Canadian Journal of Law and Technology

Volume 19 | Number 1 Article 2

1-27-2023

Digital Surveillance of COVID-19: Privacy and Equity Considerations

Elaine Gibson
Dalhousie University, Schulich School of Law

Cal DeWolfe

Ilana Luther

Digital Surveillance of COVID-19: Privacy and Equity Considerations

Elaine Gibson, Cal DeWolfe & Ilana Luther[*]

Abstract

In this paper, we examine the potentially deleterious effects of surveillance on vulnerable Canadians. A wide range of digital surveillance technologies have either been deployed or considered for deployment both in Canada and around the world in response to the international emergency created by the COVID-19 pandemic. Some of these technologies are highly effective in predicting or identifying individual cases and/or outbreaks; others assist in tracing contacts or enforcing compliance with quarantine and isolation measures. However, there are necessarily risks associated with their deployment. First are the infringements on privacy rights of citizens and groups. Second, these technologies run the risk of 'surveillance creep' in the context of their desired usage for purposes and in time frames other than for fighting a pandemic. Third, some of these technologies impact more severely on members of racialized and socioeconomically disadvantaged groups. We argue that, without addressing the impact that digital technologies have on vulnerable populations in relation to COVID-19, legislators risk deepening the inequalities that create the very conditions for transmission of the virus and that put vulnerable persons at greater risk of contracting the disease.

1. INTRODUCTION

COVID-19 (caused by the SARS-CoV-2 virus) presents a unique and significant risk not only to individuals but also to healthcare systems. We are only now experiencing the minimal initial distribution of an approved vaccine. There is no herd immunity to the virus, and it is highly contagious. As COVID-19 infection rates rise, pre-existing weaknesses in healthcare systems and in political systems generally have been laid bare.

The collection and use of data has been proposed as a partial strategic remedy. Across countries and institutions, policy-makers have implemented digital surveillance applications to reduce transmission rates and to keep economies running smoothly. In July 2020, the Federal Government launched the COVID-19 alert app (the "COVID alert app") to alert subscribers to a possible exposure. Much attention has been given to contact-tracing applications, but there are many other important electronic surveillance tools

[*] Elaine Gibson, Professor, Schulich School of Law, Dalhousie University; Cal DeWolfe, lawyer, Stewart McKelvie; Ilana Luther, former research associate, Dalhousie Health Law Institute. We would like to thank the Nova Scotia COVID-19 Health Research Funding Coalition for .for funding the research on which this article is based.

to be considered. Using data from cellphones, video, social media, wearable devices, and even wastewater, governments can implement applications that identify and track at-risk parties, predict infection patterns, and enforce quarantine measures.

There are a number of risks associated with these technologies, however, that must be addressed in considering their implementation. First, these technologies can pose risks to the privacy rights of citizens and risk instituting massive surveillance programs. Second, while some may argue that limitations on privacy may be warranted to stop the spread of an infectious disease such as COVID-19, a careful examination of the actual efficacy of these applications measured against their privacy risks is required.

Third, this analysis must take into consideration how these technologies may specifically impact marginalized groups. As some have noted, "rather than ameliorating structural inequalities, pandemic preparedness strategies sometimes contribute to them."[1] These applications run the risk of further disadvantaging already disadvantaged groups and therefore risk deepening already existing structural inequalities. Gender, race, and socioeconomic status are lenses through which public health policy must be viewed.[2] Measures that exacerbate pre-existing disadvantage cannot be lauded as effective public health strategies and may deepen the structural inequalities that make some particularly susceptible to health complications in the first place.

In the first section of this paper, we outline and discuss each of four types of digital surveillance applications—prediction, identification, contact tracing and enforcement applications. We then review these applications in terms of their adherence to privacy and constitutional principles and weigh them against considerations of ethics and efficacy. In particular, we address the impact of digital surveillance on marginalized Canadians, including the promotion of stigma, stereotype, and discrimination, the risk of "data creep" and increased police surveillance, and the risk of data marginalization.

We contribute to a much-needed weighing and analysis of these considerations by setting out the key ethical and legal challenges associated with each of the leading data-driven methods for predicting, monitoring, and reducing rates of COVID-19 infection, and we evaluate whether these applications are likely to contribute to the structural inequalities that pre-exist but may be exacerbated by the pandemic. Indeed, we argue that, even where digital surveillance applications raise few if any privacy concerns, they may serve to perpetuate existing structural inequalities if they are implemented in a way

[1] Debra Debruin, Joan Liaschenko & Mary Faith Marshall, "Social Justice in Pandemic Preparedness" (2012) 102:4 Am. J. Public Health 586 at 587. This article draws on ideas expressed in Lawrence Gostin, "Why should we care about social justice?" (2007) 37:4 Hastings Center Report 3.

[2] Françoise Baylis, Nuala Kenny & Susan Sherwin, "A Relational Account of Public Health Ethics" (2008) 1:3 J. Public Health Ethics 196 at 200-01.

that does not consider their potential disparate impact on marginalized communities.

2. DIGITAL SURVEILLANCE TECHNOLOGIES USED IN THE FIGHT AGAINST COVID-19

The COVID-19 alert app may be the best-known digital surveillance application in use in Canada today; however, there are a number of other technologies currently in use both in and outside Canada for the collection and analysis of data as a strategy in the fight against COVID-19. In Canada, we are seeing the use of data from cellphones, video, social media, wearable devices, and even wastewater to identify and track at-risk parties, predict hotspots, and enforce public health measures such as self-isolation. These may be compliant with our privacy regime, but we are also seeing the use of potentially more invasive technologies like drones and thermal imaging outside of Canada that may eventually influence our technology at home.

Below, we survey the leading digital surveillance applications being utilized in the fight against COVID-19, both inside and outside of Canada. We categorize these applications into the following four overarching categories:

(1) applications used to identify and predict hotspots and outbreaks (“predictive applications”);
(2) applications used to identify at-risk persons (“identification applications”);
(3) applications to support manual contact-tracing efforts (“contact-tracing applications” or “contact-tracing apps”); and
(4) applications to enforce quarantine and physical distancing measures (“enforcement applications”).[3]

(a) Predictive Applications

Predicting and identifying hotspots is an important public health measure. The term “predictive applications” refers to those digital surveillance applications that may serve to identify and predict COVID-19 hotspots and outbreaks. We show that, while predictive applications may be relatively non-intrusive in terms of incursions on individual privacy, poor implementation may serve to perpetuate data marginalization in ways that ultimately promote, rather than address, structural inequality.

Research that tests wastewater to identify the presence of COVID-19,[4] Google’s “COVID-19 Community Mobility Reports,” [5] and Facebook’s “Data

[3] This typology is borrowed from Uri Gasser et al, “Digital tools against COVID-19: taxonomy, ethical challenges, and navigational aid” (2020) 2:1 Lancet 425 at 426 [Gasser et al, “Digital tools against COVID-19”].

[4] Karla Renic, “COVID-19 detected in Wolfville, N.S., wastewater in experimental research”, *Global News* (27 November 2020), online: < https://globalnews.ca/news/7488765/covid-19-detected-wolfville-wastewater-research/ > .

for Good" program[6] can each be effective means of collecting aggregate data to understand where public health interventions will be most effective. Artificial intelligence such as natural language processing and machine learning are also being used in the fight against COVID-19. Big data analytics platforms such as that in use by Canadian software company, BlueDot, use artificial intelligence to analyze anonymous location data from mobile devices to assess the success of public health measures such as social distancing.[7]

Predictive applications can therefore evaluate increases or decreases in the prevalence of the virus, examine the effectiveness of already-implemented policies, and inform future policy responses by identifying and anticipating infection hotspots.[8]

Predictive applications such as those developed by Google, for example, work by collecting anonymized, aggregated data and using it to generate "flow models" (i.e., models that function based on macro-level changes in the geo-location of users).[9] The models use anonymized data to measure the number of visitors to specific categories of locations (e.g., grocery stores, parks, transit stations) every day and compare seven-day averages of current visitor levels to baseline pre-pandemic levels.[10] Insofar as high-traffic areas are loosely indicative of increased infection risk, the models' reports are capable of guiding large-scale policy responses. For instance, a report demonstrating overcrowding of particular transit stations may help a policy-maker to change or amplify messages about the need to avoid those locations.

Wastewater testing, on the other hand, works by collecting aggregate data in the form of coronavirus genetic material (RNA) and measuring the number of

[5] Joan Wong, "Countries are using apps and data networks to keep tabs on the pandemic: And also, in the process, their citizens", *The Economist* (28 March 2020), online: < https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic > ; Casey Newton, "Google uses location data to show which places are complying with stay-at-home orders — and which aren't", *The Verge* (3 April 2020), online: < https://www.theverge.com/2020/4/3/21206318/google-location-data-mobility-reports-covid-19-privacy > .

