our implementation guidance to governments primarily focuses on contact/proximity-tracing apps. This is based on two considerations: first, the technology and features of contact/proximity-tracing apps are being widely discussed as potential tools in reopening the economy; and, secondly, we are aware that such apps are currently in development in Canada.

This report is the product of the discussions of the STEP EAG over a two-week period of intense work. It is intended to be concrete and solutions-oriented so that different orders of government will be able to refer to it and act accordingly as they consider new technologies to respond to this and future pandemics.

[6] Immunity certificates are physical or digital documents that would be issued to individuals who have tested positive for antibodies to COVID-19, indicating past infection. The assumption is that these individuals are now immune to reinfection and can be allowed freedom of movement and to return to work. Jurisdictions around the world are currently exploring the viability of immunity certificates as a pathway out of the economic shutdown. For more information, see https://www.nature.com/articles/d41586-020-01115-z.

OVERVIEW OF CONTACT/ PROXIMITY-TRACING APPS

An essential public health measure in controlling the COVID-19 pandemic is tracing and identifying everyone who has come into contact with an infected individual so that they can self-isolate, monitor their symptoms, and receive testing if required. This labour-intensive process requires large teams of public health workers, and is dependent to some extent on individuals accurately recalling their actions, movements, and contacts. As such, a number of consortia and initiatives by researchers, technology companies, and governments are developing mobile phone-based technologies that may facilitate and accelerate this process.

Several approaches to contact/proximity-tracing apps with varying levels of intrusiveness have emerged—from using phones' cellular signal and/or GPS data to track a person's location, to using Bluetooth to detect and log other phones that come within a phone's proximity. Depending on the implementation, the apps are intended to fulfill one of several purposes, from notifying individuals (and public health authorities) if they have been in close proximity to infected persons so that they can self-isolate and take other health measures, to informing public health messaging and identifying "hot spot" locations or neighbourhoods where governments can devote additional resources or that people might avoid.

Through certain implementations, the data collected by these apps would be uploaded (with privacy preservation[7], e.g., through anonymization, aggregation, or differential privacy) to centralized databases that can be accessed and validated by public health authorities. Alternatively, the data may be uploaded to a non-governmental protected data environment, such as a "data trust,"[8] that is independently managed according to a charter, with a board of trustees who would make decisions on data access, security, and management.

A number of technical issues need to be resolved if the apps are to be effective. These include the concern that GPS location data is not always accurate or of a high enough resolution (e.g., for individuals on different floors of an apartment building) for the apps' stated purpose of tracking individuals' locations, as well as the inconsistencies[9] in Bluetooth's reliability to assess the true proximity of two individuals due to factors in the physical environment or the position/orientation of phones. Due to concerns about the scientific basis for these apps, a recent editorial in *Nature* recommends that "apps should not be rolled out without pilot studies or risk assessments being published."[10]

The effectiveness of the apps in capturing a realistic picture of COVID-19 cases and contacts also depends on whether people download and use the app as directed. Certain modelling studies[11] estimate that 60%–80% of a population may need to use such an app in order to effectively reduce transmission in a certain area. To date, this has been a challenge for apps deployed in other jurisdictions. For example, in Singapore, the uptake of the TraceTogether app is less than 20%[12] of the population.

7 https://blog.openmined.org/covid-app-privacy-advice/
8 https://policyoptions.irpp.org/magazines/april-2020/covid-19-tracking-data-should-be-managed-the-way-data-trusts-are/
9 https://www.technologyreview.com/2020/04/22/1000353/bluetooth-contact-tracing-needs-bigger-better-data/
10 https://www.nature.com/articles/d41586-020-01264-1
11 https://045.medsci.ox.ac.uk/for-media
12 https://theconversation.com/the-coronavirus-contact-tracing-app-wont-log-your-location-but-it-will-reveal-who-you-hang-out-with-136387

There are other important ethical, legal, and social considerations.[13] There has been significant discussion among legal scholars, computer scientists, and policy-makers about the potential privacy concerns associated with centralized databases. Some experts argue[14] that, because there is a risk for the anonymized data to be re-identified, governments could use such databases for quarantine enforcement, surveillance, or other purposes. As a result, some jurisdictions, such as Germany, have changed course recently toward more "decentralized" approaches. The companies behind the two largest mobile phone operating systems, Apple and Google, are also working to enable decentralized proximity-tracing apps on their platforms.

The lack of access to smartphones or other communications tools among children, as well as the populations most vulnerable in this pandemic (including seniors, people who are homeless, people of lower socioeconomic status, and those in rural or Northern regions, among others), presents significant equity issues. Having a tool that works for some portion of the population might be better than having no tool (by helping to reduce the workload of contact tracers so they can focus on those communities or population groups with less access to technology or provide additional support), but only to a certain extent. The potential stigma associated with areas identified as hot spots raises additional equity concerns, as well as potential legal consequences, such as whether or how individuals flagged by the apps may be targeted for mandatory self-isolation.

