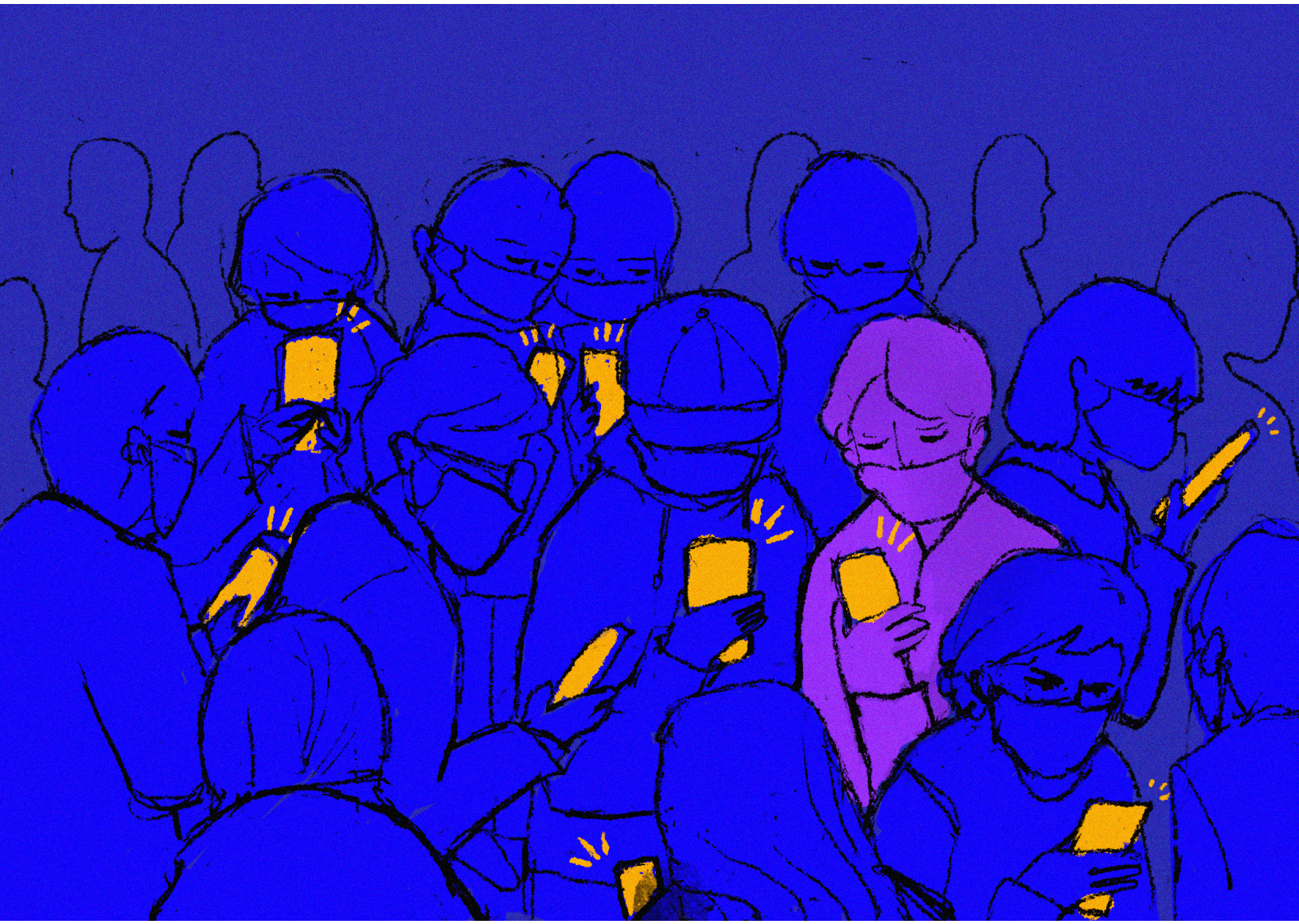
Pandemic Privacy

A preliminary analysis of collection technologies, data collection laws, and legislative reform during COVID-19

By Benjamin Ballard, Amanda Cutinha, and Christopher Parsons

SEPTEMBER 28, 2021
RESEARCH REPORT #144



munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO
THECITIZENLAB

Copyright

Electronic version first published by the Citizen Lab in 2021. This work can be accessed through https://citizenlab.ca.

Document Version: 1.0

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the authors

Benjamin Ballard contributed to this report while a fellow at the Citizen Lab. He is currently a Cybersecurity Engineer at the MITRE Corporation. He received his BA in International Relations at Connecticut College and MALD from the Fletcher School of Law and Diplomacy at Tufts University.

Amanda Cutinha contributed to this report while a fellow at the Citizen Lab. She is currently an Articling Student at Miller Thomson LLP. She received her BA Hons. and JD from the University of Toronto.

Christopher Parsons is currently a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Bachelor's and Master's degrees from the University of Guelph and his PhD from the University of Victoria.

Acknowledgements

We would, first, like to thank the first responders and health professionals who have been on the front lines of the pandemic response in the United States, United Kingdom, and Canada. Their courage, resilience, and compassion are a credit to themselves and their professions.

Several of our colleagues have generously shared their thoughts on early versions of this report. We thank Tamir Israel and Irene Poetranto, as well an individual who cannot be identified for professional reasons, for their detailed feedback and guidance in crafting the final version of this work. All remaining errors are our own.

This document could not have been produced without the able assistance and guidance by the Citizen Lab's communications team and operations manager. We thank Miles Kenyon and Mari Zhou for their contributions, and Adam Senft for helping to keep the report production process on track.

Copyedits were performed by Joyce Parsons of Stone Pillars Editing and Consulting.

We appreciated the opportunity to raise, and discuss, many of the issues addressed in this report in other venues ahead of its publication. In particular, *Policy Options*, *CBC*, *First Policy Response*, and *Slate* have hosted our writing about how governments have responded to the pandemic, and how some of their activities should be adjusted. Our opportunities to participate in roundtable discussions and panels about COVID-19, including those run by the Internet Society and the Canadian Bar Association, were helpful in testing our hypotheses and fleshing out some arguments we have further developed in this report.

This work was supported by the MacArthur Foundation, Ford Foundation, Open Society Foundations, Sigrid Rausing Trust, and Oak Foundation whose generous funding made this report possible. It was undertaken under the supervision of Prof. Ronald Deibert.

Corrections and Questions

Please send all questions and corrections to the author directly at:
chris@citizenlab.ca

Suggested Citation

Benjamin Ballard, Amanda Cutinha, and Christopher Parsons. “Pandemic Privacy: A preliminary analysis of collection technologies, data collection laws, and legislative reform during COVID-19,” Citizen Lab Research Report No. 144, University of Toronto, September 2021.

Contents

Table of Information Boxes

Table of Figures

Table of Acronyms

Application Programming Interface	API
Canadian Health Protection Act	CHPA
Center for Disease Control	CDC
Consumer Privacy Protection Act	CPPA
Coronavirus Disease of 2019	COVID-19
Digital Global Health & Humanitarianism Lab	DGHH Lab
Emergency Management Act	EMA
Emergency Management of Civil Protection Act	EMCPA
European Union	EU
General Data Protection Regulation	GDPR
Global Positioning System	GPS
Google/Apple Exposure Notification	GAEN
Health Information Custodian	HIC
Health and Human Services	HHS
Internet Protocol	IP
National Health Service	NHS
Office of the Privacy Commissioner of Canada	OPC
Personal Health Information Protection Act	PHIPA
Personal Information Protection and Electronic Documents Act	PIPEDA
Public Health Agency of Canada	PHAC
Public Health Agency of Canada Act	PHACA
Personal Protective Equipment	PPE
Severe Acute Respiratory Syndrome	SARS
World Health Organization	WHO

Executive Summary

Phrases like "[t]he pandemic which has just swept round the earth has been without precedent"[1] have been commonly read or heard throughout the COVID-19 pandemic. At the onset of the COVID-19 pandemic, there was a race to restrict mobility, undertake health surveillance to determine the source or cause of local outbreaks, and secure personal protective equipment for healthcare workers and domestic populations. Further and as in past health emergencies, there were efforts to collect and leverage available information to make sense of the spread of the disease, understand the nature of supply chains so as to determine what equipment was available to treat those affected by the disease or provide assistance to those afflicted with it, as well as to understand how the novel coronavirus was transmitted and its effects so as to develop vaccines to mitigate its worst repercussions.

In, "Pandemic Privacy: A preliminary analysis of collection technologies, data collection laws, and legislative reform during COVID-19," we undertake a preliminary comparative analysis of how different information technologies were mobilized in response to COVID-19 to collect data, the extent to which Canadian health or privacy or emergencies laws impeded the response to COVID-19, and ultimately, the potential consequences of reforming data protection or privacy laws to enable more expansive data collection, use, or disclosure of personal information in future health emergencies. In analyzing how data has been collected in the United States, United Kingdom, and Canada, we found that while many of the data collection methods could be mapped onto a trajectory of past collection practices, the breadth and extent of data collection in tandem with how communications networks were repurposed constituted novel technological responses to a health crisis. Similarly, while the intersection of public and private interests in providing healthcare and government services is not new, the ability for private companies such as Google and Apple to forcefully shape some of the technology-enabled pandemic responses speaks to the significant ability of private companies to guide or direct public health measures that rely on contemporary smartphone technologies. While we found that the uses of technologies were linked to historical efforts to combat the spread of disease, the nature and extent of private surveillance to enable public action was arguably unprecedented.

Turning from the technologies involved to collect data, we shift to an analysis of how Canadian law enabled governmental collections, uses, and disclosures of personal information and how legislation that was in force before the outbreak of COVID-19 empowered governments to overcome any legal hurdles that might have prevented state agencies from using data to address COVID-19 in Canada. Despite possessing this lawful authority,

1 Goerge A. Soper. (1919). "The Lessons of the Pandemic," *Science* 49(1274).

however, governments of Canada were often accused of inadequately responding to the pandemic, and they, in turn, sometimes suggested or indicated that privacy legislation impaired their abilities to act. These concerns have precedent insofar as they were raised following the 2003 SARS pandemic, but they were then--as now--found to be meritless: privacy legislation has not been an impediment to data collection, use, or sharing, despite claims to the contrary. The challenges faced by governments across Canada were, in fact, precedented and linked to poor governmental policies and capabilities to collect, use, and share data just as in past health crises.

Perhaps partially in response to perceptions that privacy rights afforded to Canadians impeded the pandemic response, the federal government of Canada introduced legislation in August 2020 (which ultimately did not get passed into law due to an election) that would both have reified existing exemptions to privacy protections while empowering private companies to collect, use, and disclose personal information for further 'socially beneficial practices' without first obtaining individuals' consent. While it is hardly unprecedented for governments to draft and introduce privacy legislation that would expand how personal information might be used, the exclusion of human rights to balance commercial uses of personal information stands as a novel decision where such legislation is now regularly linked with explicit human rights protections.

This report proceeds as follows. After a short introduction in Section one, we present the methodologies we used in Section two. Section three turns to how contemporary digital technologies were used to collect data in the United States, United Kingdom, and Canada. Our principal finding is that collection efforts were constrained by the ways in which private companies chose to enable data collection, particularly in the case of contact tracing and exposure notifications, and by how these companies choose to share data that was under their control and how data was repurposed for assisting in containing COVID-19. The breadth and extent of data collection was unprecedented when compared to past health crises.

In Section four, we focus on Canadian legal concerns regarding the extent to which privacy and civil liberties protections affected how the federal and provincial governments handled data in their responses to the COVID-19 pandemic. We find that privacy legislation did not establish any notable legal barriers for collecting, sharing, and using personal information given the permissibility of such activities in health emergencies, as these actions are laid out in provincial health and emergencies laws. More broadly, however, the legislative standard that allows for derogations from consent in emergency situations may be incompatible with individuals' perceptions of their privacy rights and what they consider to be 'appropriate' infringements of these rights, especially when some individuals contest the gravity (or even existence) of the COVID-19 pandemic in the first place.

Section five turns to how next-generation privacy legislation, such as the *Consumer Privacy Protection Act (CPPA*), might raise the prospect of significant changes in how data could be collected, used, or disclosed in future health crises. The *CPPA* did not enter into law as a result of a Canadian federal election, which killed the bill on the Order Paper. Nonetheless, we find that a law such as the *CPPA* could facilitate unprecedented non-consensual handling of personal information.

Section six presents a discussion of the broader themes that cut across the report. These include how the pandemic further reveals the redistribution of power between states and private organizations, the need for novel digital epidemiological processes to have strong bioethics and equitable commitments for those involved in digital epidemiological experiments, and the need to assess the roles of consent in future health emergencies, especially when new legislative frameworks might permit more permissive and non-consensual data collection, use, and disclosure for health-related purposes. Section seven presents a short conclusion to our report.

1. Introduction

The ways in which governments, private organizations, and residents alike responded to the COVID-19 pandemic were regularly declared as being 'unprecedented' despite them being at least partially based on historical experiences linked to past pandemics. At the onset of the COVID-19 pandemic, there was a race to restrict mobility, undertake health surveillance to determine the source or cause of local outbreaks, and secure personal protective equipment for healthcare workers and domestic populations. Further, as in past health risks, there were efforts to collect and leverage available information to make sense of the spread of the disease,[2] understand the nature of supply chains to determine what equipment was available to treat those affected by the disease or provide assistance to those afflicted with it,[3] as well as to understand how the coronavirus was transmitted and its effects so as to develop vaccines to mitigate its worst effects.

In many nations, including the United States and Canada, lagging and unequal investments in health information technologies meant that federal, state/provincial, and municipal governments often struggled to intake, process, make sense of, or share collected information.[4] In the context of COVID-19, a handful of technologies and rafts of data sets were explored by public and private stakeholders to respond to the pandemic. Smart thermometers were initially regarded as potentially revealing whether COVID-19 was spreading through given populations,[5] a series of smartphone applications were created to enable contact tracing or exposure notification as well as to enforce quarantine orders,[6] and telecommunications networks were seen as ways of assessing population

2 See as e.g., The Government of Republic of Korea. (2020). "Flattening the curve on COVID-19 (Report)," The Government of the Republic of Korea (April 15, 2020).

3 See as example, Andrew Leonard. (2020). "How Taiwan's Unlikely Digital Minister Hacked the Pandemic," *Wired*. Available at: https://www.wired.com/story/how-taiwans-unlikely-digital-minister-hacked-the-pandemic/.

4 American Hospital Association. (2019). "Sharing Data, Saving Lives: The Hospital Agenda for Interoperability," *AMA*. Available at: https://www.aha.org/system/files/2019-01/Report01_18_19-Sharing-Data-Saving-Lives_FINAL.pdf; Vikas N. O'Reilly-Shah et al. (2020). "The COVID-19 Pandemic Highlights Shortcomings in US Health Care Informatics Infrastructure: A Call to Action," *Anesthesia & Analgesia* 131(2): 340-344; Amanda L. Terry et al. (2014). "Gaps in Primary Healthcare Electronic Medical Record Research and Knowledge: Findings of a Pan-Canadian Study," *Health Policy* 10(1): 46-59.

5 Donald G. McNeil Jr. (2020). "Can Smart Thermometers Track the Spread of the Coronavirus?" *New York Times.* Available at: https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html.

6 Dongwoo Kim and Daniela Rodriguez. (2020). "'There's an App for That': Use of COVID-19 Apps in Singapore and South Korea," *Asia Pacific Foundation of Canada*. Available at: https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea; Katie Dangerfield. (2020). "Canada launches COVID-19 tracking app — but only in Ontario," *Global News*. Available at: https://globalnews.ca/news/7239119/coronavirus-exposure-notification-app-covid-19-ontario/; Matt Burgess. (2020). "Everything you need to know about the new NHS contact tracing app," *Wired.* Available at: https://www.wired.co.uk/article/nhs-covid-19-tracking-app-contact-tracing.

movements and potentially facilitating contact tracing.[7] Furthermore, a host of private companies raced to suggest or offer ways that governments could marshal data using proprietary data stores, data processes, or integration systems to better get the pandemic under control.[8]

Information Box One: The Onset of COVID-19

The Wuhan Municipal Health Commission in China first detected a cluster of pneumonia cases on December 31, 2019, which would subsequently be identified as COVID-19 cases. The World Health Organization (WHO) thereafter published technical guidance for states in mid-January as cases quickly propagated around the world. COVID-19 cases were first diagnosed in the United States, United Kingdom, and Canada on January 21, 29, and 25, 2020, respectively. It was not until March 11, 2020, that the WHO declared the novel coronavirus a pandemic on the basis that the world was experiencing, "an epidemic occurring worldwide, or over a very wide area, crossing international boundaries and usually affecting a large number of people."[9] Concurrent with the declaration, governments around the world that were heavily affected by the disease began to rapidly accelerate restrictions on freedoms of movement and association. Businesses in the United States, United Kingdom, and Canada were advised that they should permit employees to work remotely, while the governments simultaneously began creating policies intended to mitigate the possible fiscal impacts of mobility and association restrictions and the related impacts to individuals' economic well-being.

Alongside technology-focused efforts were persistent questions about the extent to which civil liberties inhibited private companies or public institutions from responding to the pandemic[10] as well as the efficacy of such technology-driven interventions. Specifically,

7 Serina Chang, Emma Pierson, Pang Wei Koh, Jaline Gerradin, Beth Redbird, David Grusky, and Jure Leskovec. (2020). "Mobility network models of COVID-19 explain inequities and inform reopening," *Nature* 589.

8 British Medical Association. (2020). "Public Services Private Profit: The role of private outsourcing in the COVID-19 response," BMA. Available at: https://www.bma.org.uk/media/2885/the-role-of-private-outsourcing-in-the-covid-19-response.pdf; Lizette Chapman. (2020). "Palantir's New 'Driving Thrust': Predicting Coronavirus Outbreaks," *Bloomberg*. Available at: https://www.bloombergquint.com/markets/coronavirus-news-palantir-gives-away-data-mining-tools; Teressa Scassa. (2020). "Pandemic Privacy (The Ethics of COVID)," Center for Ethics. Available at: https://www.youtube.com/watch?v=sSV4bJaVgto&feature=emb_title; minute 20:20.

9 Miquel Porta. (2014). "Pandemic," in *A Dictionary of Epidemiology* (5 Ed.). Oxford University Press. Available at: https://www.oxfordreference.com/view/10.1093/acref/9780195314496.001.0001/acref-9780195314496-e-1373.

10 Alexander Bernier and Bartha Maria Knoppers. (2020). "Pandemics, privacy, and public health research," *Canadian Journal of Public Health* 111.

civil liberties or other legal restrictions have been perceived as inhibiting some technology-enabled responses by public and private organizations that are seen as novel,[11] though many of the technologies deployed to mitigate COVID-19 as well as the legal rationales underpinning them have historical legacies.[12] These technologies were also met with doubts that they would meaningfully assist governments in responding to COVID-19 on the basis that the technologies had, in many cases, never before been tested at this scale. What remains to be seen is the extent to which the more contemporary concerns were continuations of past health-related debates, whether the technologies and policies that were adopted to combat the pandemic were truly novel and raised substantively new legal concerns, as well as whether they were meaningfully helpful in alleviating the spread of COVID-19.

This report undertakes a preliminary comparative analysis of how different information technologies were mobilized in response to COVID-19 to collect data, the extent to which health or privacy or emergencies laws impeded the response to COVID-19 in Canada, and ultimately, the potential consequences of reforming data protection or privacy laws to enable more expansive data collection, use, or disclosure in future health emergencies. After outlining our methodology in Section two, we undertake an exploratory assessment in Section three of the commonalities and differences between data collection in prior pandemic situations versus in the COVID-19 health crisis in the United States, United Kingdom, and Canada. This analysis lets us compare how allied countries, which have different political cultures, adopted technologies to collect data to inform their pandemic responses and the extent(s) to which collections significantly deviated from data collection in previous health emergencies.

Our main finding in Section three is that collection efforts were often constrained based on the ways in which private companies chose to enable data collection, particularly in the case of contact tracing and exposure notifications, and by how these companies chose to share data that was under their control and how data was repurposed for assisting in containing COVID-19. This said, the sheer amount of data that companies either collect about individuals, as is the case for mobile device companies and telecommunications companies, or about the presence of disease indicators and potential spread of disease, such as in the case of the Canadian AI-driven epidemiology company BlueDot, speaks to the potential for these digital systems to be leveraged as the current pandemic

11 Tiffany C. Li. (2020). "Privacy In Pandemic: Law, Technology, and Public Health in the Covid-19 Crisis," *Loyola University Chicago Law Journal*, Volume 52 (3).

12 Colleen M. Flood, Bryan Thomas, and Kumanan Wilson. (2020). *Reconciling Civil Liberties and Public Health in the Response to COVID-19.* Royal Society of Canada.

continues as well as in any future equivalent health emergencies. We ultimately find that the breadth and extent of data collection was unprecedented when compared to past health crises.

In Section four, we focus on Canadian legal concerns regarding the extent to which privacy and civil liberties protections affected the sharing of data in federal and provincial governments' responses to the COVID-19 pandemic. We find that privacy legislation did not establish any notable legal barriers for collecting, sharing, and using personal information given the permissibility of such activities in health emergencies, as laid out in provincial health and emergencies laws. More broadly, however, the legislative standard that allows for derogations from consent in emergency situations may be incompatible with individuals' perceptions of their privacy rights and what they consider to be 'appropriate' infringements of these rights, especially when some individuals contest the gravity (or even existence) of the COVID-19 pandemic in the first place. The mismatch between the law and normative expectations of privacy, while pronounced during the COVID-19 pandemic, is not a new or unprecedented situation.

Section five considers how next-generation privacy legislation, such as the *Consumer Privacy Protection Act (CPPA*), might raise the prospect of significant changes in how data might be collected, used, or disclosed in future health crises. The CPPA did not receive Royal Assent, and it did not become law as a result of a Canadian federal election being called, which killed the bill on the Order Paper. Nonetheless, our finding is that such a law as the *CPPA* could facilitate unprecedented and non-consensual handling of personal information.

We conclude in Section six with a discussion of the broader themes that cut across this report. These themes include how the pandemic reveals a redistribution of power between states and private organizations, the need for novel digital epidemiological processes to have strong bioethical commitments and equity commitments for those implicated in digital epidemiological experiments, and the need to assess the roles of consent in future health emergencies, especially when new legislative frameworks might permit more permissive and non-consensual data collection, use, and disclosure for health-related purposes.

2. Methodology

Using a cross- and sub-national comparative approach, we looked at how different technologies were used in the United States, United Kingdom, and Canada to facilitate COVID-19 pandemic-related data collection and at how these technologies were linked with past data collection processes. We also engaged in legal analysis to assess how Canadian emergency, health, and privacy legislation has enabled or inhibited data collection and sharing in past health emergencies and during the first year of the COVID-19 pandemic. For this last analysis, we used a case study of Canada's COVID Alert smartphone application. Finally, we analyzed the prospective implications of draft legislation on private organizations' abilities to collect, use, or disclose personal information to prevent or respond to a health crisis in the future. These methods let us assess whether the technologies used were significantly out of step with those used in the past, whether Canadian privacy legislation inhibited data collection and distribution to combat the spread of COVID-19 in Canada, and whether proposed legislation such as the *Consumer Privacy Protection Act* in Canada might establish a legal framework that could facilitate significant reforms of private-sector health-related surveillance in the future. In aggregate, our methodological choices let us assess the extent to which governmental responses in the countries under review constituted unprecedented kinds of activities or reflected a continuance of how governments had previously responded to serious health crises.

We used desk research to collate data and conducted limited informal interviews and meetings to validate the results of that research. We focused on collating information about how private organizations and governments have responded to the COVID-19 pandemic and aggregated information from corporate transparency reports, statements, and publications by government officials and corporate representatives, news reports, and existing laws and policies, as well as emergency-measures orders issued by Canadian provincial governments. We also reviewed academic literature concerning pandemic responses; literature on transparency and accountability issues, policy-making, and public-private collaborations; and legal literature(s) pertaining to privacy, human rights, and civil rights laws in Canada.

We principally focused on the collection of health data. This focus on collection, particularly in the technologies used in the United States, United Kingdom, and Canada, was justified on the basis that the pandemic is ongoing and, thus, how data collection is understood and acted upon remains in flux. Within the collection process, we focused on how technologies had been used to try and interrupt community transmission (e.g., using contact-tracing and exposure-notification technologies), conduct digital epidemiological surveillance (e.g., relying on mobile device data to track population movements), and implement distributed rapid case identification systems (e.g., deploying automated

self-diagnosis systems). While each of these elements of the data collection process have conceptual links with processes that have been adopted and used to guide public health practitioners in the past, our analysis sought to assess whether data collection practices significantly expanded upon prior conceptual frameworks.

In Canada, we focused on federal legislation as well as that of the provinces of British Columbia, Quebec, and Ontario. Together, these provinces provide a cross-section of the Canadian legal instruments that were used to govern pandemic response, with each province following different private sector privacy legislation, emergency legislation, and public health information legislation. We reviewed privacy, health, and emergency legislation in operation, both federally and provincially, to understand the legislative framework that governed the collection, use, and disclosure of personal information (including personal health information) by private and public entities amid public health crises. After mapping the timeline of these legislative enactments and amendments onto the history of disease in Canada, we looked at the legislative context of the 2003 Severe Acute Respiratory Syndrome (SARS) outbreak in Canada, during which information sharing was perceived as being problematic, to assess the arguments that privacy protection legislation had impeded information sharing during that health emergency. We reviewed the government-commissioned National Advisory Committee on SARS and Public Health's report entitled, *Learning from SARS: Renewal of Public Health in Canada*. After assessing concerns raised in the report about (the then) newly enacted federal privacy legislation, we examined how legislative and jurisprudential changes after SARS affected information sharing that occurred during the COVID-19 pandemic using the COVID Alert application as a case study.