[6] Facebook has developed a "Data for Good" program which produces maps that reflect aggregate data showing how the COVID-19 virus moves amongst the population. See KX Jin & Laura McGorman, "Data for Good: New Tools to Help Health Researchers Track and Combat COVID-19" (6 April 2020), online: < https://about.fb.com/news/2020/04/data-for-good/ > [Data for Good].

[7] Geoffrey Vendeville, "U of T Infectious Disease Expert's AI Firm Now Part of Canada's COVID-19 Arsenal", *U of T News* (27 March 2020), online: < https://www.utoronto.ca/news/u-t-infectious-disease-expert-s-ai-firm-now-part-canada-s-covid-19-arsenal > .

[8] Data for Good, *supra* note 6.

[9] Google's models are based on anonymized, aggregated data from cellphone users who have turned on their phone's "location history" setting. The models only deal with macro-level data and therefore do not require the collection or storage of personal information. Google, "COVID-19 Community Mobility Reports", (25 August 2020), online: < https://www.google.com/covid19/mobility/ > .

[10] *Ibid.*

infected individuals in a given area.[11] Persons with active COVID-19 infections expel the virus in their stool, so this predictive application can measure an area's overall positivity rate even when not everyone in the area has been tested. A further appeal of this technology is its ability to detect the presence of COVID-19 up to a week prior to physical symptoms arising in individuals.[12] This research can indicate to public health officials whether rates of COVID-19 are increasing or decreasing in a particular area, and it can therefore help to evaluate public health measures, serve as an early warning signal, and indicate where more testing needs to be done. For example, after COVID-19 was detected in the wastewater of Wolfville, Nova Scotia during the month of November 2020, the provincial government set up rapid testing sites in the area and increased capacity at the town's primary assessment centre.[13]

Because many people with COVID-19 may be asymptomatic and/or may not get tested, predictive applications like wastewater testing provide important sources of information for public health officials without compromising the privacy of residents of the area under review. By identifying current and future infection hotspots, governments can hone their public health strategies, directing fortified measures toward high-risk areas and implementing a relatively 'hands-off' approach in low-risk areas. Governments can therefore simultaneously control infection rates and allow for targeted economic re-opening.

(b) Identification Applications

Identification applications analyze and interpret health-related data collected from individuals. They subsequently identify high-risk individuals and recommend testing. Unlike predictive applications, identification applications can be supported by a variety of data sources and range in intrusiveness. This category of applications ranges from non-intrusive symptom trackers all the way to highly-intrusive drone and thermal imaging applications. Symptom trackers, for example, simply ask users to volunteer information about symptoms and, depending on that information, may recommend testing.

Somewhat more intrusive applications include gate-keeping temperature checks that have, for example, been made mandatory in Canada for patrons of some grocery stores, salons, and for all air travellers.[14] The most intrusive of these applications include those currently being relied upon in a number of Asian

[11] Ottawa Public Health, "Wastewater COVID-19 Surveillance", online: < https://www.ottawapublichealth.ca/en/reports-research-and-statistics/Wastewater_COVID-19_Surveillance.aspx > .

[12] Scott Murray, "Testing Sewage to Home in on COVID-19", *MIT News* (28 October 2020), online: < https://news.mit.edu/2020/testing-sewage-for-covid-19-1028 > .

[13] Paul Palmeter, "COVID-19 wastewater testing expanding in Nova Scotia", *CBC Nova Scotia* (8 January 2021), online: < https://www.cbc.ca/news/canada/nova-scotia/covid-19-wastewater-testing-expanding-in-nova-scotia-1.5866333 > .

[14] Meghan Collie, "Can I refuse a temperature check? What to know about the COVID-19 screening tool", *Global News* (7 July 2020), online: < https://globalnews.ca/news/

jurisdictions. For example, China and South Korea are both using high-performance infrared cameras set up in airports and other public places to secretly capture thermal images of people in real time, store and analyze that information, and rapidly detect individuals with a fever.[15] Companies in China have also started pairing facial recognition technology with thermal images to ensure that this symptom-checking technology is paired with identification data.[16] In Singapore, the government is measuring the temperatures of its citizens as they enter workplaces, schools, and public transport and, on the basis of that information, is forcing certain individuals to be tested or quarantined.[17]

In Canada, a drone was being developed that could be paired with thermal camera technology to monitor for signs of COVID-19 such as high temperatures, or overt symptoms such as coughing, and used to monitor and enforce social distancing.[18] After further development, the drone was scrapped because of privacy concerns. The company adapted the technology to "monitoring kiosks," which are currently in use at universities and in the private sector around the United States.[19] The kiosks not only monitor temperature but other vital signs, such as heart rate, breathing rate, and blood oxygen saturation, that may indicate the presence of infection.[20]

The primary value of identification applications resides in their ability to carry out a preliminary form of screening in dispersed populations of patients that would not otherwise be formally tested.[21] While widespread testing is expensive and requires trained personnel, identification applications are relatively inexpensive and easy to implement.[22]

7147041/coronavirus-temperature-checks-screening/ > [*Global News,* "Can I refuse a temperature check?"].

[15] Robert Kleinman & Colin Merkel, "Digital contact tracing for COVID-19" (2020) 192:24 Can. Medical Assoc. J. 653 ["Digital contact tracing for COVID-19"].

[16] Hannah Schaller, Gabriela Zanfir-Fortuna & Rachele Hendricks-Sturrup, "Thermal Imaging as Pandemic Exit Strategy: Limitations, Use Cases and Privacy Implications" (3 June 2020), online: *Future of Privacy Forum* < https://fpf.org/2020/06/03/thermal-imaging-as-pandemic-exit-strategy-limitations-use-cases-and-privacy-implications/ > .

[17] Sarah Bridge & Adrienne Arsenault, "Meet the public health detectives working around-the-clock to stop spread of COVID-19", *CBC News* (5 April 2020), online: < https://www.cbc.ca/news/health/covid-19-contact-tracing-1.5518746 > .

[18] Dawn Stover, "Can a Pandemic Drone Help Stop the Spread of COVID-19?", *The Bulletin* (3 July 2020), online: < https://thebulletin.org/2020/07/can-a-pandemic-drone-help-stop-the-spread-of-covid-19/ > .

[19] Andrew Spence, "Grounded pandemic drone earns second chance in the US", *INDaily* (22 February 2021), online: < https://indaily.com.au/news/2021/02/22/grounded-pandemic-drone-earns-second-chance-in-the-us/ > .

[20] *Ibid.*

[21] Gasser et al, "Digital tools against COVID-19", *supra* note 3 at 426.

[22] Sera Whitelaw et al, "Applications of digital technology in COVID-19 pandemic planning and response" (2020) 2:8 Lancet 435.

(c) Contact-Tracing Applications

Contact tracing is a process that involves identifying people who have contracted or may have been exposed to COVID-19 and retrospectively "tracing" their recent interactions to identify other at-risk parties. When systematically applied, the process can identify, educate, and recommend testing and potentially quarantine for individuals who otherwise may spread the virus.[23]

Manual forms of contact tracing have been a commonly-used public health measure for reducing the spread of disease since the yellow fever epidemic of the 19th century, and possibly as far back as the bubonic plague of the 14th century.[24] However, they have already proven inferior in many jurisdictions against COVID-19. In Alberta, for instance, reports from November 2020 indicated that manual contact-tracing officers were overwhelmed by the high number of cases they had to contact trace. As a result, they were no longer able to notify people if they have been in close contact with a person who had tested positive for COVID-19 and instead only focused on contacts who were linked to "high priority" settings such as hospitals, schools, and continuing care homes.[25]

Digital applications, such as the Federal Government's COVID alert app, support contact-tracing efforts by using smartphone Bluetooth signals to measure the spatial proximity between users. If a person tests positive, an algorithm can retrospectively analyze that person's movements in relation to other users and can flag at-risk parties by virtue of their previous proximity to the infected person.[26] Contact-tracing apps can be designed to send a digital notification to parties who have been deemed high-risk and encourage them to receive testing and self-quarantine.[27]

Contact-tracing apps are also being developed specifically for use in the workplace in Canada. For example, the COVID Safety Alert app has been developed for frontline employees of the Greater Toronto Airports Authority. After an employee has entered a confirmed positive COVID-19 test result, the

[23] Public Health Ontario, "COVID-19 Contact Tracing Initiative" (2020). As cited by "COVID-19 and the Canadian Constitution", *infra* note 32.

[24] Samuel Cohn and Mona O'Brien, "Contact tracing: how physicians used it 500 years ago to control the bubonic plague", *The Conversation* (3 June 2020), online: < https://theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248 > .

