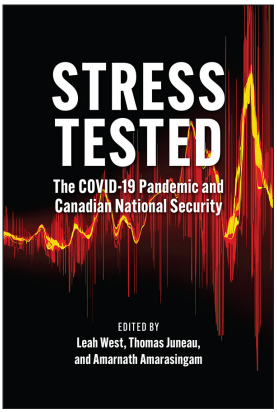
UNIVERSITY OF CALGARY
Press



STRESS TESTED: THE COVID-19 PANDEMIC AND CANADIAN NATIONAL SECURITY

Edited by Leah West, Thomas Juneau, and Amarnath Amarasingam

ISBN 978-1-77385-244-7

THIS BOOK IS AN OPEN ACCESS E-BOOK. It is an electronic version of a book that can be purchased in physical form through any bookseller or on-line retailer, or from our distributors. Please support this open access publication by requesting that your university purchase a print copy of this book, or by purchasing a copy yourself. If you have any questions, please contact us at ucpress@ucalgary.ca

Cover Art: The artwork on the cover of this book is not open access and falls under traditional copyright provisions; it cannot be reproduced in any way without written permission of the artists and their agents. The cover can be displayed as a complete cover image for the purposes of publicizing this work, but the artwork cannot be extracted from the context of the cover of this specific work without breaching the artist's copyright.

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

11

Privacy vs. Health: Can the Government of Canada Leverage Existing National Security Surveillance Capabilities to Stop the Spread?

Leah West

Introduction

In early 2020, as COVID-19 spread across Canada, officials within and outside the national security community considered how state resources and capabilities could be retooled or redirected to manage the pandemic. One of the key debates that emerged—in this country and abroad—was whether a state's surveillance apparatus, used by federal security and intelligence agencies to detect and monitor national security threats, could be leveraged in a public health crisis. Alternatively, could the federal government mandate that individuals or telecommunication service providers share the location data generated by wireless devices—namely, cell phones—with health or security agencies? This chapter looks at these questions from a legal perspective and answers them in the negative.

Divided into three parts, the chapter explains that existing legal authorities and emergency legislation do not permit the federal government's collection of Canadian location data for public health purposes. Part 1 briefly describes the use of electronic surveillance to limit the spread of COVID-19 in other countries as well as the contact-tracing application developed by the Government of Canada. It finds that Canada's choice to use a voluntary application rather than some form of mandated collection

of location data was a less effective contact-tracing tool. The application also provides no additional capacity for the enforcement of quarantine orders and public health measures.

Part 2 then canvasses the legal authorities that permit the collection of cell phone and location data by Canadian state agencies, namely, the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), and the Royal Canadian Mounted Police (RCMP). It concludes that, except for in very specific instances, existing authorities do not permit the mass collection or analysis of data necessary to trace the spread of communicable disease or enforce public health measures.

Part 3 examines Canada's emergency legislation, specifically the *Emergencies Act* and *Quarantine Act*. It refutes the arguments advanced by some scholars that the federal *Emergencies Act* in particular could be used to conduct electronic surveillance or allow cabinet to order the requisition of location data or subscriber information from Canadians or service providers. To hold otherwise would mean acknowledging property rights in personal information, a subject of debate for decades. Such a legal move would have wide-ranging implications far beyond the context of the existing pandemic and demands the full consideration of Parliament.

The chapter concludes by identifying potential legal reforms that could permit the government to leverage Canada's security apparatus to mitigate or control future public health crises. The normative question of whether the government *should* employ state surveillance tools is not addressed here but is considered by Jessica Davis and Alex Corbeil in a separate chapter in this volume.

Part 1: Surveillance to Stop the Spread?

In March 2020, the Israeli government passed emergency regulations allowing its domestic security services to conduct digital contact tracing using a classified database that compiles data provided by every telecommunications service provider in the country (Shwartz Altshuler and Aridor Hershkowitz 2020). The names of individuals who test positive are shared by health officials with the police, who then analyze the data to (1) identify and notify close contacts, and (2) enforce quarantine orders

(Landau, Kubovich, and Breiner 2020). Singapore, South Korea, and China implemented similarly sweeping surveillance measures to identify people who may be infected and to crack down on those violating public health measures (Doffman 2020). Ultimately, these measures did not prevent the spread of the coronavirus in these countries. However, they are credited with slowing the spread of the virus in Singapore (Ng et al. 2020) and South Korea (Yang 2021) in the early months of the pandemic, and with flattening the curve of infection rates in China (Sahin 2020).

Canadian privacy advocates widely decried these programs (see, e.g., CCLA 2020), but there was no robust public debate about their appropriateness or potential efficacy for slowing the spread of the virus. Ultimately, the Government of Canada chose not to implement a form of electronic surveillance or rely on security or intelligence services to assist in contact tracing. Instead, the government developed an application ("app"), COVID Alert, that users voluntarily download onto their phones. Once downloaded, users must enable the app, which then transmits a unique personal identifier via Bluetooth signal to other users. If a user tests positive for COVID-19, they can choose to enter a unique key into the app (only provided if they receive an official positive test result). The app will then notify other users whose signal crossed paths with the infected user's signal, warning them that they have come into close contact with a person with COVID-19 and encouraging them to self-isolate and get tested. At the time of its release, the app was commended by privacy experts for its strong privacy protections (see, e.g., Geist 2020). However, since then, the app's effectiveness as a public health tool has been called into question (Haggart 2020). For one, not every province and territory chose to adopt the app; the public health systems in Alberta, British Columbia, Nunavut, and Yukon do not support diagnosis reporting. Second, there is limited uptake in provinces that do support the app. By September 2020, three months after its release, less than 10 per cent of the Canadian population was using the app, and only 514 users (all within Ontario) notified the app about a positive test result; that is less than 1 per cent of the number of positive test results in the province during that period (Turnbull 2020). By March 2021, the app had been downloaded more than 6 million times, and the number of people who used it to report a positive test had increased to

20,000, yet that still only represents 5 per cent of positive cases in Canada (ISED 2021).

What is more, a flaw in the app's program identified months after its rollout requires users to ensure that the app is enabled daily. The number of notifications or contacts that have gone undetected due to the bug in the app remains entirely unknown (Daigle 2020).

Canada continues to struggle to control the spread of the virus, and the cost of the pandemic, not only in human life but to the Canadian economy, is staggering. Across the country, provinces and municipalities have undergone successive "lockdowns" to keep their health-care systems from collapsing. When the pandemic is finally behind us, we should expect policy-makers to seriously reconsider the decision to rely on citizens to volunteer their information rather than utilizing the more robust surveillance capabilities of Canada's national security and intelligence community. The need for reflection is especially important in light of the World Health Organization's warning of the likelihood of even worse pandemics in the future (WHO 2020; Dangerfield 2020).

Part 2: Canada's Domestic Surveillance Authorities

The collection of personal information by federal officials is governed primarily by the *Privacy Act* and the *Canadian Charter of Rights and Freedoms* (*Charter*). Personal information is defined as "information about an identifiable individual that is recorded in any form" (*Privacy Act*, s. 3). This includes a person's name, address, telephone number, cell phone identifier (or International Mobile Equipment Identity), and location history. The information necessary to conduct contact tracing and enforce public health orders, therefore, meets the definition of personal information.

First, under the *Privacy