Finally, we examined proposed federal privacy law reform in Canada to assess the potential implications of future legislation of its kind on the ability of private organizations to collect, use, or disclose information to other private or governmental organizations in future health emergencies. Our analysis of this proposed reform was guided by the fact that it was introduced during the COVID-19 pandemic. As such, it was presumably designed to remedy the challenges that the existing legislation posed and to create a new basis for privacy legislation that affects private organizations in Canada. Given that proposed federal privacy law reform is needed, at least in part, for Canada to be deemed 'adequate' by European regulators, thus ensuring that Canadian businesses can continue to process Europeans' data, the reform also offered a potential example of how countries might update their privacy legislation to enable pandemic-related responses while (presumptively) being compliant with European data protection requirements.

3. Exceptionality of Data Collection Technologies

Phrases like, "[t]he pandemic which has just swept round the earth has been without precedent"[13] have been commonly seen or heard throughout the COVID-19 pandemic. They have been used to characterize not just the public health crisis, but the subsequent responses to it as well. Some technologists, policy makers, and members of the public have perceived technology as a 'silver bullet'[14] as they hoped that it could provide innovative solutions to contain the coronavirus.[15] Over the course of the pandemic, public health officials relied on a range of technologies, including digital symptom checkers, digital epidemiological surveillance, and mobile contact-tracing applications to collect data regarding the disease. These technologies were representative of three central ways of containing disease outbreaks: public health surveillance, case identification, and contact tracing.[16] When these technological innovations are analyzed together, they illustrate data collection at distinct junctures in the American, British, and Canadian responses to COVID-19. While the aforementioned technologies may be novel—insofar as they had never been deployed before or are currently being deployed on a wider scale than ever before—novelty alone does not mean that their use is unprecedented or that they constitute new ways of combating disease that break from past processes or techniques.

We begin this section of the report by discussing how public health officials in the United States, United Kingdom, and Canada have historically categorized different elements of the data life cycle and explain why we focused on the data-collection stage. Next, we turn to how states sought to surveil, identify, and interrupt the spread of disease, and we discover how these activities have evolved in recent decades. We then examine how digital symptom checkers, digital community surveillance, and mobile contact-tracing applications have affected information collection during the COVID-19 pandemic. We conclude with a brief analysis of the ways in which data has been collected throughout the COVID-19 pandemic in order to assess the novelty of public health responses that

13 George A. Soper. (1919). "The Lessons of the Pandemic," *Science* 49(1274).

14 Shira Ovide. (2020). "Technology Will Not Save Us," *New York Times*. Available at: https://www.nytimes.com/2020/04/29/technology/coronavirus-contact-tracing-technology.html.

15 Jennifer Valentino-DeVries, Natasha Singer and Aaron Krolik. (2020). "A Scramble for Virus Apps That Do No Harm," *New York Times.* Available at: https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html.

16 Jobie Budd, Benjamin S. Miller, Erin M. Manning, Vasileios Lampos, Mengdie Zhuang, Michael Edelstein, Geraint Rees, Vincent C. Emery, Molly M. Stevens, Neil Keegan, Michael J. Short, Deenan Pillay, Ed Manley, Ingemar J. Cox, David Heymann, Anne M. Johnson, and Rachel A. McKendry. (2020). "Digital technologies in the public-health response to COVID-19," *Nature Medicine* 26, 1183-1192. This framework mirrors that of Budd et al. with the exception of public communications, which fall outside the scope of this report.

leveraged the aforementioned technologies. In assessing the extent to which these technologies were unprecedented, we ultimately conclude that though they are reflective of long-standing trends in data collection to manage disease outbreaks, they nevertheless represent unprecedented extensions of how, and how much, data can be collected by private sector parties to facilitate public responses to outbreaks of disease.

3.1 - Data Life-Cycle Framework

Governments use data to code and quantify the world in a manner that is intrinsically political,[17] and the same is true when they collect data about outbreaks of disease. Information Box Two summarizes how we map the data life cycles that are adopted by the American, British, and Canadian governments onto the data collection, understanding, and action model we use throughout our report.

Information Box Two: Data Life Cycles

The United States National Library of Medicine draws on the Carnegie Mellon University Data Management Plan: Design; Plan; Collect; Analyze; Publish/Preserve; and, Re-Use.[18]

In the United Kingdom, the Government Data Quality Hub has developed the Government Data Quality Framework. This framework divides the data life cycle into six ages: Plan; Collect, acquire, ingest; Prepare, store and maintain; Use and process; Share and publish; and, Archive or destroy.[19]

The Canadian Health Information Management Association has its own cycle: Collection; Capture and organization; Maintenance and preservation; Use and disclosure; Final disposition and destruction; and, Evaluation.[20]

These three models evoke a singular model that describes how data is collected, understood, and then acted upon.

17 Kate Crawford, Kate Miltner, and Mary L. Gray. (2014). "Critiquing Big Data: Politics, Ethics, Epistemology (Special Section Introduction)," *International Journal of Communication* 8.

18 CMU Libraries. "Data management 101," *Carnegie Mellon University*. Available at: https://library.cmu.edu/datapub/dms/data/101; NIH National Library of Medicine. (2020). "Data Management Plan," *Network of the National Library of Medicine*. Available at: https://nnlm.gov/data/data-management-plan.

19 Government Data Quality Hub. (2020). "Guidance: The Government Data Quality Framework," *Government of the United Kingdom*. Available at: https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework#The-Data-Lifecycle.

20 Kelly J. Abrams, Shirley Learmonth, and Candace J. Gibson. (2017). T*he Canadian Health Information Management Lifecycle.* Lulu Publishing Services.

The framework of collect, understand, and act has informed public health officials throughout the COVID-19 pandemic. At the time of writing, the pandemic remains ongoing. In certain cases, the processes through which governments analyze and interpret data to inform policy remain opaque.[21] Additionally, insufficient research has been done to effectively gauge the efficacy of many pandemic technologies.[22] Therefore, our analysis in this part of the report attends to how data has been collected during the COVID-19 pandemic and the extent to which such collection efforts were unprecedented compared to prior modes of data collection.

3.1.1 - The Collection Process

Data collection has been essential to combating past health emergencies and is the lifeblood of epidemiological responses to diseases.[23] Public health officials routinely collect large amounts of data to answer research questions [24] and to broadly facilitate and assess public health programs.[25] Traditionally, the collection of this information has been directed by the state. In 1579, for instance, London's Privy Council compiled lists of individuals who had the plague and quarantined them within Europe's first hospitals. However, many of the public health efforts throughout history have been impacted by bias, denials, or outright prejudice regarding the diseases themselves (and the individuals afflicted by them), which have had the effect of inhibiting effective responses.[26] Also, in past pandemics when information was scarce, rumours and conspiracies

21 Ian Sample. (2020). "Secrecy has harmed UK government's response to Covid-19 crisis, says top scientist," *The Guardian*. Available at: https://www.theguardian.com/world/2020/aug/02/secrecy-has-harmed-uk-governments-response-to-covid-19-crisis-says-top-scientist.

22 Jobie Budd, Benjamin S. Miller, Erin M. Manning, Vasileios Lampos, Mengdie Zhuang, Michael Edelstein, Geraint Rees, Vincent C. Emery, Molly M. Stevens, Neil Keegan, Michael J. Short, Deenan Pillay, Ed Manley, Ingemar J. Cox, David Heymann, Anne M. Johnson, and Rachel A. McKendry. (2020). "Digital technologies in the public-health response to COVID-19," *Nature Medicine* 26, 1183-1192.

23 Michael Höhle. (2017). "A statistician's perspective on digital epidemiology," *Life Sciences, Society and Policy* 13.

24 Jane Sutton and Zubin Austin. (2015). "Qualitative Research: Data Collection, Analysis, and Management," *The Canadian Journal of Hospital Pharmacy* 68(3).

25 Y. Holder, M. Peden, E. Krug, J. Lund, G. Gururaj, and O. Kobusingye (eds.). (2001). "Injury Surveillance Guidelines (WHO/NMH/VIP/01.02)," World Health Organization (in collaboration with the United States Centers for Disease Control and Prevention). Available at: https://apps.who.int/iris/handle/10665/42451.

26 Nancy Tomes. (2020)."The Making of a Germ Panic, Then and Now," *American Journal of Public Health* 90(2). As examples, in 1836 Naples, officials restricted the movement of prostitutes and beggars because of the belief that they were unclean and therefore infected with cholera (see: Eugenia Tognotti. (2013). "Lessons from the History of Quarantine, from Plague to Influenza A," *Emerging Infectious Diseases* 19(2)). The outbreak of bubonic plague in South Africa between 1900 and 1904 was used as pretext for the mass relocation of African urban populations by white government officials who viewed black urban settlement as a threat to public health (see: Maynard W. Swanson. (1977). "The Sanitation Syndrome: Bubonic Plague and Urban Native Policy in the Cape Colony, 1900–1909," *Journal of African History* 18(3). See also: Jonathan M. Berman. (2021). "When antivaccine sentiment turned violent: the Montréal Vaccine Riot of 1885," CMAJ 193(14); John Geddes. (2021). "When the plague won: a history of vaccine hesitancy," *Macleans*. Available at: https://www.macleans.ca/society/health/when-the-plague-won-a-history-of-vaccine-hesitancy/; Christopher J. Rutty. (2020). "A Pox on Our Nation," Canada's History. Available at: https://www.canadashistory.ca/explore/science-technology/a-pox-on-our-nation.

circulated amid the public's uncertainty and doubt. At times, these biases were subsequently codified into official policies.[27]

Information Box Three: The Rise of Modern Statistics and Health Policy

Since the mid-nineteenth century, modern statistical methods have let states better inform their health policies with the data at their disposal. During London's cholera outbreak of the 1860s, malignant fumes and smells were wrongly identified as the source of the disease. A surge in corpses and the accumulation of bodies in mass graves around the city formed a kind of lived experience for the inhabitants of London and propagated the belief that rotting corpses were the source of contagion. This false assumption led public health officials to focus on the proper disposal of corpses rather than on the true culprit: contaminated drinking water. During this time, however, physician John Snow upended these false presumptions about the disease's spread by applying statistical methods to make sense of the available data[28] and in doing so, he facilitated the establishment of the methodology for modern epidemiology and strengthened the validity of Germ Theory at the same time.[29] Bias and prejudice in public health persist,[30] but Snow's work served as a blueprint for government officials by revealing ways to more effectively control the spread of disease through isolation, disinfection, contact tracing, and other direct interventions in a data-driven manner.[31]

Over time, governments have recognized and adopted the lessons from past health emergencies, while emphasizing the preeminence of the state in fostering public health.[32]

---

27 Defoe, Daniel. [1722](1969). *A Journal of the Plague Year: Being Observations or Memorials of the Most Remarkable Occurrences, as Well Publick as Private, Which Happened in London during the Last Great Visitation in 1665*. Oxford University Press: New York.

28 Steven Johnson. (2006). *The Ghost Map: The Story of London's Most Terrifying Epidemic--and How It Changed Science, Cities, and the Modern World*. Penguin. P. 15

29 Theodore H. Tulchinsky. (2018). "John Snow, Cholera, the Broad Street Pump; Waterborne Diseases Then and Now," *Cases in Public Health* 77-99.

30 Alan M. Kraut. (2010). "Immigration, Ethnicity, and the Pandemic," *Public Health Reports* 125(3); Natalia Molina. (2011). "Borders, Laborers, and Racialized Medicalization Mexican Immigration and US Public Health Practices in the 20th Century," *American Journal of Public Health* 101(6); Samuel Roberts. (2003)., "'Where our Melanotic Citizens Predominate': Locating African Americans and Finding the 'Lung Block' in Tuberculosis Research in Baltimore, Maryland, 1880–1920," in *CrossRoutes, the Meanings of "Race" for the 21st Century*, edited by Paola Boi and Sabine Broeck.Transaction; Nayan Shah. (1999). "Cleansing Motherhood: Hygiene and the Culture of Domesticity in San Francisco's Chinatown, 1875–1900," in *Gender, Sexuality, and Colonial Modernities*, edited by Antoinette Burton. Routledge; Kevin JA Thomas. (2019). *Global Epidemics, Local Implications: African Immigrants and the Ebola Crisis in Dallas*. Johns Hopkins University Press.

31 Graham Mooney. (2020). "How to Talk About Freedom During a Pandemic," *The Atlantic.* Available at: https://www.theatlantic.com/ideas/archive/2020/05/freedom-pandemic-19th-century/611800/.

32 This emphasis on the role of the state was reflected in the New York Court of Appeal's 1868 statement arguing that the state has, "absolute control over persons and property, so far as the public health

For the United States' Department of Health and Human Services (HHS), the United Kingdom's National Health Service (NHS), and Health Canada, the foundation of their epidemiological investigations in recent history has consisted mostly of data collected or compiled by public health officials about individuals who interacted with the healthcare system.[33] The data collection methods most commonly used were public health surveillance and field teams deployed by public health institutions.[34] These practices relied broadly on the willing participation of persons seeking healthcare and were supplemented by the state's willingness to directly intervene when necessary. In these instances, public institutions served as the primary facilitator and coordinator for public health.[35]

The state's capacity to compel people or organizations to divulge personal health information has changed with each pandemic. While the objectives of maintaining public health and protecting civil liberties have historically been viewed in opposition to one another—also known as the "tragic view of public health"[36]— the past 50 years have seen public health agencies within the United States, United Kingdom, and Canada adopt health surveillance regimes that recognize public health and civil liberties as being complementary to one another.[37] The 1980s simultaneously saw the outbreak of the highly stigmatized disease, HIV/AIDS, and the prominent rise of bioethics in mainstream healthcare provision. Together, these developments led to the emphasis of protecting privacy rights when collecting public health data and have opened the provision of public healthcare to a wider range of stakeholders.[38]

As civil liberties and bioethics began reshaping previous data collection practices, so did the imposition of market disciplines upon public health provision. In the United Kingdom, with human rights and patient autonomy gaining prominence in the country's healthcare services,[39] incremental reforms to the National Health Service blurred the distinction between publicly provided health services and the private medical marketplace. This

was concerned." See: J. F. Witt. (2020). *American Contagions.* Yale University Press. Pg. 82.

33 Steven Johnson. (2020). "How Data Became One of the Most Powerful Tools to Fight an Epidemic," *New York Times.* Available at: https://www.nytimes.com/interactive/2020/06/10/magazine/covid-data.html.

34 Katrina Hedberg and Julie Maher. (2018). "Collecting data," from *The CDC Field Epidemiology Manual.* Centers for Disease Control and Prevention. Available at: https://www.cdc.gov/eis/field-epi-manual/chapters/collecting-data.html.

35 Alethia H. Cook and David B. Cohen. (2008). "Pandemic Disease: A Past and Future Challenge to Governance in the United States," *The Review of Policy Research* 25(5).

36 J. F. Witt. (2020). American Contagions. Yale University Press; Wendy Parmet. (2003). "Book Review: *Public Health Law: Power, Duty, Restraint*, by Lawrence O. Gostin," *Journal of Public Health Policy* 24.

37 J. F. Witt. (2020). *American Contagions*. Yale University Press. P. 95-96.

38 Austin Frakt. (2018). "Reagan, Deregulation and America's Exceptional Rise in Health Care Costs," *New York Times*, Available at: https://www.nytimes.com/2018/06/04/upshot/reagan-deregulation-and-americas-exceptional-rise-in-health-care-costs.html; Ruth Chadwick and Duncan Wilson. (2018). "The Emergence and Development of Bioethics in the Uk," *Medical Law Review* 26(2).

39 Angus H. Ferguson. (2012). "The Evolution of Confidentiality in the United Kingdom and the West," *AMA Journal of Ethics* 14(9).

process of privatization embedded private firms as an essential fixture of public health,[40] and their significance has not diminished in subsequent decades.[41] The result has been the development of pluralistic healthcare systems in the United Kingdom and United States alike, where public health institutions routinely "govern by proxy."[42]

Unlike the United States and United Kingdom, Canada has maintained many of the features of its publicly funded healthcare system,[43] although private stakeholders have increasingly served a supporting role.[44] As private firms have presided over larger shares of individuals' health data, they have been key stakeholders in the response to pandemics. In part due to these reasons, the Canadian public health response to COVID-19 shares similar characteristics with American and British responses.

A detailed examination of the development of healthcare systems is beyond the scope of this report. However, our brief survey captures how the process of data collection for health purposes has developed over time and how the state's power and willingness to compel information has evolved. The results of this evolution include an increasing focus on data, awareness of civil rights and liberties, and the enhanced roles of private stakeholders in enabling or administering aspects of public health policy. In the following sections, we examine the degree to which novel data collection technologies, which were adopted to address COVID-19, fit within these existing public health trends and traditions. Specifically, we discuss how digital technologies were used to collect data to help interrupt community transmission, enable epidemiological surveillance, and facilitate contact tracing. Additionally, we outline the degree to which these technologies were an outgrowth of existing public health methodologies and how they have been driven by private-sector influence in healthcare systems.

3.2 - Cases

Public health surveillance entails the "ongoing systematic collection, analysis, interpretation and dissemination of health data for the planning, implementation and evaluation of public health action."[45] In each of the jurisdictions we assessed, we looked at how they

40 Martin Gorsky. (2008). "The British National Health Service 1948–2008: A Review of the Historiography," *Social History of Medicine*, 21(3).

41 Tom Dehn. (2007). "Private Provision in the UK National Health Service," *Annals of the Royal College of Surgeons of England* 89(4).

42 John J. Dilulio Jr. (2002). "(Response) Government by Proxy: A Faithful Overview," *Harvard Law Review* 116.

43 June E. O'Neill and Dave M. O'Neill. (2007). "(Working Paper 13429) Health Status, Health Care and Inequality: Canada vs. the U.S.," *National Bureau of Economic Research*. Available at: https://www.nber.org/papers/w13429.

44 Michael R. Law, Jillian Kratzer, and Irfan A. Dhalla. (2014). "The increasing inefficiency of private health insurance in Canada," *Canadian Medical Association Journal* 186(12).

45 Bernard C. K. Choi. (2012). "The Past, Present, and Future of Public Health Surveillance," Scientifica 2012.

used digital technologies to interrupt community transmission, undertake digital epidemiological surveillance, and conduct rapid case identification.

Contact tracing involves identifying the individuals that a person, who is infected with a disease, encounters over a period of time (e.g., during the disease's infectious period).[46] Contact tracing is considered to be one of the key methods for interrupting disease transmission and containing disease outbreaks.[47] Governments have established public institutions to facilitate contact tracing in the event of health crises since the rise of germ theory in the 19th century, with these institutions and their corps of field teams undertaking programs of "notification, isolation, disinfection, and case finding."[48] During COVID-19, a number of technologists and public policy experts, often in more affluent nations, supplemented the contact-tracing process by developing digital tools to allow public health officials and the individuals and communities they oversee to more rapidly conduct contact tracing.[49] It is, however, worth recognizing that in less affluent countries or regions where healthcare and associated services are less developed, digital contract tracing, exposure-notification services, and other technological interventions are regarded as less of a supplement to traditional services and more of a primary way of providing services.

Case identification entails analyzing, categorizing, and diagnosing those afflicted with a particular disease[50] and is foundational to providing public health services.[51] Health workers historically have served as an initial point of contact and the primary agents for identifying the spread of disease in a population.[52] During the COVID-19 pandemic, however, state agencies routinely turned to private firms to provide relevant geographical mobility data that could potentially be used to monitor the prospective spread of disease in a population, in their attempt to understand the disease's possible movement in local and international contexts.

---

46 Matt J. Keeling, T. Deirdre Hollingsworth, and Jonathan M. Read. (2020). "Efficacy of contact tracing for the containment of the 2019 novel coronavirus (COVID-19)," *Journal of Epidemiology and Community Health* 74(10).

47 Dyani Lewis. (2020). "Why many countries failed at COVID contact-tracing — but some got it right," *Nature*. Available at: https://www.nature.com/articles/d41586-020-03518-4.

48 Graham Mooney. (2020). "'A Menace to the Public Health' — Contact Tracing and the Limits of Persuasion," *The New England Journal of Medicine* 383(19).

49 Bobbie Johnson. (2020). "The Covid Tracing Tracker: What's happening in coronavirus apps around the world," *MIT Technology Review.* Available at: https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker/.

50 Franz Calvo, Bryant T. Karras, Richard Phillips, Ann Marie Kimball, and Fred Wolf. (2003). "Diagnoses, Syndromes, and Diseases: A Knowledge Representation Problem," *AMIA Annual Symposium Proceedings Archive* 2003.

51 Darlene Berger. (1999). "A brief history of medical diagnosis and the birth of the clinical laboratory. Part 1--Ancient times through the 19th century," MLO: Medical Laboratory Observer 31(7).

52 Jie Qi Lee, Wayren Loke, and Qin Xiang Ng. (2020). "The Role of Family Physicians in a Pandemic: A Blueprint," *Healthcare* (Basel) 8(3).

Health workers historically have also been key to identifying actual, as opposed to prospective, cases of disease. In the Internet era, health workers and public broadcasters alike have been challenged in their abilities to communicate the symptoms associated with diseases like COVID-19. Individuals in highly connected countries are known to regularly use the Internet to self-diagnose their symptoms[53] without necessarily being aware that many of these Internet-accessible sources may be inaccurate or disreputable.[54] To tackle this challenge, digital symptom checkers were developed to help individuals better assess their health status[55] and to inform those affected with COVID-19 of when they should seek medical help.[56]

In each of the following cases, we examine how technologies were used in response to the COVID-19 pandemic. The focus is on the data collected, who authorized the collection, and who could access that data. Subsequently, we discuss the broader implications of the kinds of technologies that were adopted across cases to assess commonalities and differences in the data governance processes in each jurisdiction, as they pertain to the collection technologies examined.

3.2.1 - United States

3.2.1.1 - Interrupting Community Transmission Using Contact-Tracing Applications

The COVID-19 pandemic has seen dozens of countries rely on digital contact-tracing applications that were developed by private companies and contractors.[57] These digitally enabled approaches are ostensibly an outgrowth of traditional contact-tracing practices insofar as they enable the monitoring of individual's locations or contacts with other people.[58] Contact-tracing applications tend to collect geolocation information as well as information about the devices to which an application has been proximate. In contrast, exposure-notification applications typically keep on-device records of the mobile devices an individual has been proximate to and are used to inform an individual if they have been proximate to someone who has subsequently tested positive with COVID-19. Unlike contact-tracing applications, exposure-notification applications tend not to collect detailed geolocation information.

---

53 Hannah L. Semigran, Jeffrey A. Linder, Courtney Gidengil, Ateev Mehrotra. (2015). "Evaluation of symptom checkers for self diagnosis and triage: audit study," *BMJ* 351.

54 Damir Huremović. (2019). "Brief History of Pandemics (Pandemics Throughout History)," Psychiatry of Pandemics 2019.

55 Hannah L. Semigran, Jeffrey A. Linder, Courtney Gidengil, Ateev Mehrotra. (2015). "Evaluation of symptom checkers for self diagnosis and triage: audit study," *BMJ* 351.

56 Nicolas Munsch, Alistair Martin, Stefanie Gruarin, Jama Nateqi, Isselmou Abdarahmane, Rafael Weingartner-Ortner, and Bernhard Knapp. (2020). "Diagnostic Accuracy of Web-Based COVID-19 Symptom Checkers: Comparison Study," *Journal of Medical Internet Research* 22(10).

57 Dyani Lewis. (2021). "Contact-tracing apps help reduce COVID infections, data suggest," *Nature*. Available at: https://www.nature.com/articles/d41586-021-00451-y.

58 Susan Landau. (2021). *People Count: Contact-tracing Apps and Public Health.* Penguin. P 39.

Contact-tracing and exposure-notification applications are enabled by the availability of connected devices, particularly smartphones. In the United States, the decentralized nature of the pandemic response meant that 29 states deployed applications, which were created by nine different third-party developers.[59] Many of these applications used, or were replaced by, the privacy-preserving Google/Apple Exposure Notification (GAEN) system. The GAEN system is an exposure-notification system and does not permit tracking the physical locations of the devices it is installed on,[60] as opposed to a contact-tracing tool.[61] Applications using the GAEN system uses Bluetooth to detect nearby phones and are configured to deliver notifications to smartphone owners if they have been proximate to someone who has not only tested positive for COVID-19 but has also used the application and has consented to sending an alert to individuals with whom they were proximate while likely infected and contagious with COVID-19.[62]

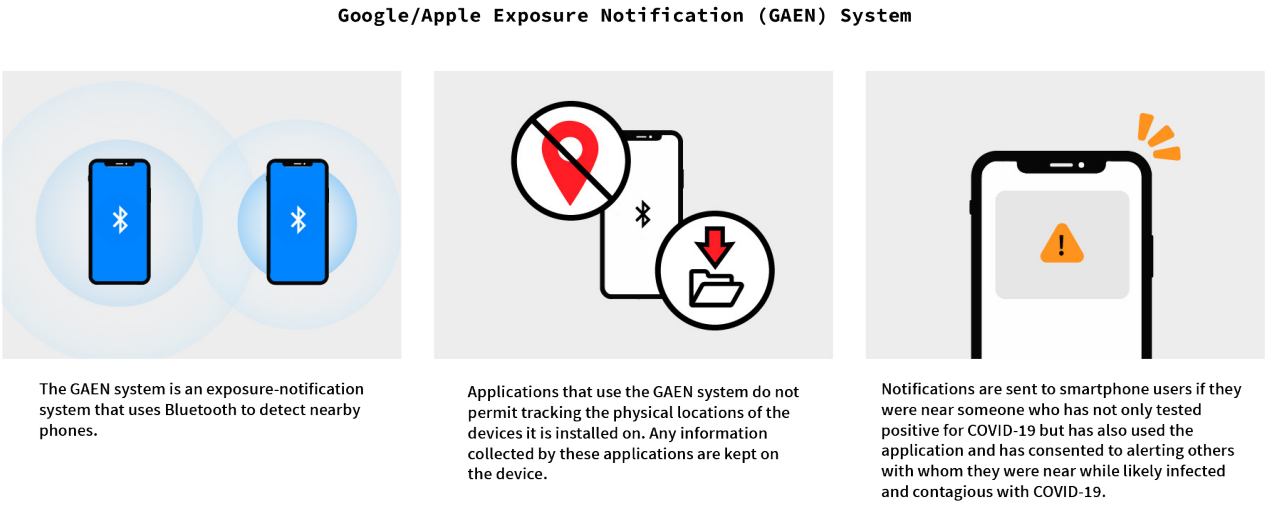


Figure 1: Infographic showing some of the main features of the GAEN system.