[25] Joel Dryden, "Contact tracers are now overwhelmed at a critical time, infectious disease experts say", *CBC News* (5 November 2020), online: < https://www.cbc.ca/news/canada/calgary/alberta-ahs-craig-jenne-deena-hinshaw-covid-19-1.5791839 > .

[26] "Digital contact tracing for COVID-19", *supra* note 15 at 653.

[27] Gasser et al, "Digital tools against COVID-19", *supra* note 3 at 426. Two updates were made to the COVID Alert app in December 2020. The first allows users to clear their screens after receiving a negative COVID test result, and the second allows users to turn the app on and off without disabling Bluetooth. See Government of Canada, News Release, "COVID Alert app updated to serve Canadians better" (10 December 2020), online: < https://www.canada.ca/en/health-canada/news/2020/12/covid-alert-app-updated-to-serve-canadians-better.html > .

app will be able to trace contact with other devices in the workplace through a "confidential log."[28]

While the analytical function of all contact-tracing applications is essentially the same, there is an important distinction with respect to data storage between "centralized" and "decentralized" apps. Centralized applications gather anonymized data and upload it to a remote server where, once a positive test is received by a public health agency, matches are made with other contacts and warnings are issued.[29] This method of data collection allows governments to access this information to better understand the spread of the disease.[30] Jurisdictions using this method, such as Norway and France, argue that it gives them more large-scale insight into the spread of the virus.[31] These centralized apps allow for a greater possibility of follow-up than decentralized apps, aggregate analysis of consolidated data, and more effective integration with manual contact-tracing systems. If data is consolidated, human contact-tracers are able to narrow their manual efforts to parties they know have not been digitally notified; if data is not consolidated, human tracers cannot discern who has and has not been notified by the app and must therefore continue manual tracing efforts even if they are duplicative.[32]

In contrast, decentralized applications store all data internally, within a user's phone.[33] Therefore, any warnings that a user receives are private. Jurisdictions using decentralized apps, such as the Canadian federal government, argue that a trade-off in analytical utility is justified if it affords users more privacy.[34] The global push for decentralized apps has been facilitated by an

[28] Greater Toronto Airports Authority, "Greater Toronto Airports Authority deploys COVID Safety Alert devices for frontline employees as part of innovative new program", *Cision* (4 March 2021), online: < https://www.newswire.ca/news-releases/greater-toronto-airports-authority-deploys-covid-safety-alert-devices-for-frontline-employees-as-part-of-innovative-new-program-803136094.html > .

[29] Cristina Criddle and Leo Kelion, "Coronavirus contact-tracing: World split between two kinds of apps", *BBC News* (7 May 2020), online: < https://www.bbc.com/news/technology-52355028 > ["Coronavirus contact-tracing"]. For example, Indian contact-tracing app, Aarogya Setu. France, the United Kingdom, and Italy favour centralization where their public health agencies receive notices instantly. See Samira Davalbhakta et al, "A Systemic Review of Smartphone Applications Available for Corona Virus Disease 2019 (COVID19) and the Assessment of their Quality Using the Mobile Application Rating Scale (MARS)," (2020) 44:164 J. Medical Systems 163.

[30] Teresa Scassa, Jason Millar & Kelly Bronson, "Privacy, Ethics, and Contact-Tracing Apps" in Colleen Flood et al, eds, *Vulnerable: The Law, Policy and Ethics of COVID-19* (Ottawa: University of Ottawa Press, 2020) 265 at 269 ["Privacy, Ethics and Contact-Tracing Apps"].

[31] "Coronavirus contact-tracing"*, supra* note 29.

[32] Lisa M Austin et al, "Test, Trace, and Isolate: Covid-19 and the Canadian Constitution" (22 May 2020), *Osgoode Legal Studies Research Paper* at 12, online: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 3608823 > ["Covid-19 and the Canadian Constitution"].

[33] *Ibid.*

Apple-Google joint venture[35] that has allowed governments to access some features of these companies' iOS and Android mobile operating systems.[36]

The tension between centralized and decentralized data storage is layered with a second tension between voluntary and involuntary participation. Several countries, including South Korea and China, have forced contact-tracing regimes on cellphone users, but such involuntary regimes have been widely rejected in North America and Europe.[37]

All methods of digital contact tracing have distinct advantages of scale and speed over manual contact-tracing efforts. In November 2020, it was reported that the federal COVID app had been downloaded 5.2 million times and used to trace and notify contacts of approximately 4,200 people who tested positive for the disease.[38] Digital contact tracing can also provide increased anonymity for index patients. While neither digital nor manual contact tracing informs contacts of the infected patient's name, manual contact tracing often functions by the index patient providing names of contacts to a tracing officer. Therefore, insofar as there must be some form of relationship between index patients and manually traced contacts, the latter can often infer who the former is. Digital tracing does not require that the index patient have any specific knowledge of the contacts, so the room for inference is greatly reduced.[39]

[34] Saltwire Network, Editorial, "Are you up for the COVID contact-tracing app?", *Chronicle Herald* (4 August 2020), online: < https://www.thechronicleherald.ca/opinion/local-perspectives/editorial-are-you-up-for-the-covid-contact-tracing-app-481239 > [Chronicle Herald, "Are you up for the COVID contact-tracing app?"].

[35] The vast majority of cellphones operate on either Apple's iOS operating system or Google's Android operating system. The Apple-Google joint venture was formed specifically in response to the COVID-19 pandemic with a view toward facilitating government contact-tracing efforts. The purpose of the joint venture has been to develop and implement an anonymized, decentralized contact-tracing system that would work across both iOS and Android operating systems on an opt-in basis. Matt O'Brien, "Apple, Google release their joint technology for pandemic-tracking apps", *CBC News* (20 May 2020), online: < https://www.cbc.ca/news/technology/apple-google-covid-app-1.5577166 > .

[36] "Coronavirus contact-tracing", *supra* note 29.

[37] Aaron Holmes, "South Korea is relying on technology to contain COVID-19, including measures that would break privacy laws in the US — and so far, it's working", *Business Insider* (2 May 2020), online: < https://www.businessinsider.com/coronavirus-south-korea-tech-contact-tracing-testing-fight-covid-19-2020-5 > [*Business Insider,* "South Korea is relying on technology to contain COVID-19"].

[38] Robson Fletcher, "Alberta Reveals its COVID-19 app has been used to trace only 20 cases in 6 months", *CBC News* (16 November 2020), online: < https://www.cbc.ca/news/canada/calgary/alberta-covid-app-abtracetogether-apple-ios-functionality-issues-1.5799537 > .

[39] It is important that the identity of index patients is protected as much as possible. The stigma associated with being identified as COVID-19 positive can contribute to anxiety and depression, and researchers have expressed concern that, if unchecked, stigma may derail the public health strategies and political investments made to combat the COVID-

(d) Enforcement Applications

Enforcement applications involve real-time monitoring of whether symptomatic patients or flagged individuals are complying with self-isolation and quarantine restrictions. The COVID Safety Alert device, for example, is not only a contact-tracing app, but it is also an enforcement app. The device enforces physical distancing requirements by buzzing and flashing when an employee is less than two meters away from another employee wearing the device.[40]

In South Korea and Taiwan, a mandatory smartphone app tracks anyone entering the country in order to help enforce two-week self-quarantine measures.[41] South Korea was, in addition, initially planning to outfit its own self-quarantining citizens with mandatory tracking bracelets but made this measure optional after receiving human rights complaints.[42]

Some identification applications, such as thermal cameras in use in China, are able to sense whether or not a person is wearing a mask.[43] Paired with other technology such as drone technology, these can be used to enforce PPE use.

While the specific mechanism used to enforce restrictions varies, all enforcement technologies overlap in using a data-driven method to ensure that infected individuals remain isolated from others.

Quarantine, self-isolation, and social distancing measures, if properly executed, are among the most effective methods available for slowing the spread of viral pathogens.[44] Historically, however, compliance has been an issue with respect to quarantining and self-isolation measures. For example, a 2011 cross-sectional study on H1N1 examined quarantining practices in Australia and found that, while 90% of respondents reportedly understood what they were meant to do during quarantine, only 55% reported compliance.[45] Data-driven enforcement measures strengthen compliance with quarantine and self-isolation, thereby enhancing their function as a primary method for lowering viral transmission.

19 pandemic. See Prince Peprah & Razak Gyasi, "Stigma and COVID-19 crisis: A wake-up call (Letter to the Editor)" (2020) 36:1 Intl J. of Health Planning & Management 215.

[40] Greater Toronto Airports Authority, *supra* note 28.

[41] *Business Insider,* "South Korea is relying on technology to contain COVID-19", *supra* note 37; Yimou Lee, "Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring", *Reuters* (20 March 2020), online: < https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK > .

[42] *Business Insider,* "South Korea is relying on technology to contain COVID-19", *ibid.*

[43] Schaller, *supra* note 16.