The following table provides an overview of some of the features of contact/proximity-tracing apps deployed or in development, in Canada and internationally, for which information is publicly available.

COMPARISON OF CONTACT/PROXIMITY-TRACING APPS DEPLOYED OR IN DEVELOPMENT

METHOD 1

LOCATION-BASED

FEATURES

- Uses GPS or cellular signal to trace the travel trajectory of individuals

BENEFITS

- Potential for comprehensive tracking of all cases
- Geographic information could be useful in identifying "hot spots"

Technical Considerations

- Accuracy/resolution of signal
- If based on apps (rather than using phone network/operating system), effectiveness depends on uptake

Privacy Considerations

- Privacy and surveillance concerns with the type or amount of data being disclosed[15]

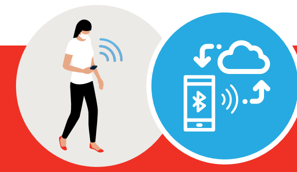
Examples

- South Korea (combined with other information, e.g., credit card data)
- MIT SafePaths[16] (data is not uploaded unless user consents); SafePaths and apps based on it (such as MyTrace[17]) plan to incorporate both GPS and Bluetooth capabilities

13 https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/
14 https://slate.com/technology/2020/04/europe-contact-tracing-privacy-apple-google-coronavirus.html
15 https://www.nature.com/articles/d41586-020-00740-y
16 https://www.media.mit.edu/projects/safepaths/overview/
17 https://www.mytrace.ca/

METHOD 2

BLUETOOTH-BASED PROXIMITY TRACKING WITH CENTRALIZED DATABASE



FEATURES

- Uses Bluetooth to detect other devices in proximity and record an anonymous ID for each "contact"
- If diagnosed, person uploads their contact log (of anonymous IDs) to a database accessible by the health authority, which processes the data and notifies possible contacts

BENEFITS

- Offers greater privacy protection by limiting amount of data leaving users' devices
- Processing of contact information in centralized database permits validation by public health authorities

Technical Considerations

- Effectiveness depends on uptake
- Inconsistencies in reliability of Bluetooth system

Privacy Considerations

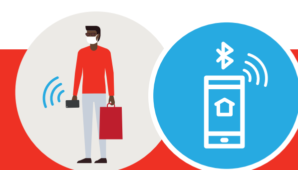
- Privacy/ surveillance concerns about government access to centralized database, where anonymized data could potentially be re-identified

Examples

- Singapore (TraceTogether app); its BlueTrace[18] protocol is now adopted by Australia, with interest from New Zealand
- Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[19] protocol, developed by an academic-industrial consortium, is being adopted by Italy and France

METHOD 3

BLUETOOTH- BASED PROXIMITY TRACKING WITH DECENTRALIZED PROTOCOL



FEATURES

- Uses Bluetooth to detect other devices in proximity and record an anonymous ID for each "contact"
- Once an individual is diagnosed, they can upload their contact log (of anonymous IDs) to a database from which all users' devices will periodically download, then data will be processed on individual phones to determine if they match

BENEFITS

- Offers greater protection of privacy by limiting amount of data leaving users' devices
- Contact logs not accessible to authorities

Technical Considerations

- Effectiveness depends on uptake
- Inconsistencies in reliability of Bluetooth system
- Device-based contact matching places higher demand on computing power on user's phone

Privacy Considerations

- Most severe privacy concerns mitigated, but remaining questions about time limitation, voluntary nature

Examples

- Decentralized Privacy-Preserving Proximity Tracing (DP-3T)[20] protocol, developed by a coalition of European academic institutions, is being adopted by several European countries including Germany, Switzerland, and Ireland
- Google and Apple[21] are releasing APIs and modifying their operating systems based on decentralized protocol to allow development of "exposure notification" apps on their platforms
- Later iterations of MIT SafePaths plan to incorporate decentralized proximity tracing

[18] https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf
[19] https://www.pepp-pt.org/
[20] https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Simplified%20Three%20Page%20Brief.pdf
[21] https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.0.pdf

PRINCIPLES

Understanding the technical, social, legal, and ethical considerations identified above, and acknowledging that public trust is a prerequisite for the acceptability and implementation of new technologies, we recommend the following principles as a framework for governments as they consider the integration of novel technologies within their broader public health strategies for managing the pandemic.

TRANSPARENCY AND ACCOUNTABILITY

Pandemic policies and implementation mechanisms should provide for ongoing public communication.

Governments will need to engage in ongoing communication with citizens in an open and transparent way about the objectives and limitations of any technological applications, in order to build and maintain public trust. Governments must clearly explain the role of a particular technology and its contribution to public health objectives (e.g., self-isolation or the identification of COVID-19 hot spots). Public trust will be reinforced by a pandemic legal framework and independent oversight mechanisms that can report publicly and in real time around the effectiveness and impacts of technology.

PRIVACY

Privacy protections must be based on clear legal and regulatory frameworks.