3.2.1.2 - Facilitating Digital Epidemiological Surveillance Using Mobile Device Data

Google Mobility Trends was used in the United States to facilitate some traditional epidemiological activities. This Google service uses geolocation data that is generated from users' devices (which are associated with their Google accounts) to assess population-level community mobility.[63] Google has stated that the surveillance was voluntary

59 Mia Sato. (2020). "Contact tracing apps now cover nearly half of America. It's not too late to use one," *MIT Business Review*. Available at: https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/.

60 Dyani Lewis. (2021). "Contact-tracing apps help reduce COVID infections, data suggest," *Nature*. Available at: https://www.nature.com/articles/d41586-021-00451-y.

61 Susan Landau. (2021). *People Count: Contact-tracing Apps and Public Health.* Penguin. P 60.

62 Google. (2020) "Exposure Notifications: Help slow the spread of COVID-19, with one step on your phone," Google. Available at: google.com/covid19/exposurenotifications/#grid-homepage-how-it-works.

63 Silvia Mendolia, Olena Stavrunova, and Oleg Yerokhin. (2021). "Determinants of the Community

and consensual and that the Trends information was aggregated and anonymized to prevent discrimination or intrusions into individuals' privacy.[64] Specifically, Google applied privacy-preserving techniques such as differential privacy[65] and excluded data where there was an insufficient number of users to ensure their relative anonymity could be maintained.[66] As a result, Google undertook regional tracking of the categories of places that individuals travelled to (e.g., retailers, groceries, parks, transit stations, workplaces, and homes) and assessed how travel destinations shifted throughout the pandemic.[67] Individual users of Google's service passively generated the information as they travelled with their mobile devices and frequented businesses, used public transit, or visited residential addresses. Google had collected this information prior to the COVID-19 pandemic and chose to reuse the information after the onset of the pandemic to inform social-distancing efforts.[68]

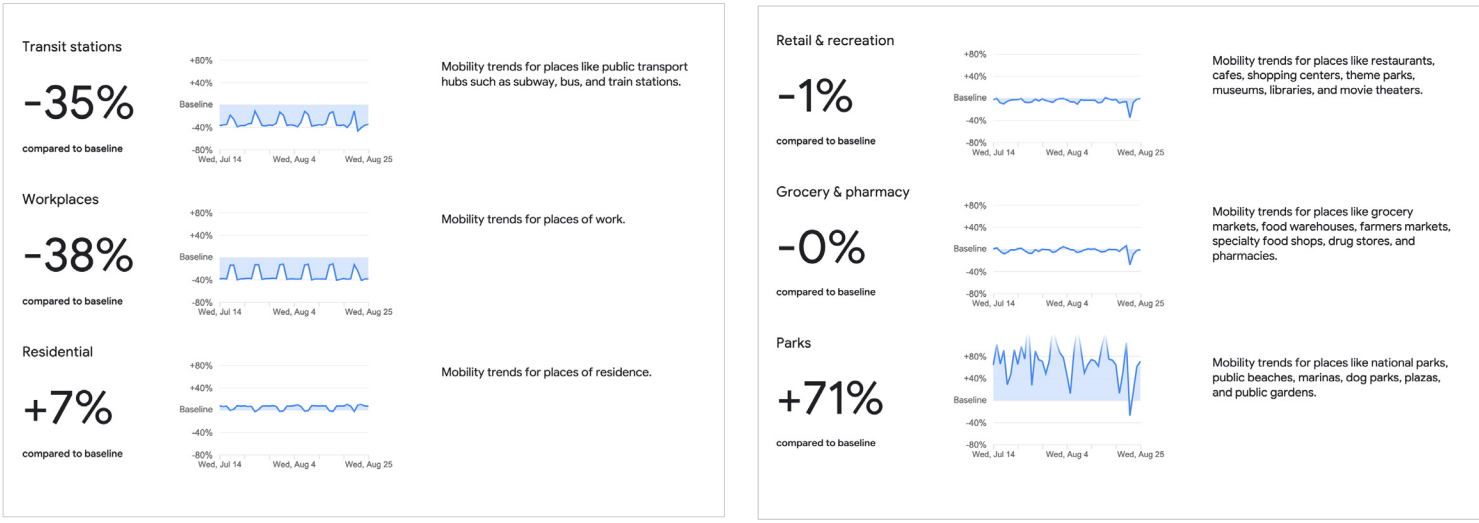


Figure 2: Screengrabs from a Google COVID-19 Community Mobility Report showing mobility data for Massachusetts, US.

Mobility during the COVID-19 Epidemic: The Role of Government Regulations and Information," *Journal of Economic Behavior and Organization* 184.

64 Casey Newton. (2020). "Google uses location data to show which places are complying with stay-at-home orders – and which aren't,"*The Verge*. Available at: https://www.theverge.com/2020/4/3/21206318/google-location-data-mobility-reports-covid-19-privacy. However, while individuals can disable the collection of Location History used to develop these mobility reports, Google has a history of duplicity insofar as disabling Location History has not actually stopped Google from collecting users' history. There is no indication that this mode of surreptitious collection was used in generating mobility reports. For more, see: Ryan Nakashima. (2018). "AP Exclusive: Google tracks your movements, like it or not," *Associated Press*. Available at: https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb.

65 Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert & Rickmer F. Braren. (2020). "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence* 2.

66 Mihály Sulyok and Martin Walker. (2020). "Community movement and COVID-19: a global study using Google's Community Mobility Reports," *Epidemiology and infection* 148.

67 Google. (2021). "United States Mobility changes," Google. Available at: https://www.gstatic.com/covid19/mobility/2021-05-14_US_Mobility_Report_en.pdf.

68 Google. (2021). "United States Mobility changes," Google. Available at: https://www.gstatic.com/covid19/mobility/2021-05-14_US_Mobility_Report_en.pdf.

3.2.1.3 - Enabling Rapid Case Identification Using Distributed Self-Assessment Services

Healthcare institutions and workers had many challenges in diagnosing and treating victims of COVID-19. To reduce resource pressures and stimulate rapid case identification, many countries implemented digital self-assessment tools that let individuals monitor their symptoms. [69] The most widely adopted self-assessment tool in the United States, called the COVID-19 Health Bot, was created by the Center for Disease Control (CDC) and Microsoft. The tool leveraged Microsoft's Healthcare Bot service by enabling individuals to conduct self-assessments without necessarily having to speak with a healthcare provider, thereby alleviating pressures on healthcare workers.[70]

Data was collected from individuals who used this self-assessment tool and self-identified as being potentially infected by COVID-19. These individuals would subsequently input their symptoms into the health 'bot,' named 'Clara.' Clara used a predetermined algorithm in the form of a dialogue with the individual using the tool to assess whether their symptoms were indicative of COVID-19.[71] The individual could then use the results in deciding to pursue further medical assistance. The Application Programming Interface (API) for the CDC's Coronavirus Self-Checker was made publicly available,[72] and the CDC encouraged third parties to embed the tool in their own websites,[73] and some did, including universities[74] and Google.[75]

This rapid case identification system, which leveraged Microsoft Azure's HealthBot[76] to assess user symptoms, was distinct from previous mechanisms of disease surveillance. While the CDC pools data from thousands of healthcare institutions across the country to identify and intervene at epicenters of a given outbreak using its National Syndromic Surveillance Program,[77] the decentralized and privacy-preserving Coronavirus

69 Fatma Mansab, Sohail Bhatti, and Daniel Goyal. (2021). "Performance of national COVID-19 'symptom checkers': a comparative case simulation study," *BMJ Health & Care Informatics* 28.

70 Brandi Vincent. (2020). "CDC Launches COVID-19 Bot to Help You Decide If You Need to See a Doctor," Nextgov. Available at: https://www.nextgov.com/emerging-tech/2020/03/cdc-launches-covid-19-bot-help-you-decide-if-you-need-see-doctor/163975/.

71 Fatma Mansab, Sohail Bhatti, and Daniel Goyal. (2021). "Performance of national COVID-19 'symptom checkers': a comparative case simulation study," *BMJ Health & Care Informatics* 28.

72 Centres for Disease Control and Prevention. (2021). "CDC COVID-19 Health Bot," GitHub. Available at: https://github.com/CDCgov/covid19healthbot.

73 Centres for Disease Control and Prevention. (2021). "Coronavirus Self-Checker," CDC. Available at: https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/coronavirus-self-checker.html.

74 See, for example: MIT Medical. (2021). " FAQ: CDC COVID-19 self-checker," MIT. Available at: https://medical.mit.edu/faqs/faqs-covid-19-self-checker.

75 PYMNTS. (2021). "Google health searches for an identity," PYMNTS.com. Available at: https://www.pymnts.com/healthcare/2021/google-health-searches-for-an-identity/.

76 Microsoft. (n.d.). "Health Bot," Microsoft. Available at:https://azure.microsoft.com/en-us/services/bot-services/health-bot/#overview.

77 Centres for Disease Control and Prevention. (2018). "Surveillance Strategy Report — Syndromic Reporting," CDC. Available at: https://www.cdc.gov/surveillance/initiatives/symptoms-signal.html.

Self-Checker did not transmit data into this surveillance program. The result is that while individuals could make judgments about their own healthcare status, the information that might have been gleaned by the Self-Checker did not assist the CDC's broader health surveillance systems.

3.2.2 - United Kingdom

3.2.2.1 - Interrupting Community Transmission Using Contact-Tracing Applications

The United Kingdom's government began its Test and Trace program in May 2020.[78] This program paired traditional analogue methods that used contact tracers to assess networks of COVID-19 infection with a centralized contact-tracing mobile device application that was meant to provide further insight into the virus' spread. The program was a departure from applications that used the decentralized GAEN system. The centralized nature of the Test and Trace application led to it being critiqued on privacy grounds, and its initial deployment was also plagued by mismanagement.[79] Updates to this initial application were subsequently blocked by Apple and Google,[80] which ultimately led the government to discard its initial centralized application in June 2020 and to replace it with a successor application in September 2020 that used the GAEN system.[81]

The National Health Service's second mobile contact-tracing system was integrated with the NHS's COVID-19 mobile device application, and it used the GAEN system's privacy-preserving and Bluetooth-enabled service. As with other implementations of the GAEN system, the NHS's application collected minimal information about the individual using it. Upon installation, and unlike applications like those deployed in Canada and the United States, however, the NHS application prompted users to enter their postcode so that policymakers could better understand the application's use at a geographical level.[82]

Data collection through the NHS application was decentralized like its counterparts, insofar as devices that the application was proximate to were saved as local records

78 Adam Briggs, Deborah Jenkins, and Caroline Fraser. (2020). "NHS Test and Trace: the journey so far," The Health Foundation. Available at: https://www.health.org.uk/publications/long-reads/nhs-test-and-trace-the-journey-so-far.

79 James Ball. (2020). "The UK's contact tracing app fiasco is a master class in mismanagement," *MIT Technology Review.* Available at: https://www.technologyreview.com/2020/06/19/1004190/uk-covid-contact-tracing-app-fiasco/.

80 Leo Kelion. (2021). "NHS Covid-19 app update blocked for breaking Apple and Google's rules," *BBC.* Available at: https://www.bbc.com/news/technology-56713017.

81 Dyani Lewis. (2021). "Contact-tracing apps help reduce COVID infections, data suggest," *Nature.* Available at: https://www.nature.com/articles/d41586-021-00451-y.

82 Chris Wymant, Luca Ferretti, Daphne Tsallis, Marcos Charalambides, Lucie Abeler-Dörner, David Bonsall, Robert Hinch, Michelle Kendall, Luke Milsom, Matthew Ayres, Chris Holmes, Mark Briers, and Christophe Fraser. (2021). "The epidemiological impact of the NHS COVID-19 app," *Nature* 594.

on mobile devices and geolocation information was not tracked. However, because the GAEN functionality was built into the NHS's COVID-19 application that had other functions, the application also contained other features. For instance, the application included a QR scanning system that let users log which businesses they visited, and it stored that information on the local device. The application would also alert the user if one of those locations was later identified as a hotspot by the NHS. In such situations, the device would examine warnings posted by the NHS and alert users if they had been at the locations during times when exposure was likely.[83]

In using the NHS COVID-19 app, users were responsible for inputting postcode information and tracking geolocation information when they scanned QR codes, and their devices passively collected information when they were proximate to other devices that had the application installed and activated. From September to December of 2020, the application was regularly used by 16.5 million users, which accounted for roughly 28 percent of the population.[84] Ultimately, the information that was collected from devices was limited to postcode information as well as situations in which individuals would upload their COVID-19 positive status. This information was subsequently used by the NHS for either planning purposes or to facilitate decentralized notification processes.

3.2.2.2 - Facilitating Digital Epidemiological Surveillance Using Mobile Device Data

Following the passage of the *Coronavirus Act* of 2020, the UK government received emergency powers that authorized it to request mobility information from telecommunications providers.[85] The hope was that mobile location data could be used to help enforce social-distancing regimes.[86]

Telecommunications providers O2 and EE (BT is the UK mobile operator of EE) were responsible for collecting the mobility information, and it was collected in the course of their subscribers carrying or using their mobile devices. In March 2020, O2 and EE confirmed that they had provided aggregate location data about their mobile phone users to inform the UK government's COVID-19 response.[87]

---

83 Susan Landau. (2021). *People Count: Contact-tracing Apps and Public Health*. Penguin. P. 96.

84 Susan Landau. (2021). *People Count: Contact-tracing Apps and Public Health*. Penguin. P. 96.

85 Department of Health & Social Care. (2020). "Guidance: What the Coronavirus Bill will do," Government of the United Kingdom. Available at: https://www.gov.uk/government/publications/coronavirus-bill-what-it-will-do/what-the-coronavirus-bill-will-do.

86 Privacy International. (2020). "Telecommunications data and Covid-19," Privacy International. Available at: https://privacyinternational.org/examples/telecommunications-data-and-covid-19.

87 Research and Information Service. (2020). "Briefing Paper: The Use Of Digital Measures To Combat COVID-19," Northern Ireland Assembly. Available at: http://www.niassembly.gov.uk/globalassets/documents/raise/publications/2017-2022/2020/health/2320.pdf. P. 26.

Relatively little has been reported about the agreement between the UK government and telecommunications providers, which makes it challenging to ascertain the scope of the data collection, though it is known that the agreement relied on telecommunications data sets, which could theoretically reveal the location of individual phones. NHS, however, stated that it did not seek such granular insights and instead had focused on broader mobility trends.[88] Other telecom providers have said that they were not approached by the government to leverage their stored customer data.[89] Civil society groups criticized the government's collection of data from telecommunications companies and warned of function creep as well as the importance of the proportionality of the data's use in combating COVID-19's spread across the country.[90]

3.2.2.3 - Enabling Rapid Case Identification Using Distributed Self-Assessment Services

The NHS Symptom Checker, like the NHS's mobile contact-tracing system, was hosted within the broader NHS COVID-19 app. The Symptom Checker was implemented following the failure of the NHS's initially deployed contact-tracing application. Individuals could use the NHS Symptom Tracker to monitor the development of health symptoms to assess whether they matched those of the novel coronavirus. The Tracker was application based and lacked a web browser-based equivalent. Those who did not own a device capable of installing the application could use the NHS 111 symptom checker that relied on a conventional phone-based symptom assessment.[91]

Individuals submitted symptom information into the application, which used an embedded algorithm to assess the likelihood of the individual having contracted the virus. If individuals wanted more information, they were directed to the phone call-based NHS 111 symptom checker from within the application.[92]

Whereas the NHS 111 symptom checker recorded information provided by callers, individuals who entered their symptoms into the NHS COVID-19 application symptom checker saw the information hosted and stored on their mobile device.[93] Responses to

88 Alexander Martin. (2020). "Coronavirus: Government using mobile location data to tackle outbreak," *Sky News*. Available at: https://news.sky.com/story/coronavirus-government-using-mobile-location-data-to-tackle-outbreak-11960050.

89 Mark Sweney and Alex Hern. (2020). "Phone location data could be used to help UK coronavirus effort," *The Guardian*. Available at: https://www.theguardian.com/world/2020/mar/19/plan-phone-location-data-assist-uk-coronavirus-effort.

90 Jay Jay. (2020). "Amid COVID-19 outbreak, hackers target UK medical research firm," *teiss*. Available at: https://www.teiss.co.uk/government-telecom-location-data/.

91 National Health Service. (n.d.). "NHS Symptom Checker," NHS. Available at: https://usetherightservice.com/self-care/nhs-symptom-checker/.

92 National Health Service. (n.d.). "When should I enter symptoms into the NHS COVID-19 app?," NHS. Available at: https://faq.covid19.nhs.uk/article/KA-01138/en-us?parentid=CAT-01036&rootid=.

93 Department of Health & Social Care. (2021). "Guidance: NHS COVID-19 app: privacy notice," *Government of the United Kingdom*. Available at: https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice.

the symptom tracker were subsequently reported to the NHS after disassociating the data from the individual and their device.[94] Data was collected through the application and guided by a number of principles that were intended to minimize the collection of user data; the data was captured within the Data Protection Impact Assessment aspect of the application and was published by the UK government.[95]

3.2.3 - Canada

3.2.3.1 - Interrupting Community Transmission Using Contact-Tracing Applications

Canada's COVID Alert application was launched in June 2020. It was initially available only in Ontario,[96] but nine provinces subsequently adopted it, and it had been downloaded approximately 6,600,000 times as of early July 2021.[97] The application was developed in collaboration with Shopify and BlackBerry and used the privacy-preserving GAEN system.[98] Users did not need to submit identifying information to use the app,[99] and if they were diagnosed as having COVID-19, they could receive a one-time key from health providers or public health officials that could then be entered into the application. Upon doing so, other individuals whose phones were proximate to the diagnosed person during a period they were likely contagious were notified of a possible exposure to COVID-19 through their own COVID Alert application.[100]

Very little data was collected by the COVID Alert application as it relied on the GAEN system. The application was assessed by federal and provincial privacy commissioners and provided a minimum of information to Canadian government servers (e.g., Internet

94 Department of Health & Social Care. (2021). "Guidance: NHS COVID-19 app: privacy notice," *Government of the United Kingdom.* Available at: https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice.

95 Department of Health & Social Care. (2020). "Guidance: NHS COVID-19 app: privacy information," *Government of the United Kingdom*. Available at: https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information.

96 Kelsey Johnson. (2020). "Canada launches COVID-19 contact tracing app as restrictions loosen," *Reuters.* Available at: https://www.reuters.com/article/healthcoronavirus-canada/canada-launches-covid-19-contact-tracing-app-as-restrictions-loosen-idUSL2N2F12N6.

97 Canadian Digital Service and Health Canada. (2021). "Download COVID Alert today," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html.

98 Dyani Lewis. (2021). "Contact-tracing apps help reduce COVID infections, data suggest," *Nature.* Available at: https://www.nature.com/articles/d41586-021-00451-y.

99 Canadian Digital Service and Health Canada. (2021). "Download COVID Alert today," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html.

100 COVID-19 Exposure Notification App Advisory Council. (2021). "Interim report on social and economic determinants of app adoption, retention and use," Innovation, Science, and Economic Development Canada (Government of Canada). Available at: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07716.html.

Protocol (IP) address information). Information disclosed to the Canadian government was accessible only to a small handful of government employees and was not intended to be used to monitor or track individuals' use of the application.

3.2.3.2 - Facilitating Digital Epidemiological Surveillance Using AI-Driven Surveillance

BlueDot was founded by University of Toronto researcher Dr. Kamran Khan in the wake of the SARS outbreak and has been used to predict the spread of disease, including the H1N1 influenza pandemic in 2009, ebola transmissions in Guinea, Liberia, and Sierra Leone in 2014,[101] and a cluster of "unusual pneumonia" infections within Wuhan, China in December 2019.[102] In the months since the World Health Organization (WHO) classified this strain of novel coronavirus, Prime Minister Trudeau announced that BlueDot would partner with the Canadian government to assist in its response to COVID-19.[103]

The BlueDot platform employed a natural language processing algorithm to query on a daily basis a database of roughly 10,000 news sources,[104] which included "news reports, blog posts, and many other (non-social-media) sources,"[105] to monitor for indicators that were associated with 150 diseases in 65 languages.[106] These indicators were subsequently assessed against concurrent airline ticketing data to anticipate potential outbreak hotspots.[107] These data points were supplemented by a range of other data sets, including national census data on population density, the global infectious disease alert, real-time climate data, and zoonotic disease data.[108] Together, these data sets enabled BlueDot to alert its clients of potential outbreaks and their associated risk.

---

101 Zaheer Allam. (2020). "The Rise of Machine Intelligence in the COVID-19 Pandemic and Its Impact on Health Policy," *Surveying the Covid-19 Pandemic and its Implications*; Thomas R. Wojda, Pamela L. Valenza, Kristine Cornejo, Thomas McGinley, Sagar C Galwankar, Dhanashree Kelkar, Richard P. Sharpe, Thomas J. Papadimos, and Stanislaw P. Stawicki. (2015). "The Ebola Outbreak of 2014-2015: From Coordinated Multilateral Action to Effective Disease Containment, Vaccine Development, and Beyond," *Journal of Global Infectious Diseases* 7(4).

102 Cory Stieg. (2020). "How this Canadian start-up spotted coronavirus before everyone else knew about it," *CNBC*. Available at: https://www.cnbc.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html.

103 Osler. (2020). "Client Spotlight – Fighting COVID-19 – BlueDot," Osler. Available at: https://www.osler.com/en/client-stories/bluedot.

104 Zaheer Allam, Gourav Dey, and David S. Jones. (2020). "Artificial Intelligence (AI) Provided Early Detection of the Coronavirus (COVID-19) in China and Will Influence Future Urban Health Policy Internationally," (Medical and Healthcare) *AI* 1(2).

105 Jen Ciarochi. (2020). "How COVID-19 and other infectious diseases spread: mathematical modeling," *TripleByte*. Available at: https://triplebyte.com/blog/modeling-infectious-diseases.

106 Wai Chee Dimock. (2021). "Languages in the Time of Corona," *PMLA/Publications of the Modern Language Association of America* 135(5).

107 Srijita Das and Joy Adhikary. (2020). "Role of Artificial Intelligence Techniques in COVID-19 Pandemic," *BKGC Scholars* 1(2).

108 Zaheer Allam, Gourav Dey, and David S. Jones. (2020). "Artificial Intelligence (AI) Provided Early Detection of the Coronavirus (COVID-19) in China and Will Influence Future Urban Health Policy Internationally," (Medical and Healthcare) *AI* 1(2).

3.2.3.3 - Enabling Rapid Case Identification Using Distributed Self-Assessment Services

The Government of Canada's Self-Assessment Tool is the product of a public-private partnership between Thrive Health and Health Canada. It lets users input their symptoms to determine their likelihood of having COVID-19. The tool was integrated within the larger Canada COVID-19 Application, which was separate from the COVID Alert app. The Canada COVID-19 Application operated as a hub for resources related to COVID-19, including regional updates and links for the COVID Alert application, as well as information on hand hygiene, social distancing, gender-based violence,[109] and more.[110] The application visualized statistics on infection rates across Canada's provinces, provided updates from the Government of Canada and local newsrooms, and contained a "Wall of Kindness" where users could publicly record acts of kindness and personal anecdotes.

Data collection involved individuals using either the self-assessment tool or the symptom tracker in the application. The former required users to answer yes or no to a series of questions regarding symptoms, travel, and contact with others. Responses could then be associated with the user's GPS location or postal code, dependent on their consent, and from their answers, the user was given a recommendation ranging from "maintain social distancing" to "call 9-1-1." The results could be downloaded or shared with others, and the user's most recent results were stored on their device.