[44] Anne Kavanagh et al, "Sources, perceived usefulness and understanding of information disseminated to families who entered home quarantine during the H1N1 pandemic in Victoria, Australia: a cross-sectional study" (2011) 11 BMC Infectious Diseases 2.

[45] *Ibid.*

There are several advantages to these four types of digital surveillance technologies in terms of promoting individual and public health; however, they each raise concerns in relation to privacy and efficacy. Below we outline some of the *Charte*r and privacy concerns that these technologies may raise. Beyond privacy, we also explore the negative effects that these technologies may have for marginalized communities in expanding surveillance, stigmatization, and data marginalization.

3. PRIVACY AND EQUITY CONSIDERATIONS INVOLVED WITH DIGITAL TECHNOLOGIES

(a) Legislation, the Charter, and Privacy Issues

In Canada, the collection, use and disclosure of personal information is regulated by applicable privacy legislation depending on whether that personal information is health information, whether it is being collected, used, or disclosed by the private or public sector, and whether the relevant actions are in relation to federal or provincial jurisdiction.

Where personal health information is collected, used, and/or disclosed to or by custodians, as defined in the applicable Act, the privacy of that information is regulated by provincial health information legislation. While canvassing all provincial health information legislation is beyond the scope of this article, it is sufficient to point out that these Acts are concerned with giving individuals control over how information that can identify them is collected, used, and disclosed by another. Therefore, where data is de-identified, such as with predictive applications (that analyze aggregate wastewater or cellphone data, for example), these will likely raise little in the way of privacy concerns. Where individuals are using identification applications like symptom trackers to collect their own data and this data is not being collected, used, or disclosed by a public or private party, it is unlikely that any privacy legislation will apply.

Where use, collection, and disclosure of personal information is sought by another entity such as the government or public health authorities, however, health information legislation stipulates a requisite level of control that people must have over their information in order to adequately protect privacy. For example, in Nova Scotia, where the province is involved in collecting, using, and disclosing information that is collected through the applications set out above and is capable of identifying individuals, either on its own or in combination with other information, the *Personal Health Information Act* (the "*PHIA*") will apply.[46] This means that, at minimum, a custodian will have to obtain the knowledgeable implied consent of the individual if the province would like to collect, use, or disclose the individual's personal health information from these

[46] S.N.S. 2010, c. 41. Pursuant to s. 3(f), a regulated health professional, the Minister of Health and Wellness, and a health authority as defined in the *Health Authorities Act* are all considered custodians under the *Act*.

applications.[47] A more exacting form of consent in the form of "express consent" will be required where the province has collected identifying personal health information and then chooses to disclose this information to a non-custodian,[48] including a non-custodian researcher.[49]

While the *PHIA* calls for knowledgeable implied consent, providing for express consent and ensuring data is de-identified to the greatest extent possible is most privacy protective. For example, with the COVID alert app, the federal government has indicated that nothing will be shared without the express permission of the user.[50] Even then, there are extra privacy protections required. If the user gives permission to share their positive diagnosis with the app, only a random code will be shared with a central server operated by the Government of Canada.[51] The app then gives the user the ability to enter details voluntarily to narrow down when you were likely the most infectious.[52]

Although some digital surveillance applications may be found to be compliant with privacy legislation, they may still raise concerns. For example, the Federal, Provincial and Territorial Privacy Commissioners have released a Joint Statement (the "Joint Statement") of principles that should guide the collection, use, and/or disclosure of personal health information obtained by contact tracing and digital apps, given the fact that the digital realm poses a unique challenge to privacy legislation in Canada.[53] These principles help to ensure best practices in protecting privacy in the context of digital applications,

[47] Section 12.

[48] Subsection 43(a).

[49] Subsection 43(f). This subsection provides that express consent is required if a custodian under the Act discloses personal health information to a researcher unless section 57 of PHIA applies. Section 57 sets out the terms under which research may be conducted with personal health information that has been disclosed without the express consent of the person. These include approval of the research by a research ethics board that determines that consent is not required, satisfaction that it is impractical to obtain consent, and satisfaction that the research cannot be conducted without using the personal health information. The health information must be limited, de-identified as much as possible, and used in a manner that ensures confidentiality. The custodian must also inform the review officer of the disclosure. Finally, the custodian and researcher must enter into an agreement as provided for by section 60 of the PHIA.

[50] Government of Canada, "Download COVID Alert today", online: < https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html?utm_campaign = hc-sc-covidalertapp-20-21&utm_medium = sem&utm_source = ggl&utm_content = ad-text-en&utm_term = %2Bcovid%20%2Bapplication&adv = 2021-0052&id_campaign = 12067433898&id_source = 115886878506&id_content = 491285390851 > .

[51] *Ibid.*

[52] *Ibid.*

[53] Office of the Privacy Commissioner of Canada, Joint Statement by Federal, Provincial, and Territorial Privacy Commissioners, "Supporting public health, building public trust: Privacy principles for contact tracing and similar apps" (7 May 2020), online: < https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/ > .

and they ensure that these practices are instituted alongside democratic values such as transparency and accountability so that public trust is maintained.

In particular, the Joint Statement highlights that governments must be transparent about why and how it is using, collecting and disclosing personal health information and must be clear about where the information will be stored and securely retained.[54] As well, it was recommended that governments should "develop and make public an ongoing monitoring and evaluation plan concerning the effectiveness of these initiatives," including oversight by an independent third party such as by a privacy commissioner's office.[55] Finally, the privacy commissioners recommended that governments institute strong legal and technical security measures, including strong safeguards in contracts with developers that ensure that non-authorized parties do not have access to the data, and that the data will not be used for anything other than the intended public health measures.[56]

Aside from compliance with privacy legislation, the use of digital surveillance technologies must not violate protections guaranteed under the *Charter of Rights and Freedoms*.[57] In Canada, sections 7 and 8 of the *Charter* respectively protect individuals against government intrusions on bodily integrity and unreasonable search and seizure. Section 8 of the *Charter* provides layered protection against state intrusions on "territorial," "personal," and "informational" privacy under its prohibition against unreasonable search and seizure.[58] Austin and colleagues point out that many of the digital surveillance applications that are currently in use abroad would likely violate protections on informational privacy in Canada.[59]

In particular, applications which track a person's movements in public spaces or which otherwise reveal "core biographical information," such as a person's congregating points and social contacts, would likely give rise to an informational privacy claim. This risk is heightened for applications that deal with centralized, non-aggregated data (for instance, predictive applications are much more likely to be compliant than certain identification or enforcement applications).

The same digital surveillance applications that would be scrutinized under section 8 of the *Charter* would similarly be at risk of violating the privacy interests that are protected under section 7, which safeguards state intrusions on "life, liberty, and security of the person." In *R. v. Mills*, the Supreme Court of

[54] *Ibid.*

[55] *Ibid.*

[56] *Ibid.*

[57] *Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982, 1982, c. 11, s. 8 ["*Charter*"].

[58] "COVD-19 and the Canadian Constitution"*, supra* note 33, s. 8; *R. v. Tessling*, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352 (S.C.C.) at paras. 20-23.

[59] "COVID-19 and the Canadian Constitution", *ibid* at 10-11.

Canada embedded a privacy analysis based on section 8 considerations within analysis of a principle of fundamental justice.[60] Although the case law remains undeveloped, the *Mills* decision indicates that section 7 also protects privacy as an aspect of liberty or security of the person.

Of course, government measures that lead to *prima facie Charter* violations may be found to be justified under section 1, which imposes "reasonable limits" on the protected rights and freedoms. Austin and colleagues caution that it is nearly impossible to predict what an adequate section 1 justification would look like in the context of digital surveillance, since justifications often turn on specific facts.[61] They do acknowledge, however, that these surveillance applications are being used for positive purposes such as reducing the need for more restrictive measures such as quarantine. Self-isolation and quarantine measures uniquely disadvantage individuals who suffer from pre-existing inequalities and who face challenges affecting their security of the person. Austin and colleagues point specifically to individuals who suffer from "mental health challenges, abusive relationships, or other vulnerabilities" as well as those who are "in situations of poverty" or live in "precarious housing."[62] Because surveillance measures serve social justice goals (and promote so-called "*Charter* values") by standing to reduce the burden on these individuals, courts are more likely to find them *Charter*-compliant.

Regardless of whether these technologies are found *Charter*-compliant, or raise few privacy concerns, they may serve to perpetuate discrimination and inequality in their implementation unless policy-makers are attendant to the ways in which the use of these technologies can have a disparate impact on marginalized populations. Below, we consider the various ways that the use of these technologies can serve to promote structural inequalities.