Clarity is needed as to what kind of data will be collected, with whom the data will be shared, what will be done with such data, for how long the data will be kept, and how the data will be safeguarded. Various technological and governance approaches, such as restricted data environments and data trusts, are being proposed to minimize, protect, aggregate, or anonymize data and to design apps so that private data is stored locally and does not leave an individual's phone. Technologies should incorporate privacy-preservation measures by design, with accessible and comprehensive user agreements (e.g. clear terms of consent). Regulators must ensure that these mechanisms for privacy protection are fit for purpose, legislated, standardized, and clearly communicated.

EQUITY AND DIVERSITY

Lack of access to technologies and unrepresentative data should not create new or exacerbate existing inequalities or stigmatize vulnerable groups.

Access to technologies such as smartphones is not equally distributed. While having technological tools that work for some portion of the population might be better than having no tools, overreliance on tools that involve differential access runs the risk of further exacerbating existing inequities. Scientific and socioeconomic data about how the virus affects all people is essential to protecting everyone's health.

COOPERATION AND MOBILITY

Harmonizing approaches, while allowing for local differences and customization, will support mobility and equity.

Canadians expect that their governments will work together during this unprecedented health and economic crisis. Accordingly, public health agencies should strive to agree on a single set of performance standards for technological applications, with the objective of sharing data that is easily comparable in order to collaborate on curbing the spread of the disease, enabling interprovincial mobility, and speeding up the reopening of the economy. Provinces/territories and other jurisdictions need to share data and resources with one another in order to monitor disease spread across jurisdictions and to build common strategies to prevent it. There should be opportunities for local customization and joint learning across jurisdictions.

NECESSITY AND PROPORTIONALITY

A clearly defined technology that offers some improvement, even if imperfect, may be worth deploying, for a limited time.

Deployment of technological interventions should be proportionate to the needs and severity of the crisis. While these technologies have the potential to assist public health management during emergencies, their invasiveness and scale of deployment should be proportional to the impact of the pandemic on public health and well-being. As a result, legislated sunset clauses and clear limitations on the purposes for which the data can be used are required.

QUALITY, SECURITY, AND EFFICACY

The design of novel technologies and regulations should be evidence-based.

Development of new technologies must ensure they are fair, safe, and effective, including the new skills required to manage and regulate these technologies. The potential security vulnerabilities of the proposed new technologies need to be well understood. All technologies should be tested prior to deployment, and because these are new technological applications in an unprecedented situation, testing and recalibration need to be ongoing once deployed.

IMPLEMENTATION GUIDELINES

Building on the principles identified above, we offer the following implementation guidelines to governments with respect to the deployment of contact/proximity-tracing apps in the current COVID-19 pandemic.

GENERAL

Digital contact/proximity-tracing apps will only be effective if there is a timely and robust system of diagnostic testing for COVID-19, and should be viewed as a complement to well-resourced manual contact tracing. Consistent with approaches in many OECD countries, installation of apps should be voluntary, with no penalties for failure to install an app or carry a device. If an app is deemed to provide useful data to a holistic public health strategy to manage the crisis, we recommend the actions below.

ESTABLISHING A LEGAL FRAMEWORK

Public health is an area of shared jurisdiction. It will be up to each province and territory to decide on the deployment of contact/proximity-tracing apps as part of their overall strategy to manage the pandemic. However, viruses can spread across provincial boundaries. In order for the technology to work across the country, shared standards and interoperability between systems need to be ensured by different jurisdictions. Canadians across the country expect to enjoy the same degree of health and economic benefit provided by this technology, as well as the same protections and safeguards, and also expect that all governments will pursue a collaborative and coordinated approach to the deployment of technology.

Federal and provincial governments, in consultation with their privacy commissioners, should consider the need for framing legislation to provide a clear legal framework for the deployment of contact/proximity-tracing apps and other technologies and the degree to which there should be a common approach across jurisdictions. The legal framework should be consistent with the Privacy Commissioner of Canada's Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19[22].

Framing legislation should address the following issues:

- The types of data that can be collected;
- The purposes for which data is collected;
- Who has access to the data;
- Requirement to delete data after a specified period, or after specified criteria are met (e.g., a finding by public health agencies that the pandemic is over);
- Provision for sunsetting the legislation after a specified time period;
- Prohibitions and penalties addressing the use of the data for unauthorized purposes.

TRANSPARENCY, OPENNESS, AND SECURITY

Technological tools deployed in a public health crisis need to be introduced transparently and openly, giving the public a clear view of the technology's efficacy and safety so as to build public trust. In particular, the government should:

- Develop a comprehensive and transparent communication plan;
- Gather and respond to public feedback (e.g., surveys, parliamentary representatives);
- Articulate the benefits and technical, ethical, and social issues of the technologies (e.g., how the level of uptake has a direct effect on the apps' effectiveness);
- Mandate that the source code for deployed apps be open-source, allowing scrutiny from independent experts and the broader public;

[22] https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid

- Be transparent about the data that will be collected, where it will be stored, the uses and purposes of the data, who will have access to the data, and any data-sharing agreements between governments, tech developers, researchers, employers, and other parties;
- Assess potential security vulnerabilities (e.g., whether/how the technologies may be subject to malicious attacks, misuse, or fraud) and communicate these to Canadians;
- Ensure app developers are committed to maintaining the tools and rapidly addressing security concerns, or to helping governments develop the capacity to take on these tasks.