Through the symptom tracker, users could record their symptoms over time. After choosing whether to disclose their GPS location or postal code, the user could indicate the symptoms they were experiencing from a preset list and record their temperature and the results from their most recent COVID-19 test. Users could also create a daily notification that reminded them to re-enter their symptoms. This information was saved to the device and within the Thrive platform, where it could be accessed in an anonymized and aggregate form by Health Canada.[111]

Individual users were responsible for entering their health information, and if shared with Health Canada, this information could be used by public health officials with other sources in efforts to develop centralized insights into the spread of COVID-19. Metadata

109 In Canada, shelters and transition houses that serve women and children affected by domestic violence have reported an escalation of violence against women during the pandemic, including a dramatic increase in crisis calls. See: Shelter Voices. (2020). "Special Issue: The Impact of Covid-19 on VAW Shelters and Transition Houses," *Shelter Voices*. Available at: http://endvaw.ca/wp-content/uploads/2020/11/Shelter-Voices-2020-2.pdf.

110 Thrive Health. (2021). "Canada COVID-19 App," Thrive Health. Available at: https://welcome.thrive.health/canada-covid19-app.

111 Thrive Health. (2020). "Privacy Notice," Thrive Health. Available at: https://www.thrive.health/privacy-notice?no-nav.

was collected from the application by additional third parties,[112] such as Segment[113] or Amplitude.[114] User's IP address, a set of randomly generated identifiers, and application usage data were sent to these and other private partners. Google Analytics similarly collected app usage data as well as the user's IP address, but here the IP address was masked to protect anonymity.[115]

3.3 - Discussion

These case studies begin to illustrate some of the digital collection processes that were deployed in response to COVID-19, and they suggest that the responses broadly fit within the historical trajectory of state collections of data in the face of a health emergency. While trends exist, they also exhibit unique features that illustrate how COVID-19 and the technologies developed to combat it are affecting how pandemics are mitigated.

When looked at from a historical vantage point, the data used to curb the spread of COVID-19 has been analogous to the data leveraged in previous pandemics. For example, information pertaining to the health of individuals and communities and the spread of disease between those people and groups as well as information on the distribution of assets to protect against and treat the disease, ranging from vaccines to PPE, has long been collected and mobilized in pandemics and other emergency situations. Unlike past health emergencies, however, public health officials were able to draw on a larger and broader pool of data. As our country-cases showcased, data was collected by public and private organizations alike and subsequently made available to public health officials—often in either an aggregated, anonymized, or semi-anonymized formats—to assist them in their health and policy interventions. The sheer volume of data that was collected was particularly apparent with regard to digital epidemiological surveillance, where Google, BlueDot, O2, and EE each leveraged either their own existing data sets or aggregated a range of publicly available data sets to garner insights. In the cases of Google Mobility Trends' and O2/EE's insights, they relied on user-generated data sets that were first created for commerce and subsequently repurposed to support public health initiatives. While repurposing data sets is increasingly common for businesses as they 'pivot' to new business opportunities, the vast repurposing of private data sources to advance government public health initiatives, at the scale witnessed throughout the pandemic, is novel. The specific data-sharing initiatives have been designed to be relatively privacy-protective, based on

112 Thrive Health. (2020). "Privacy Notice," Thrive Health. Available at: https://www.thrive.health/privacy-notice?no-nav.

113 Segment. (2021). "Privacy Policy," Segment. Available at: https://segment.com/legal/privacy/.

114 Amplitude. (2021). "Privacy Notice," Amplitude. Available at: https://amplitude.com/privacy.

115 Thrive Health. (2020). "Privacy Notice," Thrive Health. Available at: https://www.thrive.health/privacy-notice?no-nav.

information that is available to date, though they do indicate the potential for public-private data sharing to advance other, potentially non-health related, future public policy measures (e.g., for migration, law enforcement, or industrial planning policies).

While some of the collected data came from individuals as they actively interacted with public health systems (e.g., using applications made available by government agencies), mobile devices connected to cellular networks became a passive and rich source of data. The use of mobile devices and their applications to collect data, however, was complicated both by civil liberties concerns (as recognized by government agencies), and by restrictions that were put in place by application store operators, namely Apple and Google. Private companies and government agencies alike adopted policies and technologies that were meant to provide aggregated or population-level understandings of mobility data or symptom information while, at the same time, they avoided unduly infringing on individuals' associational or privacy rights. Such decisions were reached to encourage both the uptake of digital collection and to inform specific policy decisions that were focused at regional, as opposed to household, levels.

Private companies such as Apple and Google, however, also have a considerable amount of power over how mobile devices can be used to collect information to combat the pandemic. This power was perhaps best seen in how the United Kingdom was compelled, based on the functionality restrictions that Apple and Google placed upon all COVID-19 applications, to modify the NHS' COVID-19 application it provided to its residents, even though the application had been created by public health agencies to combat the pandemic. The result, in part, was that states could not collect information they may have wanted to because state agencies did not compel the private companies, like Apple and Google, which operated application stores (or developers of mobile devices' operating systems), to comport with the data collection strategies that public health officials believed would best fight the pandemic. While individuals could, in some cases, choose to share limited information with government agencies, their abilities to do so were limited to what was permissible in COVID-19 applications that included contact-tracing or exposure-notification functionalities.

Apple and Google's intentions for limiting population-level health surveillance may have been well-intentioned—designed to prevent states from abusing mobile devices' surveillance capabilities, to prevent state-driven applications from negatively impacting devices' utility, or to place individuals in control over how governments can collect or monitor information that is made available through mobile phone sensors. However, these companies' actions were likely also meant to forestall governments from compelling a variable set of technical requirements into their mobile operating systems while

clearing the way for the companies to invest in systems meant to protect their own employees should the applications be adopted and proven efficacious. Regardless, the limitations imposed by Apple and Google have inhibited states from exercising their own sovereign authorities in their attempts to mitigate the spread of COVID-19, though to date, countries have not sought to exert the fulsomeness of health or emergencies laws to try and force changes in the GAEN framework with which governments have been provided. At the same time, however, it must be recognized that the very capability for governments to design policies around GAEN applications—such as automating exposure-notification processes—constituted an entirely novel mode of (privacy-protective) surveillance that would not have been possible without Apple and Google's efforts. While it is unclear whether increased data collection would have improved states' efforts to prevent the spread of COVID-19, that states to date have been largely precluded from leveraging smartphones for data collection as they saw fit is, arguably, an unprecedented moment in disease response.

Further complicating the relationship between states and private companies has been state agencies' reliance on privately held data sources. All three methods of digital epidemiological surveillance that we surveyed relied on private stakeholders leveraging existing data sets or digital capabilities, which were subsequently used to inform policy responses to the pandemic.[116] The ascendance of the private sector in the healthcare sector is not novel, but it is indicative of an acceleration and a cementing of trends in the privatization of public health that had been developing prior to the COVID-19 pandemic.[117] Companies' significance and influence in future health emergencies may increase given their roles in enabling services, authorizing applications, deploying application programming interfaces, and collecting and analyzing health-related data that may subsequently be utilized by public health officials. In effect, the ascendance of private companies in facilitating responses to health emergencies may, in some situations, either restrict how public agencies can respond to health emergencies or drive states to test their health and emergencies laws such that state agencies become better able to forcibly guide private organizations' activities. For example, officials may need privately held data or services, and thus, public health interventions may either be adjusted to accommodate private companies' interests or concerns, or state agencies might try to compel private organizations to act in conformity with what those agencies want organizations to do. While the circumstances of the current pandemic suggest that there has been a rebalancing between public and private organizations, to the point that private organizations have

116 Shoshana Zuboff. (2019). *The Age of Surveillance Capitalism:The Fight for a Human Future at the New Frontier of Power.* Public Affairs.

117 Anna North. (2021). "What the History of Pandemics Can Teach Us About Resilience," *New York Times.* Available at: https://www.nytimes.com/2021/04/01/health/pandemics-plague-history-resilience.html.

directed many state interventions, this balance could be recast if the limitations that private organizations impose become seen as unduly restrictive of government action. At this point, governments might shift from cooperating with private organizations to compelling them to assist government responses.

3.4 - Conclusion

The COVID-19 pandemic has showcased how digital technologies can be deployed *en masse* to collect information in response to health emergencies. Many of these technologies follow a lineage of past data collection methods, though they can be more broadly distributed and can collect data in an increasingly automated fashion due to the proliferation of mobile devices. Indeed, the transition to using telecommunications infrastructures to collect data, while often repurposing privately collected data for public purposes, demonstrates both the growth in the volume and velocity of available data and how data can be made fungible. Moreover, the ways in which private organizations have restricted the availability of data, regardless of public health officials' decisions on the optimal ways of addressing health emergencies, speaks to an at least temporary rebalancing of power between public and private organizations, though this might be overturned should private activities be ultimately found to have been counterproductive for public health in the current pandemic or in future health emergencies. Ultimately, the role of private companies and their (un)willingness to enable public health responses in the face of global threats highlight potential limits of currently expressed state authority and may indicate domains where states will legislate in the future to reclaim seemingly ceded authorities.

4. Canadian Privacy Law: An Inhibitor of Effective Pandemic Response?

While public health agencies have been constrained by private organizations in the kinds of data they can collect, there have simultaneously been worries that organizations' ability to collect, use, or disclose data were inhibited by restrictions set out in privacy legislation. In this section, we turn from a cross-national comparison to focus on one of the nations in question, Canada, to assess the extent to which Canadian privacy law unreasonably impeded public and private organizations from collecting, processing, and disclosing data to aid in efforts to combat the spread of COVID-19.

We begin by discussing the relationships between federal and provincial privacy laws and the ways they intersect with health laws with an eye to unpacking how Canadian governments can collect, use, and disclose personal information and personal health information. This examination leads to a discussion of the 2003 Severe Acute Respiratory Syndrome (SARS) pandemic, including the perceived and actual challenges that were associated with collecting, using, and disclosing data during that health emergency, and the proposals that were subsequently suggested and adopted. The adopted proposals, which included creating the Public Health Agency of Canada (PHAC) and the application of emergency legislation to the public health context, created key principles that make up Canada's contemporary public health governance frameworks. While these frameworks may permit Canadian governments to collect, use, and disclose information under emergencies laws, as well as under health and privacy legislation, the case study of Canada's "COVID Alert" application underscores the divide between what law permits and what residents of Canada may normatively support.

We conclude by discussing why privacy and health information frameworks have not been the culprit in ineffective information sharing during the COVID-19 health crises. Federal and provincial decision makers have possessed lawful authority to increase information sharing in COVID-19 pandemic, but they have often responded in disconnected and uncoordinated manners. At the same time, opposition to the government's lawful abilities to collect, use, and disclose information as well as to consent-based digital technologies that were meant to mitigate the spread of COVID-19, reveal an ongoing disconnect between the lawfulness of such handling of personal information and Canadians' normative expectations of how their personal information should be handled.

4.1 - The Legislative Web of Privacy Protection

Multiple legislative instruments govern the collection, use, and disclosure of Canadians' personal information. There is federal privacy legislation (and its provincial equivalents)

that governs public and private entities, and there is provincial health legislation that governs personal health information and facilitates the effective provision of health-care. During public health crises, such as the COVID-19 pandemic, debates regularly arise concerning the effectiveness of these privacy protections and whether they unduly restrict information sharing. While some scholars and public health experts believe that governments should have been able to collect more information during the pandemic to better mitigate the transmission of the virus,[118] others have asserted that the government can respond to such emergencies while also providing robust civil liberties protections.[119] Adjudicating between individual privacy rights and collective, public health interests has, as we will see, long been an issue for legislative assemblies and the courts. As this section will outline, Canada's legislative framework provides numerous exceptions and affirmative data-processing powers that can be employed by the government in a public health emergency and, in fact, possesses few safeguards to limit these powers.

4.1.1 - The Emergence of Federal Public and Private Data Protection Legislation and its Operation

The federal *Privacy Act* was introduced in 1983 to regulate how the federal government can collect, use, and disclose personal information and to provide individuals a right of access to such information.[120] It was not until the turn of the millennium that the collection, use, and disclosure of information by the private sector was subjected to federal legislation, as per the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[121] *PIPEDA* was enacted in 2000 and implemented in stages before fully coming into force on January 1, 2004.[122] During this period, private-sector privacy laws were also passed in British Columbia, Alberta, and Quebec to govern provincially regulated corporations.[123] *PIPEDA* remains, as of writing, the governing statute for private sector

118 Amir Attaran and Adam R. Houston. (2020). “Pandemic Data Sharing: How the Canadian Constitution Has Turned into a Suicide Pact,” in *Vulnerable:* The *Law, Policy and Ethics of COVID-19*, University of Ottawa Press. Available at: https://www.canlii.org/en/commentary/doc/2020CanLIIDocs1866#!fragment//BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoBy CgSgBpltTCIBFRQ3AT0otokLC4EbDtyp8BQkAGU8pAELcASgFEAMioBqAQQBy AYRW1SYAEbRS2ONWpA;.

119 Chantal Bernier, Liane Fong and Timothy M Banks. (2015). "Pandemics in a Connected World: Integrating Privacy with Public Health Surveillance," *University of New Brunswick Law Journal* 66, pp. 117-136.

120 See *Privacy Act*, RSC 1985, c P-21. Available at: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html.

121 See *Personal Information Protection and Electronic Documents Act, SC 2000*, c 5. Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

122 Office of the Privacy Commissioner of Canada. (2013). “The Case for Reforming the *Personal Information and Protection of Electronic Documents Act*,” Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/.

123 Office of the Privacy Commissioner of Canada. (2020). “Provincial Laws that May Apply Instead of PIPEDA,” Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/.

organizations that are not governed by substantially similar legislation or that otherwise do not fall under the auspices of *PIPEDA* (e.g., political parties[124]).

PIPEDA is largely inspired by consent-based privacy regimes. That is, private sectors must obtain meaningful consent, subject to exceptions, to collect, use, or disclose personal information from the individual to whom the information belongs.[125] Personal information is broadly defined to include "any factual or subjective information, recorded or not, about an identifiable individual" and can include age, name, ID numbers, income, ethnic origin, blood type, or medical records, and more.[126] *PIPEDA*'s definition of personal information excludes that which was collected under the auspice of the federal *Privacy Act* or that was collected by provincial or territorial governments as well as business contact information, information that an individual has collected, used, or disclosed for exclusively personal purposes, or an organization's use of personal information for journalistic, artistic, or literature purposes.[127] In the common law, determining what constitutes personal information is an interpretive exercise that requires a consideration of competing values of access and privacy.[128] Ultimately, wherever either *PIPEDA* or the common law define personal information, commercial entities must have a reasonable purpose, obtain meaningful consent, and demonstrate the necessity of handling personal information.[129] The concept of meaningful consent does not refer to a single or fixed standard but depends on the sensitivity of the information, the reasonable expectations of privacy possessed by the individual,[130] and the residual risk of significant harm.[131]

---

124 Colin J. Bennett and Robin M. Bayley. (2012). "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis," Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/.

125 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, ss 6.1. Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html; *Privacy Act*, RSC 1985, c P-21, s 5-8. Available at: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html.

126 Office of the Privacy Commissioner of Canada. (2019). "PIPEDA in Brief," Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

127 Office of the Privacy Commissioner of Canada. (2019). "PIPEDA in Brief," *Office of the Privacy Commissioner of Canada*. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

128 *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403; *Gordon v Canada (Minister of Health)*, 2008 FC 258.

129 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Principle 4.3, ss 6.1, ss 5(3). Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

130 The reasonable expectations of the individual refer to whether an ordinary person would be aware that their information would be collected, used or disclosed by the organization in question in light of its purposes. See Office of the Privacy Commissioner. (2018). "Guidelines for Obtaining Meaningful Consent," Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (organizations should, in particular, highlight any purposes that would not be obvious to the individual and/or reasonably expected based on the context); see also *Englander v Telus* (organizations should make a reasonable effort to ensure that the individual is advised for the purposes for which the information will be used); *Turner v Telus* (even if the collection, use, or disclosure is an acceptable condition of service, companies ought to adequately explain these purposes).

131 Office of the Privacy Commissioner. (2002). "Air Canada Allows 1% of Aeroplan Membership to

In contrast to *PIPEDA, the Privacy Act* is less focused on a consent-driven regime. According to it, the majority of the government's data handling is justified and permitted on the basis that the collection, use, or disclosure of personal information directly relates to a government institution's operating program or is consistent with the program's purpose.[132] "Directly related to an operating activity" has been applied in contrasting ways. While the Treasury Board and Office of the Privacy Commissioner have previously assessed "directly related to an operating activity" through determining whether the collection, use, or disclosure is 'demonstrably necessary,' more recently, the Federal Court of Appeal has found that the *Privacy Act* imposes no necessity obligation on government institutions.[133] Accordingly, consent largely plays a role where government agencies wish to act outside of their mandate or to repurpose data that was collected for a different purpose.

Under both the *Privacy Act* and *PIPEDA*, public and private organizations do not always need to obtain meaningful consent before handling personal information. Public and private sector legislation enumerates a range of activities that are exempt from requiring consent, and many of these exceptions arise in the case of public health emergencies.

In *PIPEDA*, the following exceptions to consent can arise:

- if collection is in the interests of the individual and consent cannot be obtained in a timely manner[134]
- if personal information is used in the case of an emergency that threatens the life, health, or security of an individual[135]
- if the disclosure is made to a government institution in certain instances[136] or
- if the disclosure is required by law[137]

"Opt Out" of Information Sharing Practices: PIPEDA Case Summary #2002-42," Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/pipeda-2002-042/; see also *Royal Bank of Canada v Trang*, 2016 SCC 50 (when dealing with financial information not already in the public domain, the degree of sensitivity is high, requiring express consent); but see *Turner v Telus Communications Inc*, 2007 FCA 21 (the use of voice characteristics in creating a voice print does not require express consent as it has been regarded as being on the lower end of the privacy spectrum).

132 *Privacy Act*, RSC 1985, c P-21, s 4, 7(A), 8(2)(a).

133 *Canada (Union of Correctionnel Officers) v Canada (AG)*, 2019 FCA 212 at para 40.

134 *Personal information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(1)(a). Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

135 *Personal information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(2)(b), 7(3)(e). Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

136 *Personal information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(3)(c.1), 7(3)(d)(i).. Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

137 *Personal information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(3)(i). Available at: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

However, even when an exception may apply or when consent has been affirmatively obtained, the collection, use, or disclosure of personal information must still be considered reasonable. To adjudicate reasonableness, organizations are expected to assess their activities against the *Eastmond* factors. Namely, organizations must assess:

- Is the measure demonstrably necessary to meet a specific need?
- Is the measure likely effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?[138]

These questions and their application are taken up in more detail in section 4.5.2 of this report.

Under the *Privacy Act*, government agencies are not required to obtain individuals' consent before collecting, using, or disclosing data as outlined in sections 5, 7, and 8, respectively. Generally, these exceptions arise where:

- Collection, use, or disclosure is authorized by any other Act of Parliament, or any regulation made thereunder that authorizes disclosure;[139]
- A federal institution has entered into an information-sharing agreement (e.g., the Pan-Canadian Public Health Network);[140] or
- In the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from that disclosure.[141]

Each of the noted conditions can be at play in a public health emergency, such as a pandemic. The type of information being collected can span from asking about recent travel, to inquiring about an individual's health or the health of a person with whom the individual is cohabiting, to the health of an individual's children, and to whether an individual employee is working remotely.

4.1.2 - Provincial Health Information Protection Legislation

Canada has a decentralized healthcare system that sees individuals' personal health information collected, used, and disclosed by public and private entities when they interact with the healthcare system. These public and private entities tend to be referred to as Health Information Custodians (HICs) in Canadian health information legislation.

138 *Eastmond v Canadian Pacific Railway*, 2004 FC 852.

139 *Privacy Act*, RSC 1985, c P-21, s 8(2)(b). Available at: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html.

140 *Privacy Act*, RSC 1985, c P-21, s 8(2)(f). Available at: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html.

141 *Privacy Act*, RSC 1985, c P-21, s 8(2)(m). Available at: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html.

HICs must abide by federal privacy legislation, provincial privacy legislation that has been deemed substantially similar to *PIPEDA* with regard to collecting health information during commercial activities, as well as provincial health legislation.[142]

In Ontario, the *Personal Health Information Protection Act* (*PHIPA*) governs the collection, use, and disclosure of personal health information by HICs or by individuals who have custody or control of Ontarians' personal health information.[143]

Information Box Four: Health Information Custodians Under *PHIPA*

Health Information Custodians (HICs) are defined as a person who has custody or control of personal health information as a result of performing the person's or organization's powers or duties. To be an HIC, the person or organization must be described in the enumerated subparagraphs of s 3(1) of *PHIPA*:

- **A health care practitioner or a person who operates a group practice of health care practitioners**
- **A service provider within the meaning of the *Home Care and Community Services Act, 1994* who provides a community service within the meaning of that Act (regardless of whether they are publicly funded)**
- **A person who operates one of the following facilities, programs or services:**
  - **A hospital within the meaning of the *Public Hospitals Act*, a private hospital within the meaning of the *Private Hospitals Act*, a psychiatric facility within the meaning of the *Mental Health Act* or an independent health facility within the meaning of the *Independent Health Facilities Act***
  - **A long-term care home within the meaning of the *Long-Term Care Homes Act, 2007,* a placement co-ordinator described in subsection 40 (1) of that Act, or a care home within the meaning of the *Residential Tenancies Act, 2006***
  - **A retirement home within the meaning of the *Retirement Homes Act, 2010***
  - **A pharmacy within the meaning of the *Drug and Pharmacies Regulation Act***

142 Provinces with substantially similar legislation include New Brunswick, Newfoundland and Labrador, Nova Scotia, and Ontario. For more on this, see Office of the Privacy Commissioner. (2020) "Provincial laws that may apply instead of PIPEDA," Office of the Privacy Commissioner. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/.

143 *Personal Health Information Protection Act*, 2004, SO 2004, c 3, s1.

- A laboratory or a specimen collection centre as defined in section 5 of the *Laboratory and Specimen Collection Centre Licensing Act*
- An ambulance service within the meaning of the *Ambulance Act*
- a home for special care within the meaning of the *Homes for Special Care Act*
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care

- An evaluator within the meaning of the *Health Care Consent Act, 1996* or an assessor within the meaning of the *Substitute Decisions Act, 1992*
- A medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act*
- The Minister, together with the Ministry of the Minister if the context so requires
- Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons

Sections 38-50 of *PHIPA* set out instances where disclosure is allowed, including if the disclosure occurs to prevent the spread of disease and to promote and protect the health of Ontarians and if the custodian has reasonable grounds to believe that the disclosure is necessary to eliminate or reduce serious bodily harm.[144] In the case of a pandemic, these provisions can authorize the disclosure of personal health information. In British Columbia, the *E-Health (Personal Health Information Access and Protection of Privacy) Act* contains similar provisions that enable information sharing in times of a public health crisis,[145] and the Quebec *Public Health Act* allows for the disclosure of information during the state of health emergency.[146]

Information Box Five: The Reasonableness Standard for Public Disclosures of Health Information

Many health disclosure provisions operate using a reasonableness standard, whereby organizations can collect, use, or disclose personal information on

144 *Personal Health Information Protection Act*, 2004, SO 2004, C 3, ss 39(2)(b). Available at: https://www.ontario.ca/laws/statute/04p03; Health Protection and Promotion Act, RSO 1990, c H7, s 2. Available at: https://www.ontario.ca/laws/statute/90h07.

145 See: *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c 38, ss 4(f)(g)(h)(i).

146 See: Public Health Act, SQ, s 123(3). Available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/s-2.2.

the basis that a reasonable person would objectively consider the purpose reasonable in the circumstances and where there is a threat to public health. In *PHIPA* for example, a health information custodian may disclose personal health information about an individual in the following circumstances:

- to the Chief Medical Officer of Health, a medical officer of health, or a public health authority if the disclosure is made for the prevention of the spread of disease and the promotion and protection of the health of the people of Ontario[147]
- to the Chief Medical Officer of Health, a medical officer of health, or a public health authority if the disclosure is made pursuant to the Immunization of School Pupils Act[148]
- to the Ontario Agency for Health Protection and Promotion. Disclosures to such an agency are conditioned on the disclosure being designed to enhance the protection and promotion of the health of Ontarians and to contribute to efforts to reduce health inequities by establishing an agency to provide scientific and technical advice, to support those working across sectors to protect and improve the health of Ontarians, and to carry out and support activities such as population health assessment, public health research, surveillance, epidemiology, planning, and evaluation[149]

Broadly, the disclosures noted above reveal the minimal constraints that *PHIPA*, as an example, places on the circulation of health information, especially in a public health emergency. Furthermore, legislation such as *PHIPA* may prevent individuals from bringing legal action against HICs. In the case of *PHIPA,* health information custodians cannot be sued for activities undertaken in good faith and reasonable in the circumstances.[150] This provision has received limited judicial consideration, thus it is difficult to assess how the Information and Privacy Commissioner of Ontario might interpret it in any specific factual circumstance. However, the text of the immunity provision bears resemblance to the reasonableness provisions, which enable disclosure if the HIC, in good faith, believed that disclosure was reasonable to prevent the spread of disease and protect public health. The immunity provision, then, can arguably be understood to simply reinforce the idea that HICs can disclose information if done for reasonable purposes.

147 *Personal Health Information Protection Act*, 2004, SO 2004, C 3, ss 39(2)(a). Available at: https://www.ontario.ca/laws/statute/04p03; Health Protection and Promotion Act, RSO 1990, c H7, s 2. Available at: https://www.ontario.ca/laws/statute/90h07.

148 *Personal Health Information Protection Act*, 2004, SO 2004, C 3, ss 39(2)(a). Available at: https://www.ontario.ca/laws/statute/04p03; Health Protection and Promotion Act, RSO 1990, c H7, s 2. Available at: https://www.ontario.ca/laws/statute/90h07.