(b) Expanding Surveillance and Stigmatization

The pervasive use of surveillance data to fight the pandemic has also been linked to concerns regarding the normalizing of surveillance.[63] Some scholars have pointed to the power of contact-tracing apps to normalize the presence of surveillance in our lives, including outside the public health sphere, and the effect that this may have in expanding the power of both the state and private corporations going forward after the end of the pandemic.[64] The expansion of surveillance by both the public and private sectors will have an especially adverse

[60] *R. v. Mills*, 1999 CarswellAlta 1055, 1999 CarswellAlta 1056, [1999] 3 S.C.R. 668 (S.C.C.) at para. 88.

[61] "COVID-19 and the Canadian Constitution", *supra* note 32 at 12.

[62] *Ibid.*

[63] Mirca Madianou, "A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic" (6 August 2020) Social Media & Society, online: < https://journals.sagepub.com/doi/full/10.1177/2056305120948168 > .

[64] *Ibid.*

effect on marginalized groups, who tend to face higher rates of surveillance and criminalization overall.[65]

With respect to the use of digital surveillance applications in the private sphere, some private corporations have developed their own contact-tracing apps for use when employees return to in-person workplaces, such as the COVID Safety Alert in use by the Greater Toronto Airport Authority.[66] Some companies are using identification technologies such as thermal scanners to scan employees before they enter the workplace.[67] As well, there are reports of private companies such as Amazon utilizing enforcement applications, including an artificial intelligence assistant called a "distance assistance" to enforce social distancing in the workplace.[68]

The use of digital surveillance apps in the private sector may pose particular privacy considerations. The Privacy Commissioner of Canada has recently raised concerns over the ability of Canada's privacy regime to appropriately provide for Canadians' meaningful control over their personal information when it is collected and used by a public-private partnership—even where it is used for a public purpose. The Commissioner noted that numerous COVID-19-related initiatives involve public-private partnerships that rely on the private sector legal authority for obtaining consent. The effect is that, even though the initiative involves the public sector, there is no policy requirement for government institutions to ensure that consent was "meaningfully obtained."[69]

Failing to insist upon strong protections to ensure the active and meaningful participation of individuals in the use, collection, and disclosure of their personal information will further normalize the expansion of surveillance. As applications are rolled out across the private sphere, allowing companies to insist upon their use without obtaining meaningful consent could undermine the legitimacy of an

[65] See e.g. Virginia Eubanks, "The Digital Poorhouse", *Harper's Magazine* 336:2012 (January 2018) 11.

[66] Siemens and PriceWaterhouseCoopers have also developed their own apps for the workplace, see John Revill, "Siemens to roll out flexible working app for 100,000 staff", *Chronicle Herald* (23 July 2020), online: < https://www.thechronicleherald.ca/business/reuters/siemens-to-roll-out-flexible-working-app-for-100000-staff-476601/ > ; Kif Leswing, "Companies could require employees to install coronavirus-tracing apps like this one from PwC before coming back to work", *CNBC* (6 May 2020), online: < https://www.cnbc.com/2020/05/06/pwc-is-building-coronavirus-contact-tracing-software-for-companies.html > .

[67] Jason Beaubien, "More Companies are Using Technology to Monitor for Coronavirus in the Workplace", *NPR* (13 October 2020), online < https://www.gpb.org/news/2020/10/13/more-companies-are-using-technology-monitor-for-coronavirus-in-the-workplace > .

[68] *Ibid.*

[69] Privacy Commissioner of Canada, *Privacy in a Pandemic: 2019-2020 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act* (Ottawa: Privacy Commissioner of Canada, 2020) (Released 8 October 2020) at 10, online < https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/ > [Privacy Commissioner Annual Report].

individual's expectation of privacy. In doing so, it could ultimately serve to perpetuate the idea that the collection, use, and disclosure of personal information is a normal part of participating in either the private or public sphere. When we consider that some employers may prevent some employees who do not use an app from returning to work, or some businesses may deny access to individuals who cannot demonstrate that they are using surveillance applications, this obligatory collection, use, and disclosure of personal information will further normalize surveillance.

The normalizing of surveillance in the private sphere is only half the concern, however. The other half of the story is that surveillance data could be used to help police or other government agencies investigate non-health-related matters. Indeed, some countries have developed surveillance programs that, much like many counter-terrorist programs, feature intergovernmental data integration as a fundamental aspect of the platform.[70] Unlike classic infectious disease surveillance, which collects targeted information pertaining to human disease, these programs integrate dispersed data on humans, animals, and the environment collected by multiple government agencies.[71] So-called "data creep" is not a by-product of these programs, but part of their very design.

Such a system is not currently in place in Canada, but there is still a risk that public health data may be abused, particularly by law enforcement. For example, the Information and Privacy Commissioner of Newfoundland and Labrador has admitted that, while he is optimistic that health-related data will not be inappropriately shared, a centralized database would be "of interest" to law enforcement.[72] Indeed, law enforcement has inappropriately crossed privacy lines before. In the case of *Vancouver Police Department v. BC Centre for Excellence,* the Vancouver Police Department attempted to obtain private medical records from the Centre, which was responsible for keeping private records of "almost all known HIV-positive people in the province."[73] The BC provincial court rebuked the Police Department.

In Ontario, the provincial government terminated police access to a COVID-19 database after a group of human rights advocates in that province raised concerns over the practice.[74] Ontario police conducted 95,000 searches of the database, with 40% of those searches administered by the Thunder Bay police.[75]

[70] Gasser et al, "Digital tools against COVID-19", *supra* note 3 at 429.

[71] Amanda Kim and Sangwoo Tak, "Implementation System of a Biosurveillance System in the Republic of Korea and Its Legal Ramifications" (2019) 17:6 J. of Health Security 463.

[72] Ryan Cooke, "Can digital contact tracing be done without creeping surveillance? Privacy commissioner is hopeful", *CBC News* (28 April 2020), online: < https://www.cbc.ca/news/canada/newfoundland-labrador/michael-harvey-digital-contact-tracing-covid-19-1.5547425 > .

[73] Joven Narwal, "Police should not have access to data from coronavirus contact tracing apps", *The Conversation* (22 June 2020), online: < https://theconversation.com/police-should-not-have-access-to-data-from-coronavirus-contact-tracing-apps-140218 > [Narwal].

Racialized persons were overrepresented among the people searched.[76] The database was initially created to protect emergency first responders from unknowingly entering a high-risk environment. Police officers claimed that they required access to the information for the same reason. The reality, however, is that members of racialized groups are already disproportionately targeted by police—and, therefore, allowing police officers access to health information increases the risk of human rights violations and creates an even greater risk to the security and liberty of these groups.[77] Expansion of surveillance into the private sphere may serve to augment the power of the state to patrol the lives of members of marginalized groups.

The expansion of surveillance may not only promote discrimination against individuals in marginalized groups, but against these groups as a whole. For example, some worry that the collection of population-specific data could lead to stigmatization of already-disadvantaged racialized or socioeconomic groups.[78] Without providing context and explaining how structural inequalities,[79] for example, may lead to higher infection rates in some communities, this information could lead to a stigmatization of those communities.[80] In turn, this stigmatization could lead to discrimination and even physical violence—such

[74] Canadian Press, "Ontario ends police access to COVID-19 database after legal challenge", *CBC News* (17 August 2020), online: < https://www.cbc.ca/news/canada/toronto/covid-ont-police-database-1.5690220 > .

[75] Sean Fine, "Court challenge launched over Ontario disclosure of COVID-19 testing with police", *The Globe and Mail* (16 July 2020), online: < https://www.theglobeandmail.com/canada/article-court-challenge-launched-over-ontario-disclosure-of-covid-19-testing/ > ; Canadian Press, *ibid.*

[76] Kelly Grant, "Data shows poverty, overcrowded housing connected to COVID-19 rates among racial minorities in Toronto", *The Globe and Mail* (2 July 2020), online: < https://www.theglobeandmail.com/canada/toronto/article-data-show-poverty-overcrowded-housing-connected-to-covid-19-rates/ > .

[77] *Ibid.*

[78] Gasser et al, "Digital tools against COVID-19", *supra* note 3 at 429.

[79] Inequalities in access to healthcare, overrepresentation of BIPOC workers in precarious employment and inequality in living conditions are just three structural factors that can lead to higher rates of infection in racialized communities. Persons from these communities are more likely to be frontline workers who are not able to work from home and are more likely to live in high density neighbourhoods with lower air quality, for example: see VAW Learning Network, "'More Exposed & Less Protected' in Canada: Racial Inequality as Systemic Violence During COVID-19", online: *Western University* < http://www.vawlearningnetwork.ca/docs/Systemic-Racism-Covid-19-Backgrounder.pdf > .