PRIVACY

The deployment of technology should respect the privacy principles set out in the Privacy Commissioner of Canada's Framework to Assess Privacy-Impactful Initiatives in Response to COVID-19.[23]

These include:

- **Legal authority:** the proposed measures must have a clear legal basis;
- **Necessity and proportionality:** the measures should be science-based and necessary to achieve a specified identified purpose;
- **Purpose limitation:** personal information must be used to protect public health and for no other purpose, and should not be made available for purposes of law enforcement or national security;
- **Data protection and release:** use de-identified or aggregate data where possible; the risks and benefits of any public data release should be weighed, with particular attention to impact on vulnerable groups;
- **Time limitation:** exceptional measures should be time-limited, and data collected during this period should be destroyed when the crisis ends, except for narrow purposes such as research or ensuring accountability;
- **Transparency and accountability:** government should be clear about the basis and the terms applicable to exceptional measures and be accountable for them, and should provide clear and detailed information to Canadians on an ongoing basis.

Governments, in collaboration with the oversight bodies described below, should effectively interrogate developers' claims of privacy preservation. This includes conducting algorithmic and privacy impact assessments.

ACCOUNTABILITY AND OVERSIGHT

In considering the development of new oversight and accountability mechanisms, governments should consider the following issues:

- The capacity of legislative committees and privacy commissioners' offices in providing ongoing oversight of the deployment of technology;
- The role of intergovernmental committees of public health experts in sharing information about the effectiveness of technology in supporting public health strategies.

The offices of privacy commissioners should be explicitly empowered, e.g., through the framing legislation, with a mandate to provide oversight and auditing for the deployment of these technologies.

Governments should consider creating a pan-Canadian independent advisory group that includes a diverse group of citizens, as well as experts in public health, digital technology, law, and ethics. As an advisory body, the group should examine the ethical, legal, and social issues arising from the deployment of digital technologies, and should develop and recommend policies to the government. The deliberations and findings of this group should be publicly available.

In preparing for and deploying contact/proximity-tracing apps, governments should support health and social science research into the effectiveness and broader societal impact of these technologies. The Chief Science Advisor should continue to consult with expert advisory groups on these areas of research.

[23] https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/

CONCLUSION

While we recognize that these are extraordinary times, we believe it is crucial that public trust be a central consideration for even time-limited technologies. Successful deployment of novel technologies requires public participation. In turn, the public's cooperation depends on their trust in governments and developers, knowing that their best interests have been considered. Technology is not a replacement for policy, and to build public trust the government must demonstrate leadership in anticipating and addressing the technical, social, legal and ethical issues that may arise.

APPENDICES

A. SOCIETY, TECHNOLOGY AND ETHICS IN A PANDEMIC (STEP) EXPERT ADVISORY GROUP

Alan Bernstein, President & CEO
CIFAR, Canada

Alan Bernstein became CIFAR's President and Chief Executive Officer in May 2012. He was previously executive director of the Global HIV Vaccine Enterprise in New York, an international alliance of researchers and funders charged with accelerating the search for an HIV vaccine. From 2000 to 2007, he served as the inaugural president of the Canadian Institutes of Health Research (CIHR), Canada's federal agency for the support of health research. He serves on many advisory boards including the Scientific Advisory Committee on Global Health for the Bill and Melinda Gates Foundation.

Deborah Cook, Professor
McMaster University, Canada

Deborah Cook is a clinician-researcher at McMaster University. She holds an Academic Chair in Critical Care Medicine at McMaster and a Canada Research Chair for Research Transfer in Intensive Care. Deborah practices critical medicine at St. Joseph's Healthcare. She is interested in risk factors for serious illness, prevention of ICU-acquired complications, life support technology, and end-of-life decisions for critically ill patients.

Marc-Antoine Dilhac, Canada CIFAR AI Chair
Université de Montréal and Mila, Canada

Marc-Antoine Dilhac is professor of philosophy at the Université de Montréal and held the Canada Research Chair in Public Ethics and Political Theory (2014-2019). He is also a Canada CIFAR AI Chair at Mila and is director of Deliberation at the Observatory on the social impacts of AI and digital technologies. In 2017, he instigated the project of the Montreal Declaration for a Responsible Development of AI and chaired its scientific committee. His current research focuses on the ethical and social impacts of AI and issues of governance and institutional design, with a particular focus on how new technologies are changing public relations and political structures.