149 *Personal Health Information Protection Act*, *2004*, SO 2004, C 3, ss 39(2)(a.1). Available at: https://www.ontario.ca/laws/statute/04p03; *Ontario Agency for Health Protection and Promotion Act, 2007*, SO 2007 C 10, ss 1. Available at: https://www.ontario.ca/laws/statute/07o10.

150 *Personal Health Information Protection Act*, *2004*, SO 2004, C 3, s 70. Available at: https://www.ontario.ca/laws/statute/04p03; Health Protection and Promotion Act, RSO 1990, c H7, s 2. Available at: https://www.ontario.ca/laws/statute/90h07.

4.2 - Privacy and Health Legislation During SARS

An analysis of the governance of the 2003 SARS outbreak in Canada provides some answers to how privacy legislation has been applied in the health emergencies context, how health and emergencies laws have enabled information sharing to effectuate government pandemic responses.

Canada was significantly affected by SARS and saw 438 suspected cases and 44 deaths.[151] The World Health Organization (WHO) issued a travel ban on the Greater Toronto Area because of the spread of SARS in the city. A National Advisory Committee on SARS and Public Health was established to assess Canada's response to SARS and to recommend changes to public health governance in light of shortcomings. Of the Committee's recommendations, some pertained to the application of privacy legislation and the lack of effective information sharing between federal and provincial governments.

As it pertains to public sector privacy legislation, the report noted that the federal *Privacy Act* provided too little privacy protection to secure personal information in the context of a public health emergency. In particular, the report noted, in reference to the *Privacy Act*:

> The consent provisions are weaker than those envisaged in the new act, and there is no specific test of necessity for the collection, use, or disclosure of personal information. Non-consensual disclosure is permitted "for the purpose for which the information was obtained ...or for use consistent with that purpose," or "for any purpose in accordance with any Act of Parliament or any regulation." Thus, the importance of the objective, the necessity of using identifiable information, and the weighing of the benefits obtained against the damage done to the individual are neither identified nor considered. The Privacy Act does not impose any legal obligation to use those measures which are the least invasive of privacy, such as de-identification, access on a need-to-know basis, etc.[152]

In contrast, and although private sector privacy legislation was just coming into effect at the time, the report stated that:

> To the extent that *PIPEDA* does apply, provisions in the law appear designed to safeguard provider reporting obligations under federal and provincial law. However, *PIPEDA* may still impede surveillance because of its tight restrictions on the non-consensual collection of information.[153]

---

151 Paul Webster. (2020). "Canada and COVID-19: Learning from SARS," *The Lancet* 395:10228, pp 936-937. Available at: https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30670-X/fulltext.

152 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

153 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," *Government of Canada.* Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

The report also took issue with the application of consumer privacy laws without legislators having necessarily paid sufficient attention to the needs of the health sector.[154]

Broadly, the National Advisory Committee on SARS and Public Health found that the failure to provide information to the international community was the result of a lack of information sharing between governments, and this occurred, in part, as a consequence of Canadian-specific constitutional and technological realities.[155] Canada has a decentralized healthcare system where health is not constitutionally assigned to either federal or provincial jurisdiction within sections 91 and 92 of the *Constitution*.[156] As a result, which level of government is responsible for which particular element of healthcare is context-specific, and this has historically led to coordination problems between federal and provincial governments, including during the SARS pandemic.[157] Legal and institutional protectionism on the parts of government agencies, in effect, has long played a significant role in explaining information-sharing dynamics between governments in Canada, as opposed to privacy-related issues. The committee's report makes clear that data sharing had to occur more freely in the future between provincial and federal health authorities to overcome the identified deficiencies,[158] and it specifically noted that the absence of appropriate and shared databases interfered with outbreak investigation and

---

As discussed in this report's section 4.3.1, this early critique was for naught. Section 7(1)(a) in *PIPEDA* was intended to apply in a health scenario such as SARS and would allow (at least) commercial entities to collect information where it "is clearly in the interests of the individual." Section 7(2)b), similarly, allows for that data's use, "in respect of an emergency."

154 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

155 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

156 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

157 Katherine Fierlbeck and Lorian Hardcastle. "Have the Post-SARS Reforms Prepared Us for Covid-19? Mapping the Institutional Landscape," in *Vulnerable: The Law, Policy and Ethics of COVID-19*, University of Ottawa Press. Available at: https://www.canlii.org/en/commentary/doc/2020CanLIIDocs1866#!fragment//BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoByCgSgBpltTCIBFRQ3AT0otokLC4EbDtyp8BQkAGU8pAELcASgFEAMioBqAQQByAYRW1SYAEbRS2ONWpA.

158 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

management while simultaneously constraining epidemiological and clinical research into SARS.[159]

The committee's critique of public-sector privacy legislation rings true today as many commentators have called on the government to insert overarching necessity and proportionality obligations into the *Privacy Act*, a subject of reform efforts today. Conversely, the committee's critique of private sector privacy legislation was arguably coloured by the lack of jurisprudential application or interpretation of the newly enacted federal privacy legislation. At the time, there was limited understanding of how *PIPEDA* applied to the health sector, and when the report was written, most provinces aside from Quebec had not established their own legislation to govern personal health information. At no point did the report indicate that the Quebec commercial privacy legislation would specifically impede health emergency responses. Ontario's *PHIPA*, as an example, was implemented in May 2004 following the SARS outbreak.[160] These provincial legislative frameworks were intended to address the needs of the health sector and alleviate concerns pertaining to proactive information sharing that were raised in the report.

Overall, though the application of privacy protective legislation was noted by the report's authors as a potential issue in responding to future health crises, they recognized that the key problem during the SARS pandemic was the lack of shared databases and coordination between federal and provincial health agencies.[161] Privacy rights were raised as a prospective, as opposed to an actual, hindrance. These concerns were addressed through provincial health legislation that was passed into law following the SARS outbreak as well as through efforts to more generally better govern health information.

4.3 - Post-SARS Efforts to Better Govern Health Information

The National Advisory Committee on SARS and Public Health report assessed five proposals that were intended to enhance communication between and across government bodies.

159 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

160 See: *Personal Health Information Protection Act, 2004*, SO 2004, C 3. Available at: https://www.ontario.ca/laws/statute/04p03.

161 Health Canada. (2003). "Chapter 9: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

Proposals that paralleled American efforts to securitize health issues,[162] discussed in section 4.3.1, were ultimately rejected in favour of the adopted proposal concerning the use of emergency legislation and preventative monitoring, which are discussed in section 4.3.2.

4.3.1 - Rejected Proposals

Health Canada began to draft a *Food and Drugs Act* in 1998 to address "shortcomings in Health Canada's legislative basis for health protection"[163] and conducted consultations on legislative proposals in 2003.[164] The draft *Canadian Health Protection Act* (*CHPA*) would have repealed and replaced four statutes: the *Food and Drugs Act*, the *Hazardous Products Act*, the *Quarantine Act,* and the *Radiation Emitting Devices Act,*[165] and the *Learning from SARS* report advocated its adoption.

The *CHPA* included procedures to deal with communicable diseases associated with persons entering and exiting Canada and established a national framework for coordinated public-health-related surveillance.[166] The *Act* also would have established national health surveillance by creating national databases for infectious disease surveillance and implementing timeline and reporting procedures.[167] However, the *Canada Health Protection Act* did not pass into law and, as such, the proposed changes to federal private and public sector regulation did not take effect.

---

162 Alexander Kelle. (2007). "Securitization of International Public Health: Implications for Global Governance and the Biological Weapons Prohibition Regime," *Global Governance* 13(2), pp. 217-235; David P. Fidler. (2007). "Governing Catastrophes: Security, Health and Humanitarian Assistance," *International Review of the Red Cross* 89.

163 Health Canada. (2006-2007). *Report on Plans and Priorities*, p. 24.

164 Health Canada. (2006). "Blueprint for Renewal: Transforming Canada's Approach to Regulating Health Products and Food," Government of Canada. Cited by Marlisa Tiedemann. (2008). "LS-602E-Bill C-51: An Act To Amend The Food And Drugs Act And To Make Consequential Amendments To Other Acts," Library of Parliament. Available at: https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/39-2/c51-e.pdf.

165 Health Canada. (2003). "Chapter 9C.1: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

166 Health Canada. (2003). "Chapter 9C.1: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

167 Health Canada. (2003). "Chapter 9C.1: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

The *Learning from SARS* report also assessed whether it would be viable to adopt the Center for Disease Control's Model State Emergency Health Powers Act (i.e., the CDC Model Act). In the CDC Model Act, reporting obligations were triggered when a health-care provider, pharmacist, or vet suspected a biological threat and required the patient's name, date of birth, sex, race, occupation, current work and home addresses, names of health-care providers, and any other information needed to locate the patient for follow-up.[168] The Canadian advisory committee found that provincial health legislation contained reporting obligations that paralleled those in the CDC Model Act. Any differences were attributed to the "emergent focus" of the Model Act.[169] Accordingly, while they assessed the CDC Model Act, the advisory committee ultimately found that it was not necessary to adopt the model in Canada.

Information Box Six: The CDC Model Act

The CDC Model Act, drafted by Professor Larry Gostin, the Co-Director of the Center for Law and the Public's Health at both Georgetown and John Hopkins Universities, was draft model legislation to increase state powers to respond to bioterrorism or other outbreaks of disease in response to the terrorist attacks on September 11, 2001. The CDC's Model Act contained provisions regarding reporting obligations, tracking, information sharing, and access to and disclosure of health information. By December 2001, the Act was released to state legislatures for review and approval and was passed in various iterations in 40 states by August 2011.

The collection of personal health information imagined in the *CHPA* and the reporting requirements outlined in the CDC Model Act could have required changes to legislation governing personal information and its subset, personal health information. In the *Learning from SARS* report, the Committee also noted that a national system of health surveillance would require collecting vast amounts of personal information and could thus potentially collide with both public- and private-sector privacy legislation.[170] As it

168 The Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities. (2001). "The Model State Emergency Health Powers Act: A Draft for Discussion," Centers for Disease Control and Prevention. Available at: https://stacks.cdc.gov/view/cdc/6562.

169 Health Canada. (2003). "Chapter 9C.2: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

170 Health Canada. (2003). "Chapter 9D.3: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-

pertains to public-sector privacy legislation, the *CHPA* would have addressed concerns regarding the lack of necessity and proportionality obligations in the *Privacy Act* by adding these safeguards. As well, *PIPEDA* was said to potentially impede surveillance due to its tight restrictions on the non-consensual collection of information, particularly as it pertained to the transfer of personal health information. These concerns, however, were ultimately for naught as section 7 of *PIPEDA* includes exceptions to consent that can apply to the disease surveillance context, and the health legislation enacted by the provinces provided legislative frameworks to govern the intra-national sharing of personal health information; particular attention was paid to the concerns raised by the health sector and the Committee's report. As a result, the specific concerns raised in the report pertaining to private-sector privacy law were largely rejected by the federal and provincial governments, and health legislation was designed to provide greater certainty of how and under what conditions personal health information could be collected, used, or disclosed in the context of health emergencies.

4.3.2 - Adopted Proposals

The authors of the *Learning from SARS* report recommended that the Canadian government enhance how information was collected and shared to better inform and enable the government to respond to health emergencies. In 2004, the Canadian government created the Public Health Agency of Canada (PHAC). PHAC was established as a monitoring body that was tasked with preventing disease and injuries, responding to public health threats, promoting good physical and mental health, and providing information to support informed decision making.[171] Under PHAC's extensive mandate and given that the *Privacy Act* is highly permissive in enabling government organizations to collect, use, and disclose personal information when doing so is directly related to one of the organization's operational activities, almost any collection of personal information in a pandemic situation would relate directly to PHAC's public health mandate. In 2006, the *Public Health Agency of Canada Act* (*PHACA*) came into force and provided the legislative basis for the monitoring body. *PHACA* allows the minister to establish any public health collection program through regulations.[172] This organizational mandate for PHAC and new regulation-making power for the minister collectively create a powerful data-collection capability at the federal level with few explicit safeguards.

The *Learning from SARS'* authors noted that information collection, use, and disclosure constituted a significant issue that arose during the SARS outbreak, and these issues were

renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

171 See: Public Health Agency of Canada. "About the Public Health Agency of Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/corporate/mandate/about-agency.html.

172 *Public Health Agency of Canada Act,* SC 2006, c 5, Section 15.

taken up by Canadian governments following SARS. In particular, the report assessed a proposal raised by the Canadian Medical Association for a *Health Emergencies Act* to be adopted, which would provide graded increases in federal responsibility and jurisdiction based on the scale of the emergency with provincial and territorial consultation at every stage.[173] The report advocated for the adoption of the *Health Emergencies Act* in light of its harmonization of provincial and federal emergencies legislation. While the *Health Emergencies Act* was rejected, updates were made to emergency legislation in Ontario and more inclusive interpretations of emergency and health legislation emerged in Quebec and British Columbia.

In Ontario, provincial emergencies powers were first established with the 1983 *Emergency Plans Act*. Though the legislation did not contemplate public health crises, amendments in 1999 did expand the definition of emergency to include "impending situations."[174] The *Emergency Plans Act* was repealed in 2002 following its replacement by the *Emergency Management Act (EMA*). The *EMA* was in force during the SARS crisis, but its powers were not exercised. The failures during the SARS crisis were, however, used to demonstrate the need for emergency legislation in the face of a health-related emergency. As a result, the *EMA* underwent review that culminated in the *Emergency Management and Civil Protection Act* (*EMCPA*) in 2006.[175] The *EMCPA* amended the definition of "emergency" to include, "a situation or an impending situation [...] that is caused by [...] a disease or other health risk."[176] This marked the first instance where public health emergencies were explicitly contemplated in Ontario emergency legislation[177] and the amended *Act* remains in force as of writing and has been used by the Ontario government throughout the COVID-19 pandemic.

Though British Columbia and Quebec's emergency legislation has not undergone similar explicit changes as in Ontario, emergency legislation in those provinces has been understood to apply to public health crises and, thus, required no legislative changes

173 Health Canada. (2003). "Chapter 9E: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

174 Health Canada. (2003). "Chapter 9E: Learning from SARS: Renewal of public health in Canada – Some legal and ethical issues raised by SARS and infectious diseases in Canada," Government of Canada. Available at: https://www.canada.ca/en/public-health/services/reports-publications/learning-sars-renewal-public-health-canada/chapter-9-some-legal-ethical-issues-raised-sars-infectious-diseases-canada.html.

175 See: *Emergency Management and Civil Protection Act*, RSO 1990, c E9. Available at: https://www.ontario.ca/laws/statute/90e09.

176 *Emergency Management and Civil Protection Act*, RSO 1990, c E9, s 1. Available at: https://www.ontario.ca/laws/statute/90e09.

177 Eric S. Block and Adam Goldenberg. (2020). "COVID-19: Can They Do That? Part II: The Emergencies Act," McCarthy Tétrault. Available at: https://www.mccarthy.ca/en/insights/articles/covid-19-can-they-do-part-ii-emergencies-act.

post-SARS. In British Columbia, the *Emergency Programs Act* can be invoked if the provincial government is "satisfied that an emergency exists or is imminent."[178] The broad language recognizes that health crises can be treated as an emergency under the *Act*. In contrast, the province of Quebec specifically contemplates public health emergencies in public health legislation. The *Public Health Act* enables Quebec to declare a state of health emergency, without delay and without formality, to protect the health of the population.[179] The federal government, too, has emergency legislation, the *Emergencies Act*, which enables expanded powers and limited judicial review when a public welfare emergency is proclaimed under s 6(1).[180] However, such an emergency is permitted only where the use of existing statutes and the provincial response is inadequate, setting a high threshold for its use, and even when that threshold has been met, the *Emergencies Act* lacks an explicit provision to collect data in a public welfare emergency.[181] As of writing, the federal government has declined to use its emergency powers during the COVID-19 pandemic.

The inclusion of public health emergencies to emergencies legislation can have effects on information sharing during health crises, though not all such legislation applies in precisely the same way. Under Ontario's *EMCPA*, provincial decision makers can make orders that require that "any person collect, use or disclose information that in the opinion of the [Cabinet] may be necessary in order to prevent, respond to or alleviate the effects of the emergency."[182] Such information will be "subject to any law with respect to the privacy and confidentiality of personal information" – but only, "when the declared

178 *Emergency Programs Act*, RSBC 1996, c 111, s 9. Available at: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96111_01.

179 *Public Health Act*, SQ, s 123. Available at: http://legisquebec.gouv.qc.ca/en/showdoc/cs/s-2.2.

180 *Emergencies Act*, RSC 1985, c 22 (4th Supp), ss 6(1): when the Governor in Council believes, on reasonable grounds, that a public welfare emergency exists and necessitates the taking of special temporary measures for dealing with the emergency, the Governor in Council, after such consultation as is required by section 14, may, by proclamation, so declare.

181 While it is possible that section 8(1)(d) of the *Emergencies Act* could authorize data collection, this is not self-apparent upon reading the legislation. Specifically, it reads:

> "8 (1) While a declaration of a public welfare emergency is in effect, the Governor in Council may make such orders or regulations with respect to the following matters as the Governor in Council believes, on reasonable grounds, are necessary for dealing with the emergency … (d) the authorization of or direction to any person, or any person of a class of persons, to render essential services of a type that that person, or a person of that class, is competent to provide and the provision of reasonable compensation in respect of services so rendered".

We refrain from making a strong argument in favour of or opposed to a reading of this section of the *Emergencies Act* to enable data collection but, instead, simply raise that this is an area of legislation that could be clarified in future legislative reform.

182 *Emergency Management and Civil Protection Act*, RSO 1990, c E9, ss 7.0.4(4)13. Available at: https://www.ontario.ca/laws/statute/90e09.

emergency is terminated."[183] The Quebec *Public Health Act* imposes a prescriptive legal standard that must be met prior to the authorization of information sharing.[184] In British Columbia, in contrast, section 10.1(3) of the *Emergency Program Act* requires that the Minister's regulations are "proportionate" to the objectives, while simultaneously empowering the Minister to "do all acts and implement all procedures that the minister considers necessary to prevent, respond to or alleviate the effects of an emergency or a disaster."[185] In aggregate, while there are different requirements that provincial and federal Ministers and organizations must meet to collect, use, and disclose personal information in the midst of a health emergency, the conditions for such activities are extremely permissive and do relatively little to establish controls or restrictions on how governments may handle information in such situations.

4.4 - The COVID-19 Pandemic and the Case of COVID Alert

Between the 2003 SARS outbreak and the COVID-19 pandemic, the federal government and several provinces updated their respective legislation to enable governments to lawfully overcome hurdles to information sharing in a public health crisis. Overall, government agencies were empowered to better coordinate information sharing between federal and provincial governments and were authorized to share certain types of information to combat health emergencies, so long as such sharing was reasonable. The *PHAC Act* cast PHAC as responsible for proactive and reactive pandemic management and enabled PHAC to robustly share information. Additionally, emergency legislation generally authorized governments to collect, use, or disclose information in emergencies with few restrictions under their respective legislation. In aggregate, these permissions were intended to empower governments to respond to pandemics or other crises without running afoul of the concerns raised post-SARS on how privacy legislation could potentially inhibit state responses to public health emergencies.

Perhaps the most controversial or, at least, the most publicly-debated public health surveillance measure in Canada at the onset of the COVID-19 pandemic was the creation, adoption, and use of the COVID Alert application, which relied on the Google Apple Exposure Application (GAEN) framework. Such applications, in Canada as well as in other jurisdictions, generally were initially heralded as a novel way of combating the spread of COVID-19, but public commentary during their development and release regularly

183 *Emergency Management and Civil Protection Act*, RSO 1990, c E9, ss 7.0.2(7)2. Available at: https://www.ontario.ca/laws/statute/90e09.

184 Under section 133 of the Public Health Act, SQ, an organization must possess "reasonable grounds to believe that disclosure of confidential information would protect the health of the population".

185 *Emergency Programs Act*, RSBC 1996, c 111, ss 10.1. Available at: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96111_01.

raised concerns of whether they overly enabled government surveillance or if, in contrast, federal and provincial privacy legislation unduly inhibited the application's full health surveillance potentials.

The privacy and civil liberty implications of government-sponsored contact-tracing applications have been explored by many Canadian experts. The Office of the Privacy Commissioner of Canada (OPC) conducted a review of the COVID Alert application and found that the risk of re-identification was low given the use of decentralized technologies.[186] The Office noted that it was important to assess the effectiveness of the application should low adoption rates limit its value. Specifically, low adoption rates and the corresponding limited benefits to Canadians might necessitate a reconsideration of whether the collection of information was proportionate to the value of the application to public health.[187] The OPC also stated that the application should remain voluntary with a purpose that was limited to exposure notification.[188]

Other experts have considered the countervailing civil liberties at play in assessing COVID Alert. Austin et al. noted the importance of contact tracing to quell disease given the impact that self-isolation can have on individual security rights, citing individuals living in abusive relationships and those suffering from mental health challenges as examples.[189] Under Austin et al.'s analysis, if digital contact tracing was as effective as it had been optimistically presented as being, the assessment of rights should not be limited to privacy rights alone but rather, inclusive of section 7 rights to life, liberty, and security of the person.[190]

---

186 Office of the Privacy Commissioner of Canada. (2020). "Privacy review of the COVID Alert exposure notification application," Office of the Privacy Commissioner of Canada. Available at: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/rev_covid-app/. See also: Public Health Agency of Canada Privacy Management Division. (2021). "COVID Alert: COVID-19 Exposure Notification Application Privacy Assessment," Health Canada. Available at: https://github.com/cds-snc/covid-alert-documentation/blob/main/COVIDAlertPrivacyAssessment.md; Office of the Privacy Commissioner of Canada. (2020). "Supporting Public Health, Building Public Trust: Privacy Principles for Contact Tracing and Similar Apps -- Joint Statement by Federal, Provincial and Territorial Privacy Commissioners," *Office of the Privacy Commissioner of Canada.* Available at: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

187 Office of the Privacy Commissioner of Canada. (2020). "Supporting Public Health, Building Public Trust: Privacy Principles for Contact Tracing and Similar Apps -- Joint Statement by Federal, Provincial and Territorial Privacy Commissioners," Office of the Privacy Commissioner of Canada. Available at: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

188 Office of the Privacy Commissioner of Canada. (2020). "Supporting Public Health, Building Public Trust: Privacy Principles for Contact Tracing and Similar Apps -- Joint Statement by Federal, Provincial and Territorial Privacy Commissioners," Office of the Privacy Commissioner of Canada. Available at: https://priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/.

189 François Tanguay-Renaud, Lisa M. Austin, Vincent Chiao, Beth Coleman, David Lie, Martha Shaffer and Andrea Slane. (2020). "Test, Trace, and Isolate: Covid-19 and the Canadian Constitution," Osgoode Legal Studies Research Paper 2797. Available at: https://digitalcommons.osgoode.yorku.ca/scholarly_works/2797.

190 François Tanguay-Renaud, Lisa M. Austin, Vincent Chiao, Beth Coleman, David Lie, Martha Shaffer and Andrea Slane. (2020). "Test, Trace, and Isolate: Covid-19 and the Canadian Constitution," Osgoode

Recognizing that other rights were engaged, Parsons, in "Contact tracing must not compound historical discrimination," noted that exposure-notification and contract-tracing applications had to be carefully adopted by non-governmental and governmental actors alike so as to avoid the application turning into a novel way of discriminating against the less privileged in society.[191] There were risks specifically associated with these applications amplifying the 'digital divide' in society on the basis that more affluent members of society could install the application whereas others, who might not have access to smartphones for themselves and their family members, could not install the application. There was also a divide between elderly residents of Canada who may not have access to a contemporary smartphone versus younger members of society who do. Moreover, the Canadian exposure-notification application was available only in English and French languages, making it more challenging for non-native English- or French-speaking residents of Canada to understand the application, configure it, or see how it would work.[192] Furthermore, Parsons argued that the reasonableness and proportionality of data collection and disclosure might be outweighed should significant function creep take place. Similarly, staff at the Canadian Civil Liberties Association undertook a public debate about the application and provided their assessments of whether the aims of the applications were reasonable and proportionate and whether deleterious social consequences might arise as it was used by Canadians.[193]

There is at least some indication that digital contract-tracing and exposure-notification applications have not been as effective as initially envisioned. The Digital Global Health & Humanitarianism (DGHH) Lab assessed the uptake and user engagement with contact-tracing applications in a variety of different countries.[194] The DGHH Lab found that individual-, community-, and system-level factors influenced the uptake of these applications and included the following: perceptions of data collection and management; sense

Legal Studies Research Paper 2797. Available at: https://digitalcommons.osgoode.yorku.ca/scholarly_works/2797.

191 Christopher Parsons. (2020). "Contact tracing must not compound historical discrimination," *Policy Options*, Available at: https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/ and Christopher Parsons. (2020). "Equity, inclusion and Canada's COVID Alert app," *First Policy Response*. Available at: https://policyresponse.ca/equity-inclusion-and-canadas-covid-alert-app/.

192 Ross Andersen. (2021). "Majority of Canadians not using COVID Alert app, study finds," *CTV News*. Available at: https://www.ctvnews.ca/health/coronavirus/majority-of-canadians-not-using-covid-alert-app-study-finds-1.5382744.

193 Noa Mendelsohn, Michael Bryant, and Brenda McPhail. (2020). "Contact Tracing App in Canada: To Download or Not," Canadian Civil Liberties Association. Available at: https://ccla.org/contact-tracing-app/.