[80] This was a concern in the African Nova Scotian community of North Preston and was the impetus behind the project "Don't Count Us Out!" by OmiSoore Dryden, on developing a health registry collecting data to address racial inequities in health in Nova Scotia. See Chelsy Mahar, "Researchers work with African Nova Scotian communities in Dartmouth on health registry", *The Signal* (12 February 2021), online: < https://signalhfx.ca/researchers-work-with-african-nova-scotian-communities-in-dartmouth-on-health-registry/ > [African Nova Scotian health registry].

as, for instance, the recent rise in attacks on Americans of Asian descent—fuelled by public data showing high infection rates amongst this demographic.[81]

This stigma and discrimination in turn perpetuates negative health outcomes in marginalized communities. The Centers for Disease Control and Prevention ("CDC") has underscored that stigma—which is caused by racism, stereotype, and ultimately by inaccurate and incomplete information—can have a significant negative impact on the mental health of stigmatized groups and the communities they live in.[82] The physical health of stigmatized groups can be similarly impacted. Fear of being labelled often causes at-risk populations to avoid seeking care, or to not seek care until their symptoms become unmanageable.[83] Finally, certain populations may be under-resourced if there is a general societal view that the group is 'undeserving' of state support.

(c) Data Marginalization

While over-exposure of certain groups to surveillance can have adverse effects, so can "data marginalization"[84] or "data poverty";[85] that is, the practice of excluding marginalized groups from public health data. Some public health scholars have stressed the importance of improving data collection and analysis in order to reveal the existence and dire consequences of "health inequalities."[86]

In order to understand the way that socioeconomic position affects health, we must see the interplay of a complex web of social, political and economic inequalities. In Canada, long histories of colonialism and racial discrimination have rendered First Nations peoples at higher risk of contracting COVID-19 and their communities less able to manage the crisis.[87] An integral step to understanding how health inequality is promoted is by collecting data that accounts for socioeconomic position so that we can understand how gender

[81] Gasser et al, "Digital tools against COVID-19", *supra* note 3 at 429.

[82] Centers for Disease Control and Prevention, Media Release, "Coronavirus Disease 2019 (COVID-19): Reducing Stigma" (June 11, 2020), online: < https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/reducing-stigma.html > .

[83] Debra Bruns, Nina Kraguljac & Thomas Bruns, "COVID-19: Facts, Cultural Considerations, and Risk of Stigmatization" (2020) 31:4 J. of Transcultural Nursing 326.

[84] Michele Gilman & Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization" (2020) 42 NYU Rev. L. & Soc. Change 253 ["Surveillance Gap"].

[85] Daniel Castro, "The Rise of Data Poverty in America" (10 September 2014), online: *Center for Data Innovation* < https://www2.datainnovation.org/2014-data-poverty.pdf > .

[86] Lawrence Gostin & Eric Friedman, "Health Inequalities" (July-August 2020) Hastings Center Report, online: < https://onlinelibrary-wiley-com.login.ezproxy.library.ualberta.ca/doi/epdf/10.1002/hast.1108 > .

[87] Anne Levesque & Sophie Theriault, "Systemic discrimination in Government Services and Programs and its Impact on First Nations People During the COVID-19 Pandemic" in Colleen Flood et al, eds, *Vulnerable: The Law, Policy and Ethics of COVID-19* (Ottawa: University of Ottawa Press, 2020) 381.

discrimination, racism, and classism are contributing to negative health outcomes. Data which fails to reveal how structural inequalities affect the health of certain groups serves to reinforce this health inequality.[88] This was recently recognized, for example, by the Senate in its calls for race-based data on Canadian medical assistance in dying requests.[89]

While the collection and analysis of data early on in the pandemic revealed the racial disparity in COVID-19 infection and death rates,[90] this data has been criticized as incomplete, and researchers have stressed the urgent need to improve data collection and analysis to reveal the "unequal burden" of COVID-19 borne by marginalized populations.[91] Without this data, the fact that racialized communities are suffering the most severe effects of the pandemic and seeing the fewest resources to combat it will be obscured. Public health data will not only affect our understanding of how specific groups are experiencing the pandemic, but it will affect how COVID-specific resource distribution and social support programs are administered. There are numerous examples of how data marginalization has had real consequences for policy-making in North America. Census data, for instance—which has been notoriously inaccurate for racial minorities and homeless populations—has led to racist and classist methods of resource allocation in the United States, including the under-funding of public transportation and of various forms of social programming and environmental initiatives.[92]

In some respects, data marginalization has already perpetuated the unequal distribution to communities most in need. Many marginalized Canadians have already faced logistical and administrative barriers to collecting pandemic

[88] See Kwame McKenzie, "Toronto and Peel have reported race-based and socio-economic data — now we need action" (13 August 2020), online: *Wellesley Institute* <https://www.wellesleyinstitute.com/healthy-communities/toronto-and-peel-have-reported-race-based-and-socio-demographic-data-now-we-need-action/>. There are currently several projects looking at collecting race-based data in Nova Scotia. On the impact of the COVID-19 pandemic on African Nova Scotian communities, see "Study aims to understand impact of COVID-19 on Nova Scotia's Black communities", *CBC News* (12 January 2021), online: <https://www.cbc.ca/news/canada/nova-scotia/prestons-pandemic-covid-19-research-dalhousie-university-ingrid-waldron-1.5870432>; African Nova Scotian health registry, *supra* note 80.

[89] The concern here is that health inequalities will induce members of marginalized groups to end their lives prematurely. See Joan Bryden, "Senators demand race-based data on who requests, receives MAID in Canada", *Toronto Star* (11 February 2021), online: <https://www.thestar.com/politics/2021/02/11/senators-extend-sitting-hours-as-court-deadline-for-maid-bill-looms.html>.

[90] Steven Coughlin et al, "COVID-19 Among African Americans: From Preliminary Epidemiological Surveillance Data to Public Health Action" (August 2020) 110:8 Am. J. Public Health 1157.

[91] *Ibid*; Jarvis Chen and Nancy Krieger, "Revealing the Unequal Burden of COVID-19 by Income, Race/Ethnicity, and Household Crowding: US County Versus Zip Code Analyses" (1 Jan 2021) 27:1 J. Public Health Management & Practice S43.

[92] "Surveillance Gap", *supra* note 84.

benefits and supports.[93] Some had not heard of the benefits by virtue of their living circumstances; others did not have internet access or were not computer-literate.[94] The very structure of available benefits excluded some members of these populations. For example, contact-tracing applications that rely on internet access or up-to-date cellphone technology risk leading policy-makers to underestimate infection rates amongst disadvantaged populations, which in turn reinforces inadequate and discriminatory policy responses.

In sum, policy-makers must be attuned to the negative effects that the implementation of these applications may have on marginalized populations, or they risk reinforcing the very vulnerabilities which may perpetuate the spread and harmfulness of the disease to begin with.

4. EVALUATING THE POTENTIAL NEGATIVE EFFECTS OF DIGITAL TECHNOLOGIES ON MARGINALIZED COMMUNITIES

In Canada, racialized and socioeconomically disadvantaged groups have been disproportionately affected by COVID-19, and relief measures have been under-delivered.[95] As we have seen during the pandemic so far, members of marginalized groups are more likely to become infected and even to die from the virus due to effects of structural inequality and systemic discrimination.[96] Research has found that "poverty, inequality, and social determinants of health create conditions for the transmission of infectious diseases, and existing health disparities or inequalities can further contribute to unequal burdens of morbidity and mortality."[97] Members of marginalized groups are least likely to receive information, may receive little financial support, face difficulties in accessing public health advice, and "are the least able to self-isolate and social distance."[98] In implementing digital surveillance technologies to combat COVID-19, it is important not to perpetuate this self-reinforcing cycle.

[93] McKenzie, "Remembering the Forgotten", *infra* note 95.

[94] *Ibid.*

[95] Kwame McKenzie, "COVID-19: Remembering the Forgotten" (2020), online: *Wellesley Institute* <https://www.wellesleyinstitute.com/healthy-communities/remembering-the-forgotten> ["McKenzie, Remembering the Forgotten"]; Kate McGillivray, "Ontario's homeless 5 times more likely to die of COVID-19, study finds", *CBC News* (12 January 2021), online: <https://www.cbc.ca/news/canada/toronto/ontario-s-homeless-5-times-more-likely-to-die-of-covid-19-study-finds-1.5869024>.

[96] *Ibid.*

[97] Sandra Crouse Quinn & Supriya Kumar, "Health Inequalities and Infectious Disease Epidemics: A Challenge for Global Health Security" 12:5 Biosecurity & Bioterrorism: Biodefense Strategy, Practice and Science 263; Max Fisher & Emma Bubola, "As Coronavirus Deepens Inequality, Inequality Worsens its Spread", *New York Times* (15 March 2020), online: <https://www.nytimes.com/2020/03/15/world/europe/coronavirus-inequality.html>.

[98] McKenzie, Remembering the Forgotten, *supra* note 95.