Rebecca Finlay, Vice-President, Engagement & Public Policy (Facilitator)
CIFAR, Canada

Rebecca Finlay founded CIFAR's global knowledge mobilization practice in 2014, bringing together experts in industry, civil society, healthcare and government to accelerate the societal impact of CIFAR's research programs. She leads CIFAR's partnerships with governments and public sector organizations in Canada and worldwide. She serves on the Partnership on AI's Board of Directors and is a Fellow of the American Association for the Advancement of Science (AAAS).

Michael Geist, Professor
University of Ottawa, Canada

Michael Geist is a law professor at the University of Ottawa where he holds the Canada Research Chair in Internet and E-commerce Law and is a member of the Centre for Law, Technology and Society. He regularly appears in the Globe and Mail, is the editor of several monthly technology law publications, and the author of a popular blog on Internet and intellectual property law issues. Michael serves on many boards, including Ingenium, Internet Archive Canada, and the EFF Advisory Board. He is the Chair of the Digital Strategy Advisor Panel for Waterfront Toronto.

Gillian Hadfield, Professor
University of Toronto, Canada

Gillian Hadfield is the inaugural Schwartz Reisman Chair in Technology and Society, Professor of Law, and Professor of Strategic Management. She is also Director of the Schwartz Reisman Institute for Technology and Society. Her research is focused on innovative design for legal and dispute resolution systems in advanced and developing market economies; governance for artificial intelligence (AI); the markets for law, lawyers, and dispute resolution; and contract law and theory.

Bartha Knoppers, Professor
McGill University, Canada

Bartha Maria Knoppers is a Full Professor, Canada Research Chair in Law and Medicine and Director of the Centre of Genomics and Policy of the Faculty of Medicine at McGill University. She is currently Chair of the Ethics Advisory Panel of the World Anti-Doping Agency, and is Co-Chair of the Regulatory and Ethics Workstream of the Global Alliance for Genomics and Health. Her research interests include governance, human rights, biomedical ethics, medical law, and comparative medical law and policy.

The Honourable Anne McLellan, CIFAR Board Vice-Chair (Chair)
CIFAR, Canada

The Honorable Anne McLellan has served four terms as the Liberal Member of Parliament for Edmonton Centre from 1993-2006. She served as Deputy Prime Minister of Canada and as the first Minister of Public Safety and Emergency Preparedness, as well as Minister of Health, Minister of Justice and the Attorney General of Canada, and Minister of Natural Resources and Federal Interlocutor for Métis and Non-Status Indians. Anne joined Bennett Jones in 2006, where she provides strategic advice to the firm and its clients. She is also Vice-Chair of CIFAR's Board of Directors.

Morris Rosenberg, Senior Fellow
University of Ottawa, Canada

Morris Rosenberg served in several senior positions in the Canadian Public Service. He was Deputy Minister of Foreign Affairs (2010-2013), Deputy Minister of Health Canada (2004-2010) and Deputy Minister of Justice and Deputy Attorney General of Canada (1998-2004). Morris was President and CEO of the Pierre Elliott Trudeau Foundation from 2014 to 2018. He is currently a Senior Fellow at the Graduate School of Public and International Affairs at the University of Ottawa.

Mark Schmidt, Canada CIFAR AI Chair
University of British Columbia and Amii, Canada

Mark Schmidt is an associate professor in the Department of Computer Science at the University of British Columbia and is a Canada Research Chair and Alfred P. Sloan Fellow. Mark is also a Canada CIFAR AI Chair at the Alberta Machine Learning Institute (Amii). His research focuses on developing faster algorithms for large-scale machine learning, with an emphasis on methods with provable convergence rates and that can be applied to structured prediction problems.

Ashleigh Tuite, Assistant Professor
University of Toronto, Canada

Ashleigh Tuite is an infectious diseases epidemiologist and an Assistant Professor at the Dalla Lana School of Public Health at the University of Toronto. Her research interests include communicable disease epidemiology, emerging infectious diseases, mathematical modeling, and health economics.

B. INTERNATIONAL ROUNDTABLE PARTICIPANTS

On April 21st, 2020, the STEP EAG held an international roundtable with participants from 10 countries. The EAG is thankful for the insights and perspectives provided by all of the participants who responded to our invitation on short notice. Their advice has informed the recommendations in this report.

Michael Birnhack
Professor
Associate Dean
Buchmann Faculty of Law
Tel Aviv University
ISRAEL

Asaph Young Chun
Director General
Statistics Korea
SOUTH KOREA

Edward Felten
Robert E. Kahn Professor of Computer Science and Public Affairs
Director, Center for Information Technology and Policy
Princeton University
UNITED STATES

Carly Kind
Director
Ada Lovelace Institute
UNITED KINGDOM

Nomi Claire Lazar
Associate Dean of Faculty
Associate Professor of Social Sciences (Politics)
Yale-NUS College
SINGAPORE

Timo Minssen
Professor
Director, JUR Centre for Advanced Studies in Biomedical Innovation Law
University of Copenhagen
DENMARK

Sarah Rispin Sedlak
Instructor, Science and Society
Duke University
UNITED STATES

Ashkan Soltani
Independent Researcher and Technologist
Soltani LLC
UNITED STATES

Effy Vayena
Professor
Department of Public Health
ETH Zurich
SWITZERLAND

Michael Veale
Lecturer, Digital Rights and Regulation
Faculty of Laws
University College London
UNITED KINGDOM

C. CIFAR CONTRIBUTORS

Gaga Boskovic
Raymond Cheah
Amy Cook
Marta Huebsch
Johnny Kung
Catherine Riddell

D. SCAN OF CONTACT/PROXIMITY-TRACING APPS IN USE

The following is an illustrative list of known contact/proximity-tracing applications currently in use by jurisdictions around the world as of April 30th, 2020, including framing legislation wherever possible. These brief summaries have been compiled based on publicly available documentation and press releases, with source material referenced where appropriate.