194 Jennie Phillips, Petra Molnar, Rebecca Babcock, Tiana Putric, Dyllan Goldstein, Laksmiina Balasubsramaniam, Alisha Gauhar, Sarah Quayyum. (2021). *Exploring User-Uptake of Digital Contact Tracing Apps - A Practitioner Guide.* York University. Available at: https://figshare.com/articles/book/Exploring_User-Uptake_of_Digital_Contact_Tracing_Apps_-_A_Practitioner_Guide_-_Full/14423861.

of community; communications and misinformation; accessibility and inclusion; trust in public/private institutions; policy and governance; response infrastructure; and digital capability. The Lab also attributed the poor uptake of digital contact-tracing applications to five major challenges, three of which speak to the privacy perceptions of individual citizens, including:

- fears of immediate and future surveillance
- privacy perceptions may override privacy-by-design principles
- poor perceptions of app effectiveness

As of early July 2021, the COVID Alert application had been downloaded approximately 6,500,000 times and slightly less than 34,000 one-time keys had been used. During the same time, there had been approximately 1.4 million reported cases of COVID-19 in the Canadian population, which meant that notifications were delivered in approximately 2.4% of cases. Notably, downloading the application was not correlated with having activated the application nor with individuals *keeping* the application installed after they had downloaded and activated it. The application was also unavailable for download onto older smartphones at its inception, and updates to operating systems sometimes disabled its functionality. Finally, in excess of the trust metrics associated with the government-sanctioned applications, the parameters of the GAEN protocol trigger only after spending 15 minutes within two meters of someone who has been registered as infected with COVID-19. Neither the time nor distance, as of writing, were clear determinants of whether someone had likely been exposed as infections could occur in less time and over greater distances due to the aerosolized nature of the virus. These limitations suggest that underreporting of contacts are, at least in part, linked to efficacy of the technology.

4.5 - Discussion

Successive public health emergencies have raised concerns that the protection of privacy rights unduly impedes information sharing or, alternately, that privacy rights are inappropriately infringed upon due to increased sharing that occurs amid public health crises. This section assesses these positions and finds in section 4.5.1 that privacy rights have not, in fact, unduly inhibited information sharing. At the same time, section 4.5.2 raises questions about whether and to what extent novel technologies that rely on mass voluntary and consensual adoption of technologies are likely to pass the *Eastmond* test where the specific goals of a technology are not clearly declared prior to or at the moment of its deployment. Finally, section 4.5.3 outlines how a disconnect can arise between lawful collection, use, and disclosure of personal information and individuals' normative expectations of privacy and the challenges that such a disconnect can generate.

4.5.1 - Privacy Protection Frameworks Do Not Unduly Prevent Information Sharing

The critique that privacy laws unduly prevent information sharing arise from perceptions of why health emergencies were, and are, poorly handled. In the case of SARS, the failure by the federal government to adequately share information with the WHO led to Canada being criticized for its information-sharing practices. These issues resulted from poor coordination between federal and provincial governments in a decentralized federal system, as opposed to restrictions on the sharing of personal information as a result of federal or provincial privacy legislation.

One of the adopted proposals after SARS to better coordinate pandemic response, PHAC, came under scrutiny given its response to COVID-19. In her audit of PHAC after the spread of COVID-19 to Canada, Auditor General Karen Hogan concluded that although PHAC took steps to address problems that arose in the pandemic, it needed to improve upon its data-sharing agreements and information technology infrastructure to better support national disease surveillance in the future.[195] Hogan found that PHAC failed to live up to its mandate by not issuing early warnings, adequately surveying COVID-19 abroad, conducting risk assessments, or sharing data. Again, information-sharing capacities, rather than privacy legislation, appear, at the time of writing, to be principally responsible for impeding government responses to COVID-19.

4.5.2 - Public and Privacy Data Handling Laws and New Technologies to Combat Health Emergencies

The data from the DGHH Lab's study and concerning the uptake and usage of the COVID Alert application in Canada, in combination with comments from the OPC and privacy advocates, makes it difficult to ascertain whether the collection, use, and disclosure of information through COVID Alert continues to comply with privacy legislation. The GAEN framework utilizes decentralized information collection, and thus, raises questions as to the application of public and private privacy legislation that deals with identifiable personal information.

The *Privacy Act* would apply insofar as the application was predominantly operated by the public sector. So long as the collection, use, or disclosure of information was directly related to an operating activity, the COVID Alert application would likely comply with public sector privacy legislation. Notably, and as discussed previously, public health laws

195 Office of the Auditor General. (2021). "COVID-19 Pandemic Report 10: Securing Personal Protective Equipment and Medical Devices," Office of the Auditor General. Available at: https://www.oag-bvg.gc.ca/internet/English/parl_oag_202105_01_e_43839.html.

as well as emergencies legislation significantly empower government organizations to collect, use, or disclose personal information when combating a health emergency, such as COVID-19, without imposing significant restrictions on such activities. However, we set aside these considerations of how public sector legislation might enable the operation of COVID Alert on a twofold basis: first, because *PIPEDA* (and substantially similar provincial legislation) arguably plays a role given that private companies developed the underlying framework for the application, and second, because the federal and provincial governments chose to make the adoption of the application voluntary, and thus consent driven as opposed to compelling its adoption.

In turning to private sector privacy legislation, namely *PIPEDA*, for our analysis, the adoption and use of the COVID Alert application was consent driven insofar as individuals could choose to download and install the application, configure it, and delete it whenever they chose. As such, there is no need to rely on an exception to consent in *PIPEDA* to justify its installation on individuals' smartphones. However, even when consent has been obtained, it is necessary to assess whether a particular use of personal information is appropriate by way of applying the four factors in the *Eastmond* test:

- Is the measure demonstrably necessary to meet a specific need?
- Is the measure likely effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?[196]

The COVID Alert application was a new technology. The application's necessity was not well understood, its effectiveness remains unclear, and its benefits are largely unrealized a year after its launch. The result is that it is not inherently clear that the application was absolutely necessary to manage the pandemic, and given that there were successive waves of infection that took place after the application's introduction, it was not necessarily effective in meeting a need—unless retroactive analysis of the application demonstrably indicates otherwise. At the same time, it is not easily apparent how to satisfy the *Eastmond* criteria using new technologies in emergencies that rely on mass, voluntary adoption for there to be (prospective) substantial societal benefits.

As of writing, there has not been a formal assessment by governmental or civil society oversight groups about whether the application achieved the purposes it set out to meet. Indeed, the government of Canada has not disclosed the objectives that the application was expected to accomplish (or the metrics used to measure this accomplishment),

196 *Eastmond v Canadian Pacific Railway*, 2004 FC 852.

despite the application being available to the public for approximately one year, at the time of writing. The government did identify that some data on the application's adoption would be collected as of February 2021, but the standards upon which the data would be evaluated were not provided.[197]

The difficulty of ascertaining whether COVID Alert's collection, use, and disclosure of information satisfies the *Eastmond* factors magnifies the challenge of relying on these factors, let alone the reasonableness standard, to assess the utility of new technologies in emergency situations to combat the spread of diseases. There is a severe risk of adjudicating the effectiveness of new technologies based on factors that are largely created after the technology's deployment because relying on after-the-fact factors makes it challenging to determine the necessity, effectiveness, and proportionality of the technological measure prior to it even being deployed, to say nothing of whether there was a less privacy-intrusive way of achieving the same objective given the resources that were available at the time. Put another way, without reasons that clearly justify the collection, use, or disclosure of personal information, a new technology may not satisfy the *Eastmond* factors even when a technology has been consensually adopted by Canadians. Further complicating any analysis is the fact that digital technologies can be, and in the case of COVID Alert were, modified and updated over the course of their usage, which threatens to make applying the four factors that much more challenging because an initial assessment may be decided one way and a subsequent post-update assessment another. Further, without a clarity in law that restricts how such updates might modify an application, or the collection, use, or disclosure of the collected information, individuals may decline to adopt an experimental application and thus reduce the effectiveness and necessity of the technology in question.

From the use of digital contact-tracing mechanisms to the increased collection and use of data from public and private corporations, information sharing remains in the background of pandemic response and recovery efforts. Though many worried that this increase in information sharing could come with impacts on legislated privacy protections, existing permissive health and emergencies legislation as well as exemptions and permissions within privacy legislation ensured that enhanced data collection, use, and disclosure was possible over the course of the pandemic and in similar kinds of health emergencies. What remains to be seen in studies or commissions of inquiry in future months and years is whether the sharing that was authorized under existing legislation was, in fact, appropriately calibrated to mitigate the virus' transmission.

197 Health Canada. (2021). "COVID Alert updated to help evaluate its effectiveness in reducing the spread of COVID-19," Government of Canada. Available at: https://www.canada.ca/en/health-canada/news/2021/02/covid-alert-updated-to-help-evaluate-its-effectiveness-in-reducing-the-spread-of-covid-19.html; Charlie Pinkerton. (2021). "Canada might learn soon whether COVID Alert app is a dud," *iPolitics.* Available at: https://ipolitics.ca/2021/02/11/canada-might-learn-soon-whether-covid-alert-app-is-a-dud/.

4.5.3 - Privacy Protection Frameworks Do Not Adequately Address Privacy Concerns

Some of the privacy rights that Canadians normally enjoy can be modified in the face of public health emergencies such as when federal or provincial governments exercise emergency powers to justify their collection of personal information or when governments lawfully obtain or handle personal information when doing so is directly related to one of the organization's operational activities. While either of these framings may provide governments with authority to collect, use, and disclose information, individuals may feel as though their privacy rights are unduly infringed on the basis that their consent may *not* be requested.

These experiences are, in part, linked to popular conceptions of what privacy means. Privacy as a concept is often represented as casting a barrier around individuals to create a sphere wherein their private affairs can be conducted as separate from intrusion from unauthorized public and private entities.[198] These boundaries can take several forms depending on how privacy is conceptualized. For example, spatial or territorial boundaries recognize when an outsider views a space; behavioural or personal boundaries identify activities that are meant to be secure from unwanted attention and that protects bodily integrity; and informational boundaries protect types of information in differing degrees.[199] The COVID-19 pandemic triggers many of these boundaries. Spatially, individuals want their homes to be private and free from their employer's gaze. Behaviourally or personally, individuals want to move about freely and make informed choices as to vaccinations. And informationally, individuals want to keep their medical information private. Perhaps most relevant in the pandemic context is the informational boundary because of the increased information sharing.

Consent-based frameworks envision privacy as control. That is, individuals control their information and function as manual gatekeepers, choosing who can cross their privacy boundaries and who cannot. When exceptions to consent operate and reasonableness models are exercised to override their manual control or where governments directly collect information on the basis that doing so pertains to an organization's operations, individuals may naturally experience privacy violations, despite the presence of a law that potentially authorizes such boundary crossings.

Lisa Austin posits that derogations from consent should not necessarily be understood

198 Christopher Parsons. (2015). 'Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance," *Media and Communication* 3(3), pp. 1-11. Available at: https://www.cogitatiopress.com/mediaandcommunication/article/view/263.

199 Christopher Parsons. (2015). 'Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance," *Media and Communication* 3(3), pp. 1-11. Available at: https://www.cogitatiopress.com/mediaandcommunication/article/view/263.

as derogations from privacy.[200] Instead, normative conceptions of privacy acknowledge the contextual integrity of moments that activate privacy norms and expectations.[201] Rather than relying exclusively on consent-based models to empower individuals to exercise their privacy rights, a reasonable purposes model, which would see individuals giving implied consent where the purposes of the information collection, use, or disclosure are reasonable and the individual is properly notified of those purposes, might be adopted.[202] Returning to the gatekeeper analogy, under the reasonableness model, rather than individuals manually gatekeeping their privacy boundaries, automatic gatekeepers would allow boundaries to be crossed when reasonable purposes are demonstrably necessary and proportionate.

Assessing the reasonableness of purposes, however, is challenging in emergency situations where the nature of the emergency is not precisely understood, which leaves open what information is needed to respond to it, and where collections, uses, or disclosures of information may have discriminatory effects on parts of the broader population. In such cases, neither individuals nor experts may understand what boundaries ought to be crossed or what data and how much of it is required by governments to quell the emergency or how long the emergency might last.[203] In novel emergencies, government agencies that seek access to information may not know what information they need or how they will want to use collected information. These circumstances make it challenging to accurately assess the necessity and proportionality of any given measure. Finally, both contextual integrity and reasonableness standards are normatively challenged when individuals do not trust the "automatic gatekeeper" (i.e., the government or courts) to ensure that their data is not being unduly collected, used, or disclosed. Put another way, where either the context itself, government institutions, or their private sector partners are treated with suspicion and skepticism (e.g., "is the COVID-19 pandemic real?" "Will the government just change the terms under which they use my information once they have collected it?"), the very reasons used to justify the collection, uses, or disclosures of data may be contested.

Amid the COVID-19 pandemic, these concerns have loomed large. Individuals remained uninformed of the amount of data being collected about them to quell the emergency,

200 Lisa Austin. (2006). "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA," *University of Toronto Law Journal* 56. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=864364.

201 Helen Nissenbaum. (2009). "Privacy in Context: Technology, Policy and the Integrity of Social Life," Stanford University Press.

202 Lisa Austin. (2006). "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA," *University of Toronto Law Journal* 56. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=864364.

203 Lindsay F. Wiley and Stephen I. Vladeck. (2020) "Coronavirus, Civil Liberties, and the Courts: The Case Against 'Suspending' Judicial Review," *Harvard Law Review Forum* 133(9). Available at: https://harvardlawreview.org/2020/07/coronavirus-civil-liberties-and-the-courts/.

which still has an unknown duration. Additionally, governments have experimented with new technologies, such as the COVID Alert application, without certainty regarding the effectiveness or necessity of the information that has been collected. Lastly, individuals often lacked trust in public institutions that were tasked with protecting their privacy and associated rights.[204] How governments will address these challenges is left to future parliamentary committees, commissioners of inquiry, or even Royal Commissions to answer. What is clear is that the pandemic has once more thrown into relief the difficulties of defining and protecting privacy rights and interests and the conditions under which government agencies or their proxies can collect, use, or disclose information generally, as well as in the midst of a health emergency.

4.6 - Conclusion

The COVID-19 pandemic represents the first public health crisis in which Canada's federal and provincial privacy, health, and emergency legislation operated simultaneously, highlighting the use of these powers to collect, use, and disclose personal information. As a result of a poorly coordinated government response to SARS, proactive and reactive tools to combat public health threats were implemented, including the creation of the Public Health Agency of Canada (PHAC) and the application of emergency legislation to public health crises. Both PHAC and the emergency legislation were used during the COVID-19 pandemic. Lawful information sharing also occurred often, despite individuals remaining uninformed of the amount of data being collected about them. Additionally, the COVID-19 pandemic was novel in terms of the digital technologies used to collect information, which raised concerns as to how existing legislation governs new technology when its necessity and proportionality remain unclear. Moreover, the low user uptake of the COVID Alert application, in particular, suggests that despite the privacy-protecting nature of the GAEN technology, individuals still had concerns about their privacy. Considering these problems, the ways in which Canada governs information sharing and protects privacy rights ought to be revisited and reformed following the conclusion of the COVID-19 pandemic.

204 Edelman. (2021). "Edelman Trust Barometer 2021," Edelman. Available at: https://www.edelman.ca/sites/g/files/aatuss376/files/trust-barometer/2021%20Canadian%20Edelman%20Trust%20Barometer_0.pdf. Polling showed that only 59% of Canadian trusted government institutions (p. 7), 47% were concerned about losing their freedom and 17% fearful of this happening (p. 10), and that trust in leaders (p. 20) and spokespersons (p.21) were below 50%. See also: Ryan Tumilty. (2021). "COVID pandemic corroded Canadians' trust in politicians — even their neighbours, poll finds," *National Post*. Available at: https://nationalpost.com/news/politics/covid-pandemic-eroded-canadians-trust-in-politicians-science-and-even-their-neighbours-poll-finds.

5. Canadian Law Reform and Future Pandemic Responses

The Government of Canada introduced the *Consumer Privacy Protection Act (CPPA*), an expansive piece of legislation, during the COVID-19 pandemic. It would have reified some aspects of existing federal privacy legislation while expanding how information could be collected, used, or disclosed to other public or private parties without first obtaining individuals' consent.[205] The legislation ultimately died on the Order Paper when a federal election was called in August 2021.

In this section, we first outline how selected parts of the legislation (which are linked with the non-consensual collection, use, or disclosure of personal information) could inform future data-handling practices as they pertain to health research and health emergencies; then we proceed to discuss their ramifications. Given that the *CPPA* was intended to replace the existing legislation, the *Personal Information and Protection of Electronic Documents Act* (*PIPEDA*), we do not distinguish between what has been slightly modified in the update and what has been newly introduced because the *CPPA,* in its entirety, would guide how personal information might be used in future health emergencies. After outlining the legislation and some of its ramifications, we conclude by discussing the key principles that Western democratic states should integrate into privacy law reforms that either reify existing practices or that broaden non-consensual collections, uses, or disclosures of personal information in responding to health crises.

5.1 - Legislative Summary

Had it been passed into law, the *CPPA* would have replaced the existing federal commercial privacy legislation, *PIPEDA. PIPEDA*, as of writing, continues to establish the minimal standards that Canadian organizations in Canada must comply with when operating in a federally regulated sector or should they engage in cross-provincial business. Provincial governments can pass significantly similar legislation (i.e., either similar to or exceeding the standards in *PIPEDA*) that is applied to organizations under those governments' jurisdiction.

The *CPPA* was broadly intended "to maintain, modernize, and extend existing rules and to impose new rules on private sector organizations for the protection of personal information."[206] This would have included both re-enacting "a range of provisions in the Personal

205 At time of writing, a series of provinces are also at different stages of reforming their privacy laws. These provinces include Alberta, British Columbia, Quebec, and Ontario.

206 Department of Justice. (2020). "Charter Statement: An Act to enact the Consumer Privacy Protection Act

Information Protection and Electronic Documents Act that allow organizations to disclose an individual's personal information to a government institution without their knowledge or consent in certain circumstances" as well as "related provisions allowing an organization to collect personal information for the purposes of some of these disclosures",[207] and introducing new provisions pertaining to the non-consensual collection, use, or disclosure of personal information. For the purposes of this legislative summary and analysis, we focus principally on sections 29-39 of the *CPPA* as they pertained to the non-consensual collection of personal information and the ways in which such information might have been used to combat future health emergencies.

Under the draft legislation, organizations could have used data in the public interest when doing so would protect an individual[208] or provide notice to their next of kin;[209] mitigate financial abuse;[210] and contribute to statistical or scholarly study or research,[211] archival purposes,[212] journalistic or literary purposes;[213] or more broadly for 'socially beneficial purposes.'[214] In our analysis, we do not include situations of notifying next-of-kin, financial abuse, archival uses, or journalistic or literary purposes.

In accordance with the legislation, an organization could have collected[215] or used[216] an individual's personal information if doing so was in the interests of the individual but where consent could not be obtained in a timely way. The *CPPA* would have reified a provision in *PIPEDA* concerning emergency situations. Specifically, under the *CPPA*, organizations could have used an individual's personal information without their knowledge or consent, "for the purpose of acting in respect of an emergency that threatens the life, health or security of any individual".[217] Only if the information had been disclosed to

---

and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts (C-11)," Government of Canada. Available at: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html.

207 Department of Justice. (2020). "Charter Statement: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts (C-11)," Government of Canada. Available at: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html.

208 *Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (CPPA)* (First Reading), Section 29-31.

209 *CPPA* (1st Reading), Section 33. This is currently enshrined in *PIPEDA*, Section 7(3)(c.1)(iv).

210 *CPPA* (1st Reading), Section 34. This is currently enshrined in *PIPEDA*, Section 7(3)(d.1-d.3).

211 *CPPA* (1st Reading), Section 35. This is currently enshrined in *PIPEDA*, Section 7(3)(f).

212 *CPPA* (1st Reading), Section 36. This is currently enshrined in *PIPEDA*, Section 7(3)(g).

213 *CPPA* (1st Reading), Section 38. This is currently enshrined in *PIPEDA*, Section 7(1)(c).

214 *CPPA* (1st Reading), Section 39.

215 *CPPA* (1st Reading), Section 29(1).

216 *CPPA* (1st Reading), Section 29(2).

217 *CPPA* (1st Reading), Section 30. This is currently enshrined in *PIPEDA*, Section 7(2)(b).

another party would the organization have to retroactively notify the individual of the activity and do so in writing, "without delay".[218] Relatedly, an organization could have disclosed the identity of an individual without their knowledge or consent "if the disclosure is necessary to identify the individual who is injured, ill or deceased and is made to a government institution, a part of a government institution or the individual's next of kin or authorized representative".[219] The organization would then have been required to inform the individual of this disclosure, without delay and in writing, if they were alive.

Organizations would also have been permitted to disclose individuals' personal information without their consent in situations where the disclosure was made, "for statistical purposes or for scholarly study or research purposes and those purposes cannot be achieved without disclosing the information",[220] and where it would be impractical to obtain consent,[221] and the Privacy Commissioner of Canada was alerted ahead of the disclosure.[222] There are no limitations included in the legislation that describe what constitutes a valid or an appropriate kind of statistical or scholarly study or research project.

The broadest and most novel situation in which an organization might have been able to disclose an individual's personal information under the *CPPA* was when doing so would have advanced a socially beneficial purpose. In such situations, an organization might have disclosed personal information without an individuals' knowledge or consent so long as criteria contained within section 39(1) had been met:

a. the personal information is de-identified before the disclosure is made;
b. the disclosure is made to
    i. a government institution or part of a government institution in Canada,
    ii. a health care institution, post-secondary educational institution or public library in Canada,
    iii. any organization that is mandated, under a federal or provincial law or by contract with a government institution or part of a government institution in Canada, to carry out a socially beneficial purpose, or
    iv. any other prescribed entity; and
c. the disclosure is made for a socially beneficial purpose.

218 *CPPA* (1st Reading), Section 31. This is currently enshrined in *PIPEDA*, Section 7(3)(e).

219 *CPPA* (1st Reading), Section 32. This is currently enshrined in *PIPEDA*, Section 7(3)(d.4).

220 *CPPA* (1st Reading), Section 35(a). This is currently enshrined in *PIPEDA*, Section 7(3)(f).

221 *CPPA* (1st Reading), Section 35(b). This is currently enshrined in *PIPEDA*, Section 7(3)(f).

222 *CPPA* (1st Reading), Section 35(c). This is currently enshrined in *PIPEDA*, Section 7(3)(f).

The *CPPA* defined "socially beneficial purposes" as constituting "a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose".[223] Prescribed entities and other prescribed purposes would have been set using orders in council as opposed to requiring legislative authorization.[224]

5.2 - Discussion

If passed into law without modification, the *CPPA* would have perpetuated existing exceptions to consent while creating new ones that could have been used in future health emergencies. In our discussion, we outline how existing exceptions could be used under *PIPEDA* today and reified had the *CPPA* received Royal Assent, as well as how new exemptions surrounding socially beneficial uses of personal information could be used by private organizations.

To begin, maintaining a condition in which organizations can collect and use information in the interests of the affected individual when consent cannot be obtained in a timely way threatens to continue the practice of private organizations justifying their decisions to handle data in excess of what an individual might consider to be in their personal interests. As an example, during the COVID-19 pandemic, marketing companies used information that was collected for one purpose— such as advertising or facilitating the data brokerage economy more broadly—to provide assessments of residents' mobility patterns and communicate that individuals' movements may be spreading infections.[225] Many such data brokers collected information from applications on mobile

223 *CPPA* (1st Reading), Section 39(2).

224 Privy Council Office. (2021). "Orders in Council: Glossary," Government of Canada. Available at: https://www.canada.ca/en/privy-council/services/orders-in-council.html. The Government of Canada defines an 'Order in Council' as: "A legal instrument made by the Governor in Council pursuant to a statutory authority or, less frequently, the royal prerogative. All [Orders In Council] are made on the recommendation of the responsible Minister of the Crown and take legal effect only when signed by the Governor General."

225 Jennifer Yang, Kate Allen, and Andrew Bailey. (2020). "What cellphone mobility data can teach us about why lockdown might not be working, and what to expect from the holidays," *Toronto Star*. Available at: https://www.thestar.com/news/gta/2020/12/13/what-cellphone-mobility-data-can-teach-us-about-whos-driving-covid-infections-in-toronto-and-what-to-expect-from-the-holidays.html; Jennifer Yang. (2021). "Why did Ontario COVID-19 rates surge after Christmas? New cellphone mobility data offers some clues," *Toronto Star*. Available at: https://www.thestar.com/news/gta/2021/01/10/why-did-ontario-covid-19-rates-surge-after-christmas-new-cellphone-mobility-data-offers-some-clues.html; Jennifer Yang and Andrew Bailey. (2021). "Cellphone data shows people are on the move again. What mobility patterns tell us about 'leaky lockdowns' and a possible third wave," *Toronto Star.* Available at: https://www.thestar.com/news/gta/2021/03/10/cellphone-data-shows-people-are-on-the-move-again-what-mobility-patterns-tell-us-about-leaky-lockdowns-and-a-possible-third-wave.html. Data for the articles produced by the Toronto Star came courtesy of Environics Analytics (https://environicsanalytics.com/en-ca), which per the company's privacy policy (see: https://environicsanalytics.com/en-ca/footer/privacy/services-privacy-policy) partners with cuebiq (https://www.cuebiq.com), Ubermedia (https://um.co), and Veraset (https://www.veraset.com) to collect location information. Location information is often collected when individuals install an application that uses one of the aforementioned companies' software development kits (SDKs);

devices without any specific interaction with the owners of those devices. As such, they had no way of directly or meaningfully obtaining consent for additional uses of the collected data.[226] These kinds of unilateral collections or processing of information, of which individuals may have no knowledge, by organizations could persist and expand in the future should the existing language in *PIPEDA* be reified in future privacy legislation, as was the case in the *CPPA*. By way of example, this reification may mean that in future health emergencies that sensors, which have been distributed around a city for the purpose of calculating population density (e.g., by assessing how frequently people pass down a street), may subsequently be used to identify individuals who possess some potential disease symptom (e.g., a particular skin tone, gait pattern, etc.) without seeking affirmations from individuals that they consent to such uses of their personal information.