By evaluating the four types of digital technologies currently in use to combat COVID-19, we will show that if policy-makers are solely attentive to their privacy implications, they will miss the effects that these technologies may have on the surveillance, stigmatization, or underrepresentation of marginalized groups, thereby perpetuating overarching structural and health inequalities. Indeed, digital technologies that use aggregate, anonymized data will not likely raise privacy concerns, but if data is collected and analyzed without attention to the ways in which hotspots or outbreaks may be caused by the effects of structural inequality, the data will serve to obfuscate these inequalities, leaving marginalized populations vulnerable to infection.

Having said this, the negative effect of surveillance is obviously tied to privacy in the sense that the consequences for individuals may be greater where their personal information can be mined and exploited. Furthermore, where individuals are not able to participate in the collection, use, and disclosure of their personal information, this can raise grave ethical concerns. For example, many forms of identification applications that identify the presence of symptoms of the virus, such as drones and thermal cameras, may be used without consent (consider the above-noted cases of China and Singapore). They are therefore ethically problematic. These identification apps raise privacy concerns, as health-related data is potentially exposed to multiple parties and in many cases is stored in a centralized location, leaving the data to potentially be abused by hackers or by the state. This data can then be used by the state to place restrictions on the individual that interfere not only with their right to privacy, but also their right to liberty.

Aside from the state, as discussed above, we are seeing the use of technologies such as enforcement (i.e., to maintain social distancing) and contact-tracing applications in workplaces as a requirement of entering and engaging in the workplace and therefore of employment. These requirements extend this digital surveillance into more and more spheres of an individual's life.

In Canada, the constitutional shortcomings of certain contact-tracing applications have been well documented. Austin and colleagues, for example, argue that an app that collects more information than needed and that fails to protect this information with adequate safeguards may run afoul of section 7 of the *Charter* because the app may expose personal information to persons and for purposes unconsented-to by the user.[99] As well, the Privacy Commissioner of Canada has raised concerns in his annual report that third parties may force Canadians "to disclose information as to their use of the app, including any exposure notifications."[100]

While these applications raise privacy concerns in general, they raise additional concerns for marginalized groups. For example, these highly intrusive applications are especially pernicious in terms of expanding surveillance. While it

[99] "Covid-19 and the Canadian Constitution", *supra* note 32 at 11.

[100] Privacy Commissioner Annual Report, *supra* note 69 at 10.

is questionable whether in many cases these applications would even be effective to address the COVID-19 pandemic,[101] when combined with predictive applications that use data such as wastewater and cellphone data to predict outbreaks and hotspots, it is easy to see how they may be placed in greater use in areas with higher rates of infection. These may correlate to lower socioeconomic areas and therefore expand surveillance in these areas without effectively addressing public health concerns.

The use of enforcement applications (i.e., those that monitor whether individuals are complying with self-isolation and quarantine restrictions) may also be highly problematic for marginalized communities. While enforcement applications can assist in ensuring compliance with some of our most effective methods of fighting the COVID-19 pandemic to date—quarantine and social distancing—they raise the spectre of institutional overreach and the possibility of expanding surveillance for non-public health uses.

Marginalized populations are at greater risk of surveillance and subsequent criminalization by police.[102] Given the over-exposure to surveillance, and the stigmatization and criminalization of marginalized populations, these groups may be at greater risk of experiencing punitive measures should it be judged that they have violated COVID conditions. As discussed above, police departments have demonstrated a willingness to attempt to use the court process to compel access to similar databases.[103]

In the context of violating public health restrictions, over-surveillance of already marginalized populations could have the effect of implementing onerous mobility restrictions and imposition of monetary fines, both of which would be especially difficult on populations that already occupy a lower socioeconomic status. The quasi-criminalization of this group will serve to reinforce already existing disadvantages, promote stigmatization, and, ultimately, introduce an intrusive intervention by public health authorities into communities that may already have long histories of mistrust with government authorities.

But even less problematic technologies, in terms of privacy concerns, can have negative effects, and these will be amplified for marginalized communities. As discussed above, the pervasive use of digital surveillance technology to combat the spread of viruses, even if voluntary, will over time serve to normalize

[101] Applications that rely on temperature-checking have a margin for error within which symptomatic individuals will fail to be detected. This shortcoming has been underscored by Canadian Chief Public Health Officer Theresa Tam, who has repeatedly warned that "the more you actually understand [COVID-19], the more you begin to know that temperature-taking is not effective at all." She has similarly cautioned that, beyond the problem of undetected symptomatic individuals, "asymptomatic or pre-symptomatic people. . . reduce the effectiveness [of temperature-checking applications] even more." See *Global News,* "Can I refuse a temperature check?", *supra* note 14.

[102] See Akwasi Owusu-Bempah & Scot Wortley, "Race, Crime and Criminal Justice in Canada" in Sandra Bucerius & Michael Tonry, eds, *The Oxford Handbook on Race, Ethnicity, Crime and Immigration* (New York: Oxford University Press, 2014).

[103] Narwal, *supra* note 73.

surveillance in our everyday lives. Even where the efficacy of certain digital surveillance technologies is called into question, societal norms about the overall ability of technology to combat the virus may spur on accepted notions of the good of using such technology.

For example, there has been widespread promotion of the Federal COVID-19 alert app without proof of the efficacy of the app. The efficacy of the app is predicated on active participation by a large number of users and the ability to transmit data between these users. Contact-tracing applications are only able to identify contacts when both the infected and exposed individuals have their phones near them, and both individuals have downloaded and activated the app; therefore, more than other forms of digital surveillance, contact-tracing apps require a high volume of participation in order to function properly.

Thus far, in Canada, a sufficient level of participation has been difficult to achieve. Some news reports are indicating that, even where people have downloaded the COVID alert app, few are entering positive test results. One report from September 2020 indicates that, while nearly 3 million users downloaded the app, only 514 entered their positive test results.[104] On November 20th, 2020, the Nova Scotia Health Authority confirmed that 11 persons who had tested positive for COVID-19 had downloaded the COVID alert app, but only six had entered their key codes indicating they had tested positive for COVID-19.[105] Therefore, it is important to note that download rates alone do not indicate active participation with the app.

Further, contact-tracing apps risk measurement error *among* participants. The strength of Bluetooth signals is hardware-dependent and exhibits substantial fluctuations.[106] Signals are also affected by indoor obstacles such as walls and floors—this is particularly problematic given that the risk of COVID-19 transmission is highest indoors.[107] Ultimately, modelling studies have suggested that contact-tracing apps can reduce transmission, but no substantial evidence has been produced demonstrating that the apps are effective.[108]

[104] Sarah Turnbull, "COVID Alert app nears 3 million users, but only 514 positive test reports", *CTV News* (29 September 2020), online: < https://www.ctvnews.ca/health/coronavirus/covid-alert-app-nears-3-million-users-but-only-514-positive-test-reports-1.5125256 > .

[105] Elizabeth McSheffrey, "Public Health Officials Encourage Nova Scotians to Download COVID alert app, use it properly", *Global News* (20 November 2020), online: < https://globalnews.ca/news/7474679/nova-scotians-download-covid-19-alert-app-properly/ > .

[106] "Digital contact tracing for COVID-19", *supra* note 15 at 654.

[107] *Ibid.*

[108] Provinces have been raising concerns regarding the efficacy of the app because of the vagueness of the information it provides. At the time of writing, a number of Western provinces and territories had still not adopted the Federal COVID alert app. British Columbia Provincial Health Officer Dr. Bonnie Henry has raised efficacy concerns because the app cannot be used "for specific times and places instead of the current

Questions of efficacy notwithstanding, heavy reliance on digital surveillance technologies may be understandable during a global pandemic in which the common good is in jeopardy; however, as civil rights advocates have argued, once monitoring capabilities ramp up, it may be hard for governments to scale back down.[109] Further, even if governments were able to scale down, enforcement applications present the risk of "data creep" during the time in which they are operational. While using data purely to educate infected individuals and ensure that they maintain quarantine is reasonable, using that data for other reasons may not be. For instance, companies are already seeking to profit by utilizing data acquired by governments for *bona fide* public health reasons.[110]

This data creep and normalizing of surveillance may have negative effects for all Canadians. However, the effects are amplified for marginalized Canadians. The expansion and normalization of surveillance may reduce the ability of marginalized communities to challenge the use of surveillance technologies going forward, further entrenching their exposure to surveillance, stigmatization, and criminalization.