COUNTRY/ REGION	LAUNCH	DESCRIPTION	UPTAKE	REGULATION
Australia	COVIDSafe[24] launched on April 26th, 2020 by the Department of Health	A voluntary, Bluetooth-based contact-tracing app based on Singapore's OpenTrace model	**2.44 million (approximately 10% of total population)**[25]	On April 25th, the Australian government enacted the Biosecurity Act[26] to legislate how the app is to be used
European Union	An EU toolbox[27] released on April 16th, 2020 by member states	A toolbox for guiding the use of mobile applications for contact tracing and warning in response to COVID-19 by other Members	N/A	The EU mandates that all apps must adhere to the General Data Protection Regulation[28]
Israel	HaMagen[29] launched on March 22nd, 2020 by the Ministry of Health	A voluntary app that cross-checks the GPS history of the user's mobile phone with historical geographic data of patients from the Ministry	**1.5 million (17%)**[30]	On April 26th, the Supreme Court ruled that the government must enact proper legislation for security agency to provide Ministry of Health with cellular location data[31]
Norway	Smittestopp[32] launched on April 16th, 2020 by the Norwegian Institute of Public Health	A voluntary app that uses Bluetooth and location services to identify when users have been in contact with a user diagnosed with COVID-19	**1.6 million (30%)**[33]	On March 27th, the government passed legislation[34] to regulate the use of the app

24 https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
25 https://www.cnn.com/2020/04/28/australia/covidsafe-coronavirus-tracing-app-australia-intl/index.html
26 https://www.legislation.gov.au/Details/F2020L00480
27 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
28 https://gdpr-info.eu/
29 https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/
30 https://www.reuters.com/article/us-health-coronavirus-israel-apps/1-5-million-israelis-using-voluntary-coronavirus-monitoring-app-idUSKBN21J5L5
31 https://www.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUSKCN2280RN
32 https://helsenorge.no/coronavirus/smittestopp
33 https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html
34 https://lovdata.no/dokument/LTI/forskrift/2020-03-27-475

Singapore	TraceTogether[35] launched on March 20th, 2020 by Government Technology Agency	A voluntary Bluetooth-based app that logs contact between participating phones	**1.1 million (20%)**[36]	Use of the app is primarily regulated by the Infectious Diseases Act[37,38]
South Korea	Corona 100m (Co100) launched February 11th, 2020 by a third party and endorsed by the government of South Korea[39,40]	Uses government data (gathered from a variety of sources including phone location data, CCTV footage, and credit card transactions) to alert users when they come within 100 metres of a location visited by an infected person	**>1 million (2%)**[41]	South Korea's responses to COVID-19 are regulated by the 2009 Infectious Diseases Control and Prevention Act[42]

AUSTRALIA

The Australian Department of Health launched COVIDSafe,[43] a contact-tracing phone application based on Singapore's open-sourced OpenTrace technology (see below), on April 26th, 2020. As in Singapore, the app is voluntary, uses Bluetooth to track encounters between participating devices, and encrypts user data to protect privacy. When a user tests positive for COVID-19, with their permission, the encrypted contact information is uploaded by the state and territory health official to a secure IT storage system. The health authority then uses the user's contact history to inform other users who may have been exposed to the virus while protecting the infected user's identity. At the end of the pandemic, users will be prompted to delete the app from their phones, which will delete all app information on a person's phone. The information contained in the IT storage system will also be destroyed at the end of the pandemic. On April 28th, Australia announced over 2.44 million app downloads, about 10% of the total population.[44] The Department of Health commissioned a Privacy Impact Assessment[45] to ensure that privacy risks were being addressed throughout development and deployment for the "privacy by design" app. The commissioned assessment recommends that the source code be released to the public, which the Department says it will do, "subject to consultation with the Australian Signals Directorate's Australian Cyber Security Centre."[46] On April 25th, the Australian government enacted the Biosecurity Act,[47] which legislates how app data can be collected, used, and stored, as well as regulation about coerced use of the app.