In turning to how private organizations might mobilize information in the advent of an emergency, the *CPPA* replicated the pre-existing exemptions to obtaining consent that have been associated with section 7(2)(b) of *PIPEDA*. Specifically, the *CPPA* did not define precisely what constitutes an emergency. When this absence of a definition is combined with the breadth of situations where an individual might be identified, governments have the ability to mount a strong argument that they should be permitted to use information from private telecommunications networks to respond to a health crisis. Over the course of the pandemic, telecommunications companies in Canada, the UK, and the United States have all been restricted in how they could or would assist governments, in part due to questions concerning the efficacy of their assistance[227] as well as consumer perceptions of privacy concerns; in Canada, at least, the same companies might have been challenged in arguing that *PIPEDA* (or the *CPPA*, had it been passed into law) would have precluded such data sharing. If the *CPPA* had been passed into law, telecommunications companies would, in theory, have been able to share information under that legislation on the basis that the legislation affirmed that organizations could use individuals' personal information for the purposes of "acting in respect of an emergency that threatens the life [or] health...of any individual".[228] In effect, this would replicate the pre-existing permissive sharing conditions found in *PIPEDA*'s section 7(2)(b).

---

each asserts that consent is required before the companies can collect the information, though it is dubious that users typically understand that consenting to such collection to activate a feature in a smartphone application results in the location data also being transmitted to the aforementioned data brokerage companies.

226 Ronald J. Deibert. (2020). *Reset: Reclaiming the Internet for Civil Society*, House of Anansi Press.

227 Murad Hemmadi and Caroline Mercer. (2020). "Trace me on my cellphone: The different ways governments are using phones to fight COVID-19," *The Logic*. Available at: https://thelogic.co/news/special-report/trace-me-on-my-cellphone-the-different-ways-governments-are-using-phones-to-fight-covid-19/; Alex Boutilier. (2020). "Governments aren't tracking your cellphone in the battle against COVID-19. But they might," *Toronto Star*. Available at: https://www.thestar.com/politics/federal/2020/03/24/governments-arent-tracking-your-cellphone-in-the-battle-against-covid-19-but-they-might.html.

228 *CPPA* (1st Reading), Section 30.

Yet, where the specific symptoms of a disease are unknown or the ways a disease is communicable are still in question, any company that collected information could use that personal information to try to assess or solve these kinds of questions and any other question that pertain to responding to threats to the life, health, or security of any individual. In effect, this element of *PIPEDA*, which would have been recertified in the *CPPA,* threatens to permit any use of any collected data without organizations needing to notify the individuals whose data is being used, so long as an organization can justify the usage.

In a related vein, under the *CPPA,* in emergency situations organizations could, "disclose an individual's personal information without their knowledge or consent to a person who needs the information because of an emergency that threatens the life, health or security of any individual".[229] In the case that this information was disclosed, the individual must subsequently be notified "without delay" about the disclosure in writing.[230] (These permissions and requirements also exist in *PIPEDA* at 7(3)(e).[231]) In cases where organizations collect information about individuals but may lack a home or work address, phone number to send a text message, or email address, it may be functionally impossible to contact individuals about such disclosures. This inability may not have prohibited the disclosure of information under the *CPPA* (or *PIPEDA*), so long as organizations committed to notifying individuals in writing without delay by perhaps taking out advertisements meant to target individuals whose data had been disclosed. As an example, a company might collect movement data throughout an urban environment, which constitutes information about identifiable individuals, and disclose information about who was proximate to super-spreader disease events to other organizations under section 31 of the *CPPA*. Despite having a rich set of personal information, the organization may lack a defined way of contacting the specific individuals; while the organization might assume it knows where the individuals work or live, in dense urban environments, this movement information may not be linked to a specific home address or a desk or station at which that the individual works. Nonetheless, when disclosed to another organization that could overlay additional information atop that disclosed, the individual might be quickly and easily identified by the party to whom the information was shared, without this information

229 *CPPA* (1st Reading), Section 31. Emphasis not in original.

230 *CPPA* (1st Reading), Section 31.

231 *PIPEDA* 7(3)(e): "7(3): For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is … (7(3)(e)) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure."

transitioning to the original disclosing party. The result is that while the information might be used by the organization to whom information had been disclosed, the originator of the information might be prevented from informing individuals of the disclosure.

Per section 35(a) of the *CPPA* or section 7(3)(f) of *PIPEDA*, novel epidemiological situations or situations where an epidemic or pandemic threatens a region of Canada could be investigated, in part, by undertaking statistical or scholarly research or study. Such investigations might, as an example, involve sharing Internet of Things sensor information that in aggregate is deeply revelatory of a person's behaviours, inclusive of their political, medical, or sexual activities.[232] Per section 35 of the *CPPA*, this kind of information could have been shared for the aforementioned reasons when they could not be achieved "without disclosing the information"[233] or where it would be "impracticable to obtain consent",[234] so long as the "organization informs the Commissioner of the disclosure before the information is disclosed"[235] These requirements would have encouraged the sharing of information and were not designed such that the Commissioner would have had to approve the disclosure before the research began or occurred. While the notification requirement would, positively, not have seen the Commissioner intrude into research processes, it would have had the effect of preventing individuals from knowing that their information had been disclosed, including to potentially facilitate statistical analyses they might have opposed (e.g., on the grounds that researchers could potentially create statistical models or machine-learning data sets or models that could negatively impact the individual's life chances). The legislation also did not require the Commissioner to broadly publicize the regularity at which they were informed of such disclosures or for the Commissioner to publicize their responses in assessing the appropriateness of the disclosure itself. All of these deficits would have reified the pre-existing problems within *PIPEDA*, as they replicate legislative functions contained within the currently existent law.

In the case of disclosing a person's de-identified personal information when doing so serves a socially beneficial purpose, which introduced new ways of handling individuals' personal information in excess of what is currently permitted under *PIPEDA*, the individuals whose information would have been disclosed would not have needed to be notified of the activity, even if it were possible to do so. While the definition of 'socially beneficial purpose' in the *CPPA* was restricted to include purposes "related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment" they could have been subsequently expanded to include, "any other prescribed

232 Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. (2014). "Privacy in the Internet of Things: Threats and Challenges," *Security and Communications Networks* 7.

233 *CPPA* (1st Reading), Section 35(a).

234 *CPPA* (1st Reading), Section 35(b).

235 *CPPA* (1st Reading), Section 35(c).

purpose".[236] In effect, so long as information had been de-identified, it could have been shared to a government institution or a part of such an institution or a healthcare or post-secondary institution or a library or an organization mandated to carry out socially beneficial activities or "any other prescribed entity".[237] This provision had the potential to see information—which may be biased or have otherwise deleterious consequences on the specific individuals whose information was shared, the classes of individuals they were linked to, or the broader sub-populations with which they may have been associated—shared to develop policy responses or mathematical models, which themselves might be biased, in response to health emergencies.

In aggregate, under the *CPPA*, personal information might have been disclosed without individuals understanding how or why, so experts might understand a disease or address a health emergency. In many of the aforementioned cases, however, there was a significant lack of accountability or transparency around non-consensual data collection, use, and disclosure, which could endanger public trust in the models or health responses derived from such data. Notably, given that many of these legislative proposals were included in *PIPEDA*, it is already possible for private organizations to engage in a range of potentially deleterious activities with individuals' personal information without obtaining their consent, or publicly certifying the necessity and proportionality of their non-consensual handling of individuals' personal information. Further, in the case of assessments of how and to what end data may have been used under the *CPPA*, key questions of necessity, proportionality, and reasonableness were not directly engaged as conditions that must be satisfied prior to the more indiscriminate data-handling conditions being activated. How such data was to be used and from where it was to be collected assumes heightened importance in health emergencies, given that what is collected and how it is used can potentially lead to highly inequitable health policy responses. Such an outcome could have had the twofold effect of insufficiently addressing the given health emergency, while fanning flames of distrust in health response measures.

Finally, and perhaps most importantly, a key lesson of the 2003 SARS pandemic and, thus far, of the COVID-19 pandemic in Canada has been that there are deficits in information sharing—which are not due to these activities being prohibited by privacy law—and inequitable mobilization of health resources such that those who have been least advantaged in society have borne the brunt of the health and economic fallout of COVID-19. This, broadly, calls into question the very need for further reification of non-consensual data collection, processing, and sharing of information to address health emergencies generally.

236 *CPPA* (1st Reading), Section 39(2).

237 *CPPA* (1st Reading), Section 39(1)(b)(iv).

5.3 - Required Principles for Law Reform

Privacy is not an absolute right in Canada or other jurisdictions, in that there are conditions under which rights to privacy may be legitimately abridged by private or public interests. This is especially true in the case of serious health emergencies that affect significant swaths of a jurisdiction's population. As was discussed in section four, government officials will often handle data absent individuals' consent so long as the collection, use, or subsequent disclosure pertains to a government agency's mandates or functions, or on the basis that such activities are authorized under health or emergencies legislation. Furthermore, principles associated with contextual integrity, which recognize that individuals should be able to make decisions about how their data is used at the time of use instead of in advance of such uses, are recognized as opening pathways to using personal information for legitimate (and desirable) purposes while still empowering the individuals from whom the information is derived or obtained.

When the Canadian government handles personal information, it is, by necessity, guided by the *Charter of Rights and Freedoms*, as well as relevant legislation and case law that dictate how personal information can be legitimately handled. In contrast, private organizations are not guided by the same legal touchstones. One of the many reasons why governments have passed privacy and data protection legislation is to ensure that these organizations adhere to minimum standards of practice, which are, in some cases, either indirectly or directly informed by human rights commitments.

In the case of European countries, many of them have adopted data protection legislation that takes a human-rights-first approach. As such, their legislation is written such that businesses that handle European residents' information are required to adhere to standards based on international human rights norms and principles. This is demonstrated throughout the General Data Protection Regulation (GDPR), wherein it is explicit that the privacy and data protection commitments imposed on private organizations are intended to secure a range of rights and freedoms. Recital 4 of the GDPR, as an example, attends to the importance of "the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."[238]

Canada's *PIPEDA* and the proposed *CPPA*, on the other hand, are largely predicated on different conceptual foundations. As a piece of consumer legislation, the *CPPA* did not

238 European Union. (2016). "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

assert that organizations' handling of personal information was meant to be interpreted through a rights-based lens. As noted by Emily Laidlaw, "[c]onsumer privacy legislation that does not acknowledge the right to privacy is a glaring absence. It misses the elephant in the room in terms of the privacy threats we face, and fails to provide direction to the Privacy Commissioner, new Tribunal and courts that will be tasked with interpreting the provisions."[239] Teresa Scassa similarly recognized that the *CPPA* failed "to address privacy as a human right" and, as such, it did not cohere with the organizing principles of the Convention 108+ that "puts human rights front and centre" as well as the GDPR, which also "directly acknowledges the human right to privacy, and links privacy to other human rights."[240] Per Colin Bennett, privacy legislation does not need to include a human rights analysis to receive an European Union adequacy judgement, though he noted that it is "very puzzling" as to why the *CPPA* was framed through an explicit economic lens, given repeated calls by the Office of the Privacy Commissioner of Canada for reforms of federal commercial privacy legislation to be grounded in human rights.[241]

Privacy is not an issue that pertains exclusively to individuals and that can be negotiated by consent-based contracting. Instead, it simultaneously engages individual and collective interests. A human-rights-based framing for privacy or data protection laws can serve to clarify these broader and often collective sets of rights, which are implicated in what are often cast as privacy-related disputes.[242] In the absence of clarity regarding the use of human rights norms and principles to interpret the *CPPA*, balancing competing interests would have been limited to those exclusively stated in the legislation. That is, where data was collected, used, or disclosed pursuant to a health incident or research, organizations would have been freer to share information than when they need to consider a broader set of rights that would mediate their handling of personal information. As noted by Scassa, federal privacy reform in Canada is clearly required given the volume, velocity, and variety of data that is being handled today. But such reforms must both recognize a fundamental right to privacy and acknowledge "the interrelationship between privacy and the right of individuals to exercise their other rights with autonomy and dignity."[243]

239 Emily Laidlaw. (2020). "Canada's Proposed New Consumer Privacy Protection Act: The Good, the Bad, the Missed Opportunities," *University of Calgary Faculty of Law*. Available at: https://ablawg.ca/2020/11/30/canadas-proposed-new-consumer-privacy-protection-act-the-good-the-bad-the-missed-opportunities/.

240 Teresa Scassa. (2020). "It's not you, it's me? Why does the federal government have a hard time committing to the human right to privacy?," *Teresa Scassa* (Personal Homepage). Available at: http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=333:it's-not-you-it's-me?-why-does-the-federal-government-have-a-hard-time-committing-to-the-human-right-to-privacy?&Itemid=80.

241 Colin J. Bennett. (2021). "Canada's new Consumer Privacy Protection Act: Will it be 'adequate'?" *Privacy Laws & Business* 169.

242 Christopher Parsons. (2015). "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance," Media and Communication 3(3).

243 Teresa Scassa. (2020). "A Human Rights-Based Approach to Data Protection in Canada," in Elizabeth Dubois and Florian Martin-Bariteau (Eds). *Citizenship in a Connected Canada: A Research and Policy Agenda.* University of Ottawa Press. Pp. 178.

Failure to both adopt a rights-based approach and delimit the range and rationales for which personal information might be collected, used, and disclosed creates a risk of an adequate framework to guide private organizations operating in Canada and an inability to empower Canadians to flourish in digitized societies. Had the *CPPA* been passed into law in its form at first reading, private organizations that handle European residents' data would have been required to abide by European regulations (i.e., the GDPR) and, as such, would either be required to apply stronger European standards in their Canadian operations (i.e., capture both Europeans and Canadians under a common, more comprehensive, European regulatory umbrella) or applied the weaker Canadian regulations to Canadians' personal information and the stronger protections to Europeans. In the latter case, they would have had the effect of creating a bifurcated system where Europeans enjoyed one high standard of protection and Canadians a lower standard of protection.[244] Furthermore, creating a bifurcated international regulatory environment would have run the risk of increasing costs to Canadian organizations that operate internationally.[245] The result of compelling organizations to make this decision would have been to either mitigate some of the influence of Canadian law if organizations simply adopted strong European privacy protections or to prevent residents of Canada from enjoying equivalent protections to residents of other leading Western democracies if companies opted to apply weaker privacy regulations to Canadians and stronger ones to non-Canadians. Indeed, given that *PIPEDA* presently applies to Canadian organizations and its clauses would have been integrated into the *CPPA*, Canadian organizations are already bearing the costs of making decisions concerning which privacy regulations apply to which consumers. Future federal Canadian privacy legislation should ensure that organizations can adopt strong, harmonized, privacy protections as opposed to once more reimposing the cost of deciding which customers receive which strong protections and which receive weak ones.

Absent the more comprehensive protections set out in the GDPR or other human-rights-based privacy legislation, Canadian residents may be less able to flourish should legislation such as the *CPPA* ultimately be adopted, given that privacy is intractably entwined with freedoms of expression, association, religion, and more. Only by making clear that any assessment of the necessity and proportionality of an abridgement of privacy right must be made, based on a consideration of its impact on human rights, can

244 For more, see: Colin J. Bennett. (2021). "One set of privacy rights for Europeans, a lesser one for Canadians? Why the Canadian Consumer Privacy Protection Act and the EU's General Data Protection Regulation should be in alignment," *Colin J. Bennett* (Personal website). Available at: https://www.colinbennett.ca/canadian-privacy/one-set-of-privacy-rights-for-europeans-a-lesser-one-for-canadians-why-the-canadian-consumer-privacy-protection-act-and-the-eus-general-data-protection-regulation-should-be-in-alignment/.

245 For more, see: Lex Gill, Cynthia Khoo, Jeffrey Knockel, Adam Molnar, Christopher Parsons, and Kate Robertson. (2020). "Submission to the Ministry of Government and Consumer Services Consultation: Strengthening Privacy Protections in Ontario," Citizen Lab. Available at: https://citizenlab.ca/wp-content/uploads/2020/11/ON-Gov-Privacy-Consultation-Sept-30-2020.pdf. Pp 9-10.

rule-making empower individuals and communities. In the case of health emergencies, such human-rights-based assessments are of particular importance given the need to ensure that emergency responses engender the trust of Canadians (citizens and residents alike) and respect the fundamental rights and freedoms as outlined in the *Charter*. As we have noted previously,[246] trust is essential in producing positive public health outcomes. Developing a rights-based privacy legislation is a crucial step toward reassuring individuals and their communities that they can trust the organizations or institutions that are handling their data in response to a novel virus or other emergent health risks.

In addition to injecting a rights-based approach to privacy into legislation such as the *CPPA*, stronger accountability and transparency schemas need to be integrated to ensure that private organizations behave in full conformity with the meaning and intent of the legislation. Efforts to ensure greater transparency may take the form of publicly written declarations that are understandable to the general public and experts alike (e.g., regarding the ways in which personal data is collected, used, or disclosed without consent), while greater accountability may be achieved through a requirement to report activities to the Office of the Privacy Commissioner of Canada or its provincial counterparts, accompanied by the potential for sanctions if organizations intentionally misconstrue the authorizing legislation (or have made serious errors in the application of the law). The goal of such efforts would not be to unduly burden private organizations, but, instead, to ensure that they are responsible for the ways that they handle information and can be held accountable for accidental or malignant uses of personal data. In terms of using data without consent for health-related purposes (including in emergency situations), strengthening transparency and accountability mechanisms in the law could enhance Canadian residents belief that their personal information has been collected or used in accordance to the law, and, by extension, improve their trust in institutions that use their personal data as required to combat or mitigate the spread of disease.

5.4 - Conclusion

Canada's *Consumer Privacy Protection Act* (CPPA) was introduced in November 2020 in the midst of the global COVID-19 pandemic and ultimately died on the Order Paper in August 2021. The bill included a range of situations where personal information could be collected, used, or disclosed without first obtaining an individual's consent. Moreover, the legislation would not have relied on human rights norms and principles to set limits to how organizations might share information. It also did not empower the Office of the Privacy Commissioner of Canada to prevent or be required to authorize many of these non-consensual handlings of individuals' information.

246 See Section 4.4 of this report.

While privacy has been noted in the past (e.g., in the aftermath of the 2003 SARS outbreak) as a potential inhibitor of data sharing in Canada, during the pandemic, reports and audits of the government's own behaviour have not borne out this claim. However, had the *CPPA* (or its future legislative equivalent) been passed into law and subsequently used as a model to update privacy legislation that could receive a European adequacy assessment, other jurisdictions may have been incentivized to adopt similar legislation. The consequences of such adoptions may have included the further de-emphasis of consent-based and human rights-respecting privacy principles while simultaneously enabling businesses to use personal information in ways that are not transparent to the public and that are significantly unaccountable to government regulators. Consent-based frameworks cannot be the exclusive format for how personal information is managed but are arguably of heightened importance in situations where other legislative factors are not in place to limit potentially deleterious collections, uses, or disclosures of personal information in emergency situations.

6. Discussion

Governments in the United States, United Kingdom, and Canada scrambled to respond to the COVID-19 pandemic. When information about how the disease spread or presented symptoms was uncertain, these governments, along with the private sector, regularly sought to derive insights from existing stores of data and to establish new techniques for collecting and analyzing data. Private stakeholders played a major role throughout the pandemic response. In addition to collecting, assessing, and sharing data they collected, some of these stakeholders functionally set the terms for smartphone-based location surveillance to curb the virus' spread. In the three countries examined in this report, an ongoing concern with the protection of fundamental human rights, in particular privacy rights, was seen as both a potential hindrance to data collection and as a way to encourage trust in government actions to mitigate the disease. At the same time, in Canada, the pandemic has cast into relief how privacy law reform may affect how private and public organizations can collect, use, or disclose personal information in a future health emergency.

In this part of the report, we briefly address some of the broader themes that cut across the report and how the processes of personal information collection, legal conceptions of privacy, and privacy law reform may all have effects on future responses to health emergencies.

6.1 - Redistribution of Power Between States and Private Organizations

States have historically led data collection efforts when combating health emergencies and have used collected data to help direct state responses. The current COVID-19 pandemic is no exception. State agencies continued to play their traditional roles in collecting information that was subsequently used to try and mitigate the spread of COVID-19. And, as in past health emergencies, private organizations provided surveillance and logistical support. There have, however, been instances during the COVID-19 pandemic that indicated a shift in the abilities of both states or private organizations to collect and present information.

In the case of contact-tracing and exposure-notification applications, the Google Apple Exposure Notification (GAEN) framework has become the default in the three countries, even when states initially sought to leverage mobile devices to more actively collect information in support of their pandemic responses. The United Kingdom, as an example, deployed a non-GAEN application at the outset of the pandemic, but the government was ultimately forced to transition to an application that was GAEN-compliant. States, cities, and universities in the United States created their own applications, some of which were

GAEN-compliant, while others were not. Meanwhile, in Canada, the province of Alberta declined to adopt a GAEN-compliant application, and although most of the rest of Canada did ultimately adopt a GAEN-compliant application, the actual efficacy of the Canadian application, COVID Alert, remains uncertain at the time of writing.

Governments around the world reportedly tried to encourage Google and Apple to modify the GAEN framework to facilitate contact tracing instead of providing just exposure notification. At no point, however, were governments successful in advancing their case.[247] Apple and Google were likely resistant to a more surveillance-capable framework for fear that it could be used by some non-rights respecting governments (e.g., Bahrain or Kuwait[248]) to harm their customers, and while this is a laudable aim, the fact remains that a mode of technological health-related surveillance was denied on the basis of private organizations' fiat. At the same time, however, the GAEN-compliant applications represented a novel way of attempting to collect a massive amount of data in a privacy protective way and a process that saw private organizations modify the most popular smartphone operating systems in the world to facilitate this new form of opt-in, decentralized, mass surveillance.

The significance of private partners was made even more pronounced as governments increasingly relied upon these partners to organize and interpret data to guide and evaluate pandemic countermeasures. In some cases, reliance on private partners involved governments compelling information from private telecommunications companies (e.g., the case of O2 and EE in the United Kingdom), whereas in other situations, companies like Google or mobile advertising data brokers provided information that they insisted was anonymized and could be used to indicate the efficacy of mobility restrictions. It remains to be seen just how useful these disclosures were in informing policy development. Nevertheless, what is notable is that international companies that collect incredible volumes of data about individuals in the course of their regular operations clearly recognized the ability to transform consumer movement insights (e.g., Google Mobility Trends) to health surveillance insights and, also, disclosed at least some of this information. Whereas previously, such information may have been more discrete as it

247 Alex Hern. (2020). "France urges Apple and Google to ease privacy rules on contact tracing," *The Guardian.* Available at: https://www.theguardian.com/world/2020/apr/21/france-apple-google-privacy-contact-tracing-coronavirus; Demi Knight. (2020). "Kenney says federal government told Apple, Google not to work with Alberta on contact tracing apps," *Global News*. Available at: https://globalnews.ca/news/7171872/kenney-says-feds-stopping-apple-google-work-on-alberta-contact-tracing-app/; Reed Albergotti. (2020). "European government officials call for tech companies to loosen grip on contact-tracing technology," *Washington Post.* Available at: https://www.washingtonpost.com/technology/2020/05/29/apple-google-contact-tracing/; Reuters staff. (2020). "Apple and Google still in talks with UK about COVID-19 app technology," *Reuters*. Available at: https://www.reuters.com/article/us-health-coronavirus-apps-britain-idUSKBN22W2QM.

248 Amnesty International. (2020). "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy," Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/.

was held by governments and pertained principally to specific national localities, this information is now held by global companies who have access to massive subsets of humanity's movement and communications records and patterns. While these companies' willingness to share that information may have been helpful, it was demonstrative of the value of data held by private firms, showcased the data collection and governance relationship between private and public organizations, and revealed the first time that communications infrastructure was broadly seen as a source of data that could be used to respond to a global health emergency.

In aggregate, our limited exploratory assessment of data collection processes raises at least two areas to which future policymakers should attend. First, policymakers should assess the extent to which contact tracing, exposure notification, and other forms of digital health surveillance should continue to be dictated (or even driven principally) by private organizations, which have global networks that can be leveraged for surveillance. Second, policymakers should assess the roles that private stakeholders should continue to play in presenting information to the government that they have collected versus government officials, themselves, interpreting collected data. To what extent will an ongoing relationship, characterized by public institutions receiving information without necessarily framing what is to be collected, or how and under what conditions, persist? Relatedly, what might a focus on digital modes of health data collection mean for populations with reduced access to Internet connectivity? This is a significant concern, given that the current COVID-19 pandemic has accentuated the impact of the digital divide. If populations are disadvantaged due to their limited access to digital networks, there is a risk that present digital public health policies and the public-private partnerships they depend on may further accentuate existing inequities.