COVID alert app style, where users have it on their phone consistently." Dr. Henry's concerns relate to the fact that the app is not specific to time and place but rather contains data which may stretch back 14 days, at which time it is unlikely that a person would have been infected, thereby bogging down the contact-tracing effort. Alberta's Premier has raised concerns over the app's efficacy as it does not connect to the province's contact-tracing network, ABTraceTogether. In his annual report to Parliament, the Privacy Commissioner of Canada recommended that, given concerns over the efficacy of the app, use of the app should be monitored by way of an audit, and if it is proven to be unable to achieve its intended purpose, it should be decommissioned. Ottawa refined the app at the end of October to meet this concern in part. People can now disclose when their symptoms start or the date of their COVID-19 test. See David Carrigg, "Premier Horgan says no to federal government's COVID Alert app", *Vancouver Sun* (28 January 2021), online: < https://vancouversun.com/news/local-news/premier-horgan-says-time-for-british-columbians-to-dig-deep-in-covid-19-fight > ; Katya Slepian, "COVID alert app has 'been a challenge,' not suitable for B.C. yet: Dr. Henry", *The Free Press* (27 October 2020), online: < https://www.thefreepress.ca/news/covid-alert-app-has-been-a-challenge-not-suitable-for-b-c-yet-dr-henry/ > ; Carrie Tait & Xiao Xu, "Why B.C. and Alberta aren't signing on to the federal COVID app", *The Globe and Mail* (7 November 2020), online: < https://www.theglobeandmail.com/canada/british-columbia/article-why-bc-and-alberta-arent-signing-on-to-the-federal-covid-app/ > .

[109] Arjun Kharpal, "Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends", *CNBC News* (26 March 2020), online: < https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html > .

[110] Nicole Bogart, "Privacy, surveillance concerns are an increasing side-effect of pandemic life: expert", *CTV News* (4 May 2020), online: < https://www.ctvnews.ca/health/coronavirus/privacy-surveillance-concerns-are-an-increasing-side-effect-of-pandemic-life-expert-1.4924927 > .

But as discussed above, over-exposure is only half the problem. The other half involves the way that data collection and use can obscure and therefore reproduce existing structural inequalities.

One such example is that of predictive applications. Predictive applications use aggregate data such as from wastewater or cellphone data to predict hotspots or outbreaks and, as such, are a relatively non-intrusive avenue for public health policy-makers to obtain potentially valuable information. If cellphone users have privacy concerns, they can turn off their location history settings; however, these concerns may be minimal, as the application's reliance on aggregate data lessens these concerns relative to other digital applications.

While this collection of aggregate data may be *Charter*-compliant and fairly innocuous in terms of privacy concerns, the manner in which this data is collected and analyzed may serve to obfuscate the way that structural inequalities have contributed to high rates of infection in marginalized communities.[111] For example, some of the strongest predictors of high-risk areas—namely, a high number of poorly ventilated indoor spaces and a concentration of people who are unable to abide by physical distancing measures—have a limited relationship with flow models but correlate with socioeconomically disadvantaged areas.[112]

Policy-makers who focus solely on flow patterns but ignore other predictive factors may fail to take measures to protect marginalized populations who are at high risk of contracting COVID-19. Pinpointing a high prevalence of infection in a certain area while failing to effectively scrutinize or respond to the reasons for

[111] Predictive applications that rely on aggregate, macro-level data, have a notable limitation: the data they collect is not granular enough to measure the duration and exact proximity of person-to-person interactions and so do not measure transmission risk. While it is helpful for policy-makers to be able to predict and identify infection hotspots, digital surveillance is not the only means by which reasonable predictions can be made. For example, widely available statistics on population density, positive tests, hospital check-ins, and public transport utilization can, in concert, predict and identify hotspots independently of cellphone data. Indeed, researchers from the University of Waterloo are currently working on a reliable, multidimensional flow model that incorporates commuter data, hospitalization and testing rates, the prevalence of mask wearing, and other variables to ultimately determine how many cases given regions of Ontario can expect in the coming months. See Hannah Ritchie et al, "Statistics and Research: Coronavirus Pandemic (COVID-19*)", Our World in Data* (August 2020), online: < https://ourworldindata.org/coronavirus >; Roland Bouffanais and Sun Sun Lim, "Cities — try to predict superspreading hotspots for COVID-19" (2020) 58:3 Nature 352 at 355; James Jackson, "University of Waterloo researcher will model possible COVID-19 resurgence", *The Record* (23 July 2020), online: < https://www.therecord.com/news/waterloo-region/2020/07/23/university-of-waterloo-researcher-will-model-possible-covid-19-resurgence.html >.

[112] Craig Scott, Jen Zwicker, & Ron Kneebone, Media Release, "Vulnerable Populations and the COVID-19 Pandemic" (March 2020), online: *University of Calgary School of Public Policy* < https://webcache.googleusercontent.com/search?q = cache:Ia-Fi48EaQrgJ:https://www.policyschool.ca/wp-content/uploads/2020/03/COVID-19-Trends-Final.pdf + &cd = 2&hl = en&ct = clnk&gl = ca >.

infection serves to stigmatize the residents of that area without addressing root problems and stopping infection.[113]

Indeed, even non-intrusive technologies that ask for voluntary compliance may serve to reproduce disadvantage if implemented with no attention to structural inequalities. For example, symptom trackers that are fairly non-intrusive, asking users to volunteer information about symptoms and, depending on that information, recommend testing, may have pernicious effects on marginalized populations without necessarily raising privacy concerns.[114] Ignoring inequalities like the "digital divide," these technologies may exclude populations without cellphone and internet access such as persons in rural areas, elderly persons, low income persons, and some persons with disabilities.[115] Furthermore, while the Government of Canada has run the COVID Alert app through accessibility testing, there still may be outstanding issues for persons with literacy challenges and for persons with disabilities such as visual or language impairments.[116] These limitations undermine the app's reliability in general and could create insidious information-gaps that risk excluding groups from the policy responses that are informed by the app.

Even if issues of efficacy and access are addressed, members of racialized groups may choose not to participate in digital applications due to high levels of distrust in government and public sector agencies caused by histories of racism. This observation has been made most recently with respect to vaccinations.[117]

[113] In April 2020, members of African Nova Scotian communities expressed concern about stigmatization after the premier of the province referred to predominantly African Nova Scotian areas as virus "hotspots" and insinuating people in the area were breaking public health protocols. See Haley Ryan, "Preston group upset premier singled community out for COVID-19 criticism", *CBC News* (8 April 2020), online: < https://www.cbc.ca/news/canada/nova-scotia/preston-covid-19-premier-mcneil-nova-scotia-stigma-1.5526032 > .

[114] For example, the COVID Near You Website: < https://www.covidnearyou.org/ca/en-CA/ > ; World Health Organization, "Digital Tools for COVID-19 Contact tracing" (2 June 2020), online: < https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1 > .

[115] Statistics Canada, "Use of Internet services and technologies by age group and household income quartile" (accessed 10 June 2020), online: < https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid = 2210011301&pickMembers%5B0%5D = 1.1&pickMembers%5B1%5D = 3.1&pickMembers%5B2%5D = 4.1 > ; Jonathan Lazar & Paul Jaeger, "Reducing Barriers to Online Access for People with Disabilities" (2011) 27:2 Issues in Science & Technology 68.

[116] *Ibid.,* Government of Canada, Accessibility Statement for COVID Alert, online: < https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/accessibility-statement.html > .

[117] See Brendan Kennedy, "Bringing a COVID-19 vaccine to Black and Indigenous communities distrustful of the health system has unique challenges. Here are some places to start", *Toronto Star* (28 December 2020), online: < https://www.thestar.com/news/gta/2020/12/28/bringing-a-covid-19-vaccine-to-black-and-indigenous-communities-distrustful-of-the-health-system-has-unique-challenges-here-are-some-places-to-start.html > .

These exclusions are particularly insidious because members of these groups are, on average, at elevated risk for contracting COVID-19 and for suffering from life-threatening complications.[118]

5. CONCLUSION

In the wake of the COVID-19 pandemic, there has been a surge in the development and deployment of digital public health technologies for pandemic management. While governments may be tempted to rely upon digital surveillance applications to address the pandemic, they must carefully consider the ethical, legal, and other implications of each potential surveillance measure.

While adhering to best practices for privacy legislation and *Charter* compliance is important for a rights-based model of public health interventions, governments must also be attuned to the ways in which these interventions can be used to further inequality, including health inequality. With respect to digital surveillance applications, these considerations include expanding surveillance and criminalization, perpetuating stigma, discriminating against marginalized populations, and relying upon data that is incomplete and omits the needs and experiences of these populations.

Governments have an obligation to ensure that the populace in general is not subject to data creep and the normalization of expanded surveillance on their lives even once the pandemic is over. This concern is especially acute for those in racialized communities that are more likely to be criminalized and further marginalized due to expanded surveillance. Without addressing the impact that digital technologies have on marginalized populations, legislators risk deepening the inequalities that create the very conditions for transmission of the COVID-19 virus and put members of marginalized groups at greater risk for contracting the disease.

[118] Centers for Disease Control and Prevention, "COVID-19: People Who Are at Increased Risk for Severe Illness" (June 2020), online: < https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-increased-risk.html > .