EUROPEAN UNION

EU member states announced on April 16th, 2020 that they have developed an EU toolbox[48] for the use of mobile applications for contact tracing and warning in response to COVID-19.[49] This toolbox provides a practical guide for member states for how

35 https://www.tracetogether.gov.sg/
36 https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html
37 https://www.moh.gov.sg/policies-and-legislation/infectious-diseases-act
38 https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea
39 https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
40 http://www.korea.net/NewsFocus/Society/view?articleId=183129
41 https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html
42 https://www.loc.gov/law/help/health-emergencies/southkorea.php
43 https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
44 https://www.cnn.com/2020/04/28/australia/covidsafe-coronavirus-tracing-app-australia-intl/index.html
45 https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf
46 https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-agency-response.pdf
47 https://www.legislation.gov.au/Details/F2020L00480
48 https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
49 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670

to implement their own contact-tracing apps, with essential requirements that include that they should be fully compliant with the EU data protection and privacy rules; be implemented in close coordination with public health authorities; be installed voluntarily and deleted when they are no longer needed; use privacy-enhancing technology, such as Bluetooth rather than location tracking; be based on anonymized data; be interoperable across the EU; and be anchored in accepted epidemiological guidance that reflects best practices in cybersecurity and accessibility. EU public health authorities will assess the effectiveness of their respective apps at the national and cross-border levels by April 30th, and will report on their processes by May 31st.

ISRAEL

On March 22nd, 2020, the Israeli Ministry of Health launched the HaMagen[50] phone application with the intention of tracing whether users have been in the presence of anyone diagnosed with COVID-19. The app cross-checks the GPS history of the user's mobile phone with historical geographic data of patients from the Ministry of Health. The app will send users updates and show users the exact time and location where they may have had contact with a COVD-19 patient. The user can then review and confirm or reject. If the user confirms that this contact and potential contamination took place, he or she will receive information about how to report their exposure to the Ministry. GPS history and data is kept on the user's phone and is not sent to a third party, nor back to the Ministry, though there are plans to implement changes to the app in the future to allow diagnosed individuals to share their trajectories with the Ministry. The user is responsible for reporting incidents of contamination based on the information about existing cases provided through the app. The Ministry announced that the app had been downloaded by approximately 1.5 million users, about 17% of the total population.[51] The Ministry has open-sourced the source code with the intention of making the app available to the rest of the world and maximizing transparency. In addition to the app, Israel's domestic security agency Shin Bet had been using cellular network data to track the movement of COVID-positive individuals before and after diagnosis, providing the information to the Ministry of Health to alert potential contacts. On April 26th, Israel's supreme court ruled that the government must enact proper legislation (rather than emergency regulations) before it can continue the practice.[52]

NORWAY

The Norwegian Institute of Public Health (NIPH) launched Smittestopp,[53] a voluntary app designed to notify users when they have been in close contact with another app user who has been diagnosed with COVID-19, on April 16th, 2020. In the first few weeks of operation, the Smittestopp app will primarily collect data about user movements; once the notification system is implemented, users will be able to receive messages about potential exposure to infection and will be advised about how to avoid infecting others. The app uses Bluetooth and location services to detect when other app users are nearby and notifies users via SMS messaging. Through the app, the NIPH receives anonymized data about social movement patterns, which are monitored to analyze the effectiveness of restriction measures and help determine when they should be lessened or tightened. User data is available only to authorized personnel when a user tests positive for COVID-19; when users are notified about potential contact, the infected user is not identified. On March 27th, the Norwegian government passed legislation[54] to regulate the use of this app, mandating the use and storage of user data. Among other details, the Act requires that location data be deleted after 30 days, or once the app has been deleted from a user's phone. The NIPH announced that 1,427,000 users, about 26% of a total population of 5.5 million, had downloaded the app

50 https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/
51 https://www.reuters.com/article/us-health-coronavirus-israel-apps/1-5-million-israelis-using-voluntary-coronavirus-monitoring-app-idUSKBN21J5L5
52 https://www.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUSKCN2280RN
53 https://helsenorge.no/coronavirus/smittestopp
54 https://lovdata.no/dokument/LTI/forskrift/2020-03-27-475

in the week following its launch.[55] Uptake is estimated to be close to 30% as of April 29th.[56]

SINGAPORE

On March 20th, 2020, Singapore launched TraceTogether,[57] a voluntary Bluetooth-based contact-tracing app. The first in the world, it is built on the BlueTrace protocol,[58] designed by the Government Digital Services team at the Government Technology Agency of Singapore. TraceTogether logs Bluetooth encounters between participating devices, which exchange non-personally identifiable messages that are stored in the users' encounter history on their own devices.[59] Users who become infected are asked to share their encounter history with the health authority, which cannot directly access user data but is the sole entity with the power to decrypt it. BlueTrace is designed to supplement manual contact tracing not only by being more scalable and less resource intensive, but also by giving more details about an infected person's contact history. It is also intended to protect user privacy by anonymizing and encrypting their contact history and personal data. As of April 17th, approximately 1 million people had installed the app, approximately 17% of the total population.[60,61] Since its launch, Singapore has open-sourced the app as OpenTrace, which has been adopted by Australia (see above) and is being considered by New Zealand. Though use of the app is voluntary, refusal to share the app's data with the Ministry of Health may be subject to prosecution under the Infectious Diseases Act,[62,63] under which it is a criminal offence for anyone to withhold or provide inaccurate information to Ministry officials during contact tracing. On February 26th, two individuals were charged under the Act for giving officials false information about their movements and whereabouts.[64]