While governments have raised significant concerns about the power and capabilities of digital technology companies during the COVID-19 pandemic,[249] these capabilities were already on the rise well before the pandemic began.[250] Companies such as Google and Apple arguably acted within the scope of law and ostensibly in the interests of their customers, though they came to decisions about their users in excess of the decisions that governments had made about the residents in their sovereign territories. While we hesitate to state that this is entirely unprecedented—as opposed to a part of a continuum of influence that these companies possessed prior to the pandemic—it certainly suggests a significant reification of the pre-existing power dynamics. The GAEN framework by

249 Tom Loosemore. (2020). "Google and Apple's diktat to governments on coronavirus contact-tracing apps is a troubling display of unaccountable power," *Business Insider.* Available at: https://www.businessinsider.com/opinion-google-apple-contact-tracing-app-troubling-governments-2020-6.

250 Martin Moore. (2016). "Tech Giants and Civic Power," *Kings College London*. Available at: https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf; Emily Laidlaw. (2010). "A framework for identifying Internet information gatekeepers," I*nternational Review of Law, Computers & Technology* 24(3); Rebecca MacKinnon. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* Basic Books: New York.

Google and Apple may ultimately be regarded as yet another example in a long list of examples of corporate influence over how governments make decisions while, at the same time, representing an entirely novel kind of privacy-protective and decentralized mass surveillance. In aggregate, the activities undertaken by private organizations throughout the COVID-19 pandemic indicate a need to rearticulate the power relationship between states and private organizations, especially given that states have the responsibility to protect the health and security of their citizens and resident populations.

6.2 - Real Time Digital Epidemiological Experimentation

COVID-19 is the first pandemic where a significant proportion of those living in the relatively affluent countries that we examined possessed mobile phones with contemporary smartphone operating systems. Government and non-government stakeholders alike theorized that leveraging mobile phones to assist in epidemiological surveillance or notification could help to combat the spread of COVID-19. In countries such as South Korea and China, existing consumer and health services were quickly repurposed to help trace potential exposures to COVID-19.[251] Singapore created its own smartphone application that was initially heralded as an important element of their response to COVID-19.[252] These early adoptions of digital technology to combat the COVID-19 pandemic, along with recognition of how widely mobile phones were distributed, led to expectations that affluent governments would similarly develop applications to help mitigate the spread of the virus. The issue, however, was that applications had never previously been developed and deployed on a mass scale, which was presumably needed to combat a global pandemic.

The COVID-19 pandemic, therefore, represented the first opportunity to determine the efficacy of applications in informing public health officials, assisting contact tracers, or facilitating exposure notification. At the time of writing, it remains unclear what conditions must be met for applications like those reliant on the GAEN framework to effectively

251 Government of the Republic of Korea. (2020). "Flattening the curve on COVID-19: How Korea responded to a pandemic using ICT," Government of the Republic of Korea. Available at: https://overseas.mofa.go.kr/gr-en/brd/m_6940/down.do?brd_id=5893&seq=761548&data_tp=A&file_seq=1; Economist Staff. (2020). "To curb covid-19, China is using its high-tech surveillance tools," *The Economist.* Available at: https://www.economist.com/china/2020/02/29/to-curb-covid-19-china-is-using-its-high-tech-surveillance-tools; Yasheng Huang, Meicen Sun, and Yuze Sui. (2020). "How Digital Contact Tracing Slowed Covid-19 in East Asia," *Harvard Business Review.* Available at: https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia.

252 Dongwoo Kim and Daniela Rodriguez. (2020). "'There's an App for That': Use of COVID-19 Apps in Singapore and South Korea," *Asia Pacific Foundation of Canada*. Available at: https://www.asiapacific.ca/publication/theres-app-use-covid-19-apps-singapore-and-south-korea; see also: Andreas Illmer. (2021). "Singapore reveals Covid privacy data available to police," *BBC.* Available at: https://www.bbc.com/news/world-asia-55541001. See also: Irene Poetranto and Justin Lau. (2020). "COVID-19 and Its Impact on Marginalised Communities in Singapore, South Korea, Indonesia, and the Philippines," *Datactive*. Available at: https://data-activism.net/2020/07/bigdatasur-covid-covid-19-and-its-impact-on-marginalised-communities-in-singapore-south-korea-indonesia-and-the-philippines/.

reduce the spread of COVID-19—though some early publications suggest the United Kingdom saw fewer cases due to residents' use of the applications,[253] while other recommendations have also emerged.[254] Nonetheless, there have been no firmly established determinations of efficacy in the United States or Canada.[255]

In addition to contact tracing and exposure notifications, other experiments that assessed movement of individuals were, at least in part, designed to showcase the effectiveness of mobility restrictions. However, the actual public assessment of this data often left unclear why mobility restrictions were sometimes ineffective in limiting movement amongst some communities but still led to arguments that policies to limit mobility were ineffective. For example, when essential workers had to continue travelling extended distances to get to work, their mobility patterns tended to persist as they travelled to their places of work, despite the mobility restrictions that generally applied to populations. These mobility patterns of essential workers were sometimes used to demonstrate the ineffective implementation of mobility restrictions more broadly, as opposed to facilitating nuanced understanding of why some mobility waned because restrictions applied to some, but not all, segments of society (e.g., mobility restrictions did not affect essential workers). Relatedly, when private organizations were responsible for communicating when mobility had (or had not) diminished, their decisions on what constituted excessive movement could have policy implications. The assessments of mobility information, and evaluations of whether individuals or groups were moving too far or too frequently, could have particularly significant impacts for how policymakers interpreted the efficacy of their policies when private firms created their own rules for what constituted excessive mobility, potentially even where they were in excess of formal mobility rules laid down by governments.[256] The result, in total, has been that public and private organi-

253 Chris Wymant, Luca Ferretti, Daphne Tsallis, Marcos Charalambides, Lucie Abeler-Dörner, David Bonsall, Robert Hinch, Michelle Kendall, Luke Milsom, Matthew Ayres, Chris Holmes, Mark Briers & Christophe Fraser. (2021). "The epidemiological impact of the NHS COVID-19 App," *Nature* https://doi.org/10.1038/s41586-021-03606-z (2021).

254 Jennie Phillips, Petra Molnar, Rebecca Babcock, Tiana Putric, Dyllan Goldstein, Laksmiina Balasubsramaniam, Alisha Gauhar, and Sarah Quayyum. (2021). "Exploring User-Uptake of Digital Contact Tracing Apps - A Practitioner Guide," Digital Global Health and Humanitarianism Lab. Available at: https://figshare.com/articles/book/Exploring_User-Uptake_of_Digital_Contact_Tracing_Apps_-_A_Practitioner_Guide_-_Full/14423861.

255 Betsy Ladyzhets. (2021). "We investigated whether digital contact tracing actually worked in the US," *MIT Technology Review*. Available at: https://www.technologyreview.com/2021/06/16/1026255/us-digital-contact-tracing-exposure-notification-analysis/.

256 In Canada, as an example, journalistic reporting from the *Toronto Star* often assessed the regularity at which people were increasing their average mobility, as defined as moving beyond 500m from their home. Ontario lacked a legal requirement that compelled individuals to remain in their home or within 500m of their place of residence. Despite this lack of strict government directive, whenever individuals ventured more than 500m to get groceries, go for a state-recommended walk, or partake in outdoor recreation more generally they were identified as undertaking excessive movement, with the implication that such movement was partially responsible for the exponential spread of COVID-19 in the population. For more, see: Jennifer Yang, Kate Allen, and Andrew Bailey. (2020). "What cellphone mobility data can teach us about why lockdown might not be working, and what to expect from the holidays," Toronto Star. Available at: https://www.thestar.com/news/gta/2020/12/13/what-cellphone-

zations alike have leveraged existing sensor networks and pools of data in their efforts to combat COVID-19, and sometimes, they have done so in ways that have not been concretely connected to demonstrated efficacy.

In the absence of pre-existing data and efficacy measurements due to novel health emergencies, we are not suggesting that technological experimentation should not take place. However, the ability to leverage vast volumes of data at population levels, which may guide public health policy decisions, reinforces the need for context-sensitivity and proper safeguards when it comes to conducting such experimentations. Moreover, given that negative health outcomes linked to COVID-19 are often associated with the social determinants of health (e.g., gender, socio-economic position, race/ethnicity, Indigeneity, and homelessness),[257] technological experimentation should be undertaken with care so that outcomes do not worsen already uneven access to healthcare and health services, or worsen the deficient social structures that make it challenging for individuals to live safely in the middle of health emergencies (e.g., availability of sick pay or sick days, rent forbearance or holidays, moratorium on evictions, and others). Relatedly, any expansion to what constitutes 'health data' must be assessed by considering the biases that may be built into the data. Specifically, we must consider what is being measured, how it is being measured, and who is being measured, and how must the measured data be overlaid with socio-economic information that can offer context to policy-makers. In other words, while technological or policy experimentation in a crisis may be required, such experiments should not be left solely or principally to technologists or engineers, nor should private organizations be permitted to disclose data prior to it having been assessed for inequities or bias that might otherwise provide problematic and inequitable policy guidance. At the time of writing, retroactive analyses of the consequences of these experiments remain to be written and issued. But the inherent dangers of these experiments will almost certainly persist until efforts are made to expose and address biases built into technologies that are launched or applied in emergency situations.

mobility-data-can-teach-us-about-whos-driving-covid-infections-in-toronto-and-what-to-expect-from-the-holidays.html; Jennifer Yang. (2021). "Why did Ontario COVID-19 rates surge after Christmas? New cellphone mobility data offers some clues," *Toronto Star*. Available at: https://www.thestar.com/news/gta/2021/01/10/why-did-ontario-covid-19-rates-surge-after-christmas-new-cellphone-mobility-data-offers-some-clues.html; Jennifer Yang and Andrew Bailey. (2021). "Cellphone data shows people are on the move again. What mobility patterns tell us about 'leaky lockdowns' and a possible third wave," *Toronto Star*. Available at: https://www.thestar.com/news/gta/2021/03/10/cellphone-data-shows-people-are-on-the-move-again-what-mobility-patterns-tell-us-about-leaky-lockdowns-and-a-possible-third-wave.html.

257 Public Health Ontario. (2020). "COVID-19 – What We Know So Far About...Social Determinants of Health," *Government of Ontario.* Available at: https://www.publichealthontario.ca/-/media/documents/ncov/covid-wwksf/2020/05/what-we-know-social-determinants-health.pdf?la=en; Elissa M Abramsa and Stanley J Szefler. (2020). "COVID-19 and the impact of social determinants of health," *Lancet Respiratory Medicine* 8(7).

6.3 - The Public Law versus Public Norms of Obtaining Health Information

At the outset of the COVID-19 pandemic, civil liberties organizations, government regulators and privacy commissioners, and academics acknowledged that privacy was not an absolute right and that privacy laws were not meant or expected to inhibit pandemic response. At the same time, privacy laws and regulations require government organizations to demonstrate that any effort to infringe upon individuals' rights was necessary and proportionate. Government's ability to obtain individuals' data over the course of the pandemic shifted because of the use of emergencies laws and elements of pre-existing health laws.

The role of consent in privacy legislation has been debated in the past decade, resulting in an understanding that the so-called 'barrier' concept of privacy—where privacy shields individuals from others—is often unaligned with the contextual applications of privacy to facilitate social and community life.[258] Nonetheless, the 'right to be let alone' has often been understood by the public as what privacy means and, as such, any intrusion past the 'barrier' is popularly regarded as constituting an infringement of rights, regardless of the rationale for the infringement (e.g., as part of a broader response to combating a health emergency).

When individuals have been presented with opportunities to use smartphone applications to potentially facilitate exposure notification, such as in the United States and Canada, they often declined to do so.[259] In practice, some residents of Canada maintained that their rights would somehow be infringed (often based on nebulous understandings

258 See generally: Christopher Parsons, Colin J. Bennett, and Adam Molnar. (2015). "Privacy, surveillance and the democratic potential of the social web," in B. Roessler & D. Mokrosinksa (Eds.), Social dimensions of privacy. Cambridge: Cambridge University Press; Priscilla Regan. (1995). *Legislating privacy: Social values and public policy.* Chapel Hill: University of North Carolina Press; Valerie Steeves. (2009). "Reclaiming the social value of privacy," in I. Kerr, V. Steeves, & C. Lucock. *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 191-208). Toronto: Oxford University Press; Helen Nissenbaum. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Redwood City: Stanford University Press; Daniel Solove. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.

259 COVID-19 Exposure Notification App Advisory Council. (2021). "Interim report on social and economic determinants of app adoption, retention and use," Innovation, Science and Economic Development Canada. Available at: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07716.html#s5.2.1; Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer. (2020). "Americans' willingness to adopt a COVID-19 tracking app: The role of app distributor," *First Monday* 25(11); Rolfe Winkler. (2020). "More States Offer Covid-19 Contact-Tracing Apps, but Adoption Is Uneven," *Wall Street Journal.* Available at: https://www.wsj.com/articles/more-states-offer-covid-19-contact-tracing-apps-but-adoption-is-uneven-11605974401. As of early July 2021, the COVID Alert application had been downloaded approximately 6,500,000 times, indicating that of the approximately 32 million Canadians over the age of 15, at most slightly more than 20% had downloaded the application (it is unclear how many individuals downloaded the application to multiple devices they may have owned, or re-downloaded the application if they had deleted it at some point). There is no available information that indicates the precise number of people who installed the application, had it in operation, or who kept it installed after downloading and configuring it.

of government actions), or they doubted the efficacy of the applications, or they lacked trust in the institutions that had developed them, and thus, they declined to volunteer even minimal amounts of personal information.[260]

In part, due to an unwillingness of individuals to share their personal information, health laws and emergency laws include provisions that enable government agencies to obtain, use, and disclose personal information without first obtaining individuals' consent. Instances where this occurs, however, are regularly viewed with skepticism. This distrust is partly informed by historical cases of mistreatments by the health and medical professions, non-consensual medical experimentation, and the repurposing of 'beneficent' technologies to accentuate social inequities, all of which led to opposition against governmental collection or obtainment of classes of personal information or modes of data collection and use.[261] While opposition to the collection of personal information during a health emergency is not new,[262] the unwillingness of some individuals, such as those in Canada, to use an application that is designed to minimally collect information and serve only to warn individuals of their potential proximity to persons who have been infected with COVID-19, speaks to the gap between the law as written and trust in the institutions empowered by those laws. Public health measures depend on the population trusting those leading the interventions, and the case of Canada's COVID Alert app suggests that trust is lacking even when it comes to the public installing privacy-protective applications on their devices, let alone on the use of the more intrusive measures that may also have been available to state agencies.

---

260 COVID-19 Exposure Notification App Advisory Council. (2021). "Interim report on social and economic determinants of app adoption, retention and use," Innovation, Science and Economic Development Canada. Available at: https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07716.html#s5.2.1; Jennie Phillips, Petra Molnar, Rebecca Babcock, Tiana Putric, Dyllan Goldstein, Laksmiina Balasubsramaniam, Alisha Gauhar, Sarah Quayyum. (2021). *Exploring User-Uptake of Digital Contact Tracing Apps - A Practitioner Guide.* York University. Available at: https://figshare.com/articles/book/Exploring_User-Uptake_of_Digital_Contact_Tracing_Apps_-_A_Practitioner_Guide_-_Full/14423861.

261 W. M. Byrd and L. A. Clayton. (2001). "Race, medicine, and health care in the United States: a historical survey," J*ournal of the National Medical Association* 93(3 Suppl); Kelly M. Hoffman, Sophie Trawalter, Jordan R. Axt, and M. Norman OliverKelly M. Hoffman, Sophie Trawalter, Jordan R. Axt, and M. Norman Oliver. (2016). "Racial bias in pain assessment and treatment recommendations, and false beliefs about biological differences between blacks and whites," *Proceedings of the National Academies of Sciences of the United States of America* 113(16); Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. (2019). "Dissecting racial bias in an algorithm used to manage the health of populations," Science 366(6464); Wanda Phillips-Beck, Rachel Eni, Josée G. Lavoie, Kathi Avery Kinew, Grace Kyoon Achan, and Alan Katz. (2020). "Confronting Racism within the Canadian Healthcare System: Systemic Exclusion of First Nations from Quality and Consistent Care," *International Journal of Environmental Research and Public Health* 17(22); Allan M. Brandt. (1978). "Racism and Research: The Case of the Tuskegee Syphilis Study," *The Hastings Center Report* 8(6).

262 Stigma is a key rationale for some members of society to resist sharing information or concealing whether they are exhibiting symptoms of disease. For more, see: American Psychological Association. (2020). "Combating bias and stigma related to COVID-19," *APA.* Available at: https://www.apa.org/topics/covid-19/bias; Alison M. O'Connor and Angela D. Evans. (2020). "Dishonesty during a Pandemic: The Concealment of COVID-19 Information," *Journal of Health Psychology* (August); John E. Pachankis, Mark L. Hatzenbuehler, Ford Hickson, Peter Weatherburn, Rigmor C. Berg, Ulrich Marcus, and Axel J. Schmidt. (2015). "Hidden from health: structural stigma, sexual orientation concealment, and HIV across 38 countries in the European MSM Internet Survey," *AIDS* 29(10).

6.4 - Health Surveillance in a Consumer Privacy World

Legislatures have continued to operate during the pandemic and have assessed the extent to which privacy laws have enabled or impeded private organizations' abilities to respond to the pandemic by undertaking their own data collection, understanding, or disclosure, and they have determined how laws have affected government responses to the pandemic. Many governments, including the Canadian government, have also had to reform laws in advance of forthcoming European Union privacy law assessments while generally updating outmoded privacy laws. In the Canadian case, Parliament introduced a consumer-focused privacy legislation, the *Consumer Privacy Protection Act* (*CPPA*) in November 2020, which would update elements of existing law (the *Personal Information Protection and Electronic Documents Act*) while also reifying other elements of it in the proposed statutory framework.

A key element of the *CPPA* would have reshaped consent-based frameworks that have operated as the publicly understood theoretical underpinning for privacy law. Specifically, while consent provisions exist, the *CPPA* would have expanded the range of activities that private organizations could undertake to collect, use, or disclose personal information without first obtaining consent. The non-consensual use or collection of personal information was not constrained by a human rights-respecting framework, so broader social interests would not have served to discipline or restrict how such non-consensual collections, uses, or disclosures were conducted by private organizations.

Operationally, the risk that legislation such as the *CPPA* poses in Canada and in other jurisdictions that adopt a similar legislative approach is that it would worsen the existing distrust in private and public bodies when it comes to their handling of individuals' personal information. Without establishing that human rights norms and principles are the lens through which privacy reforms are applied, the regulators and courts tasked with administering and adjudicating the law will be limited in how they interpret the law, for example, on the right to privacy. In a health emergency context, the absence of such a framing creates a real risk that private organizations would be challenged in obtaining the trust of the individuals whom they collect information from. As a result, the outcomes of their collections, uses, or disclosures of information may be seen as inherently problematic by the very communities whom the organization's work may be meant to benefit. More broadly, this distrust could cause policy or medical interventions to be cast into disrepute with the effect of eroding the trust that is needed between health systems and the population to mitigate the health emergencies. While a human rights framework alone cannot ameliorate all of these trust and privacy concerns, such a framework can establish more robust safeguards that can be communicated to those

whose information is collected, used or disclosed, and it could potentially alleviate some of the major risks or concerns.

If legislation similar to the *CPPA* is not grounded in human rights and if this model of legislation is ultimately deemed adequate by the European Union, it could serve as a novel way for nations to handle European residents' information. Perhaps most significantly, should legislation like the *CPPA* be adopted, it might set the course for how certain kinds of non-consensually collected health-related data can be used, potentially in variance with countries that have adopted a more robust, rights-based approach to privacy. Should this transpire, bifurcated regions might emerge where different classes of health or medical research could be conducted based on the *CPPA*'s frameworks. While bifurcated markets for privacy and different rules on how information can be used for health research are not new, the act of deliberately creating a non-rights-driven legislation at a time when rights-based legislation is becoming the global norm would stand as a highly noteworthy decision, which would likely have long-term consequences as nations around the world reform their privacy legislation on right-based grounds.

7. Conclusion

Public health crises have often led public and private organizations to marshal all of their available resources to understand and mitigate the source of the crisis. During the COVID-19 pandemic, governments and private organizations used a host of technologically mediated systems to collect information about populations and their behaviours in efforts to curb the spread of the disease. Despite privacy rights having been regarded as an impediment to states' responses to COVID-19, an analysis of Canada's response to the pandemic has revealed that privacy, health, and emergencies legislation broadly created a legislative web that enabled the collection, use, and disclosure of personal information to mitigate the virus' spread. Additionally, new legislation, the *Consumer Privacy Protection Act* (*CPPA*), introduced by Canada's federal government would have further broadened the capacity of private organizations to non-consensually collect, use, and disclose personal information in future responses to health emergencies if it had been passed into law.

This report, "Pandemic Privacy: A preliminary analysis of collection technologies, data collection laws, and legislative reform during COVID-19," showcases that, with regards to the technologies and jurisdictions examined, the processes of collecting personal information cohere with past trends while simultaneously bringing into relief the sheer influence and power of private organizations and their potential to repurpose personal information en masse. While private organizations have had significant roles in combating health emergencies for some time, the ability of technology companies to strongly influence how digital epidemiological surveillance can be conducted is arguably a notable and concerning expression of their power, regardless of the positive intentions that may have driven these corporate decisions. At the same time, the COVID-19 pandemic has showcased how contemporary digital communications technologies can be utilized in ways not previously foreseen, with the effect of expanding the aperture of how technologies may be used to conduct surveillance. At the same time, governments' information technology systems in the Canadian context have continued to be a problem. Rather than privacy legislation inhibiting government responses, it has been a failure of the government to prepare or plan for a pandemic or to learn from past lessons that have significantly stymied responses. If one of the positive elements of federalist systems of government is to enable divergent policy experiments amongst provinces, the pandemic has shown that most such experiments have largely been unsuccessful. Unfortunately, rather than develop legislation to enhance or maintain the privacy of personal information, including that which pertains to an individual's health or that is used in the service of health research, the Canadian federal government chose an approach that would further diminish the expectations of privacy that the country's residents might have regarding their personal information when it introduced the *CPPA*.

As we release this report, the COVID-19 pandemic continues around the world, including in the jurisdictions we studied. Only the earliest assessments of how collected data was analyzed or used have begun. However, in focusing principally on the collection of data, it is apparent that private actors have, in the digital space, inhibited some governments' abilities and desired objectives during a public health crisis. Governments, like those in the United States, United Kingdom, and Canada, have not been completely ineffectual, but neither were they as efficacious as they might have desired in times of crisis. Despite government efforts to prepare, legislatively-speaking, for these situations (e.g., by modifying health laws or creating emergencies legislation), the agencies responsible for pandemic response have often been uncoordinated or overwhelmed. The solution is arguably not to further diminish privacy rights, which are needed to garner public trust, but to strengthen such rights while also bolstering the capabilities of government agencies and private organizations to coordinate and properly respond to emergencies. Governments must also be able to effectively work with private actors during emergencies.

This report was motivated, in part, to assess the extent to which governmental and private actions undertaken during the course of the pandemic were truly 'unprecedented'. In the course of undertaking this assessment, we evaluated the use of data collection technologies; the supposed impediments raised by privacy rights; and the introduction of new privacy laws during the pandemic to enable data collection, use, or sharing. Ultimately, our conclusion is that while many of the technologies themselves do follow a historical trajectory, at the same time, the repurposing of communications infrastructures and personal electronic devices to combat pandemics have revealed new sources of data that future governments might use in grappling with health emergencies. The sufficiency of the privacy, transparency, and accountability systems linked to the repurposing of this personal information remain in question. At the same time, the availability of contemporary digital infrastructures has often been linked to the willingness of private companies to assist governments, showcasing the influence of private organizations in guiding what data can be collected, the conditions under which it is disclosed, and ways in which it can be used. Ultimately, while we found that the uses of technologies were linked to historical efforts to combat the spread of disease, the nature and extent of private surveillance to enable public action was arguably unprecedented.

The laws that were employed in Canada to respond to the pandemic were not new, but they were passed in the aftermath of the 2003 SARS outbreak and so were meant to ensure governments were well equipped, legislatively, to respond to health crises such as the COVID-19 pandemic. The failure of government agencies to use these laws effectively in responding to health emergencies is sadly not unprecedented, but it is similar to the ineffective response to the SARS outbreak. Privacy has not impeded government responses, meaning that future reviews, commissions, and inquiries will likely repeat the questions (and, potentially, answers) that were raised in the aftermath of the SARS outbreak.

Finally, Canada's introduction of privacy legislation during a pandemic that could have further diminished the privacy rights of Canadians was not in itself new, given trends of governments to erode the right to privacy around the world. However, if a flawed law such as the *CPPA* serves as a template for other jurisdictions, it would further set back the privacy protections applied to data that is collected, used, or disclosed without consent for health-related purposes. It remains to be seen just how such legislation might be exercised should a version of it ultimately pass into law, but if it is, such legislation could both reify existent, and arguably overly permissive, ways that private organizations can collect, use, or disclose information for health-related purposes in Canada, while also opening the door to collections, uses, and disclosures in excess of those that are contemplated in existing federal legislation. Therefore, a law that bears resemblance to the *CPPA* might enable truly unprecedented ways of handling and making use of personal information in the future. It will be up to legislators, advocacy groups, and residents of Canada alike to engage with government and private organizations to ensure that any such uses do not promote or deepen the inequities that have characterized responses to COVID-19 thus far, and it will be up to their international counterparts to assess whether Canada's legislative experiment should be followed or avoided.