SOUTH KOREA

While the government of South Korea has not itself launched an official contact-tracing app,[65] apps developed by third parties are popular and have been endorsed by the government. The most popular app, Corona 100m (Co100), was launched on February 11th, 2020, and uses government data (gathered from a variety of sources including phone location data, CCTV footage, and credit card transactions) to alert users when they come within 100 metres of a location visited by an infected person.[66,67] The app shares the patient's diagnosis date, nationality, age, gender, and prior locations, but protects the patient's identity by assigning a case number.[68] The app is intended to help users avoid potentially dangerous locations without checking the travel histories of those infected. The government has also endorsed Coronamap,[69] which shows the travel histories of confirmed COVID-19 patients, and Coronaita[70], which acts like a search engine to provide information on coronavirus-hit areas. Coronamap was designed to visually present government data about COVID-19 cases in a way that was understandable and accessible for the public.[71] South Korea's quick response to COVID-19 has capitalized on public health strategies developed since the 2015 MERS outbreak.

55 https://www.forbes.com/sites/davidnikel/2020/04/25/norway-14-million-people-download-coronavirus-tracking-app-despite-security-concerns/#7608331c7832
56 https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html
57 https://www.tracetogether.gov.sg/
58 https://bluetrace.io/
59 https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf
60 https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea
61 https://theconversation.com/the-coronavirus-contact-tracing-app-wont-log-your-location-but-it-will-reveal-who-you-hang-out-with-136387
62 https://www.moh.gov.sg/policies-and-legislation/infectious-diseases-act
63 https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea
64 https://www.moh.gov.sg/news-highlights/details/two-charged-under-infectious-diseases-act-for-false-information-and-obstruction-of-contact-tracing
65 On March 7th, 2020, the Ministry of the Interior and Safety launched a Self-isolation Safety Application, designed to monitor individuals that are required to self isolate. Through this app, those who have been ordered to stay home are able to stay in contact with and update case workers on their progress and activity: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/
66 https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
67 http://www.korea.net/NewsFocus/Society/view?articleId=183129
68 https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia
69 https://coronamap.site/
70 https://coronaita.com/#/
71 https://www.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html

E. FURTHER READING

Ada Lovelace Institute. "Exit Through the App Store? A Rapid Evidence Review of the Technical Considerations and Societal Implications of Using Technology to Transition from the COVID-19 Crisis." *Ada Lovelace Institute*, 20 April 2020

https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf.

European Commission. "Joint European Roadmap Towards Lifting COVID-19 Containment Measures." *European Commission*, European Union, 14 April 2020

https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf.

Gasser, Urs, Mercello Ienca, James Scheibner, Joanna Sleigh, and Effy Vayena. "Digital Tools against COVID-19: Framing the Ethical Challenges and How to Address Them."

https://arxiv.org/ftp/arxiv/papers/2004/2004.10236.pdf.

Hart, Vi, et al. "Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks." *Edmond J. Safra Center for Ethics*, Harvard University, 3 April 2020

https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf.

Kim, Dongwoo and Daniela Rodriguez. "'There's an App for That': Use of COVID-19 Apps in Singapore and South Korea." *Asia Pacific Foundation of Canada*, 27 April 2020

https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea.

McDonald, Sean. "The Digital Response to the Outbreak of COVID-19." *Centre for International Governance Innovation*, 30 March 2020

https://www.cigionline.org/articles/digital-response-outbreak-covid-19.

Nature Editorial Board. "Show Evidence that Apps for COVID-19 Contact-Tracing Are Secure and Effective." *Nature,* Springer Nature, 29 April 2020

https://www.nature.com/articles/d41586-020-01264-1.

Office of the Privacy Commissioner of Canada. "A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19." *Office of the Privacy Commissioner of Canada*, Government of Canada, April 2020

https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/.

Soltani, Ashkan, Ryan Calo and Carl Bergstorm. "Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis." *TechStream*, Brookings Institute, 27 April 2020

https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

The Government of the Republic of Korea. "Flattening the Curve on COVID-19: How Korea Responded to a Pandemic Using ICT." *UNDP Seoul Policy Centre for Knowledge Exchange through SDG Partnerships*, United Nations Development Program, 15 April 2020

http://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2019/flattening-the-curve-on-covid-19.html.

CIFAR

CIFAR is a Canadian-based global charitable organization that convenes extraordinary minds to address the most important questions facing science and humanity.

MaRS Centre, West Tower
661 University Ave., Suite 505
Toronto, ON M5G 1M1 Canada

cifar.ca
@CIFAR_News
Facebook.com/CIFAR
Linkedin.com/company/CIFAR

For partnership opportunities, contact donations@cifar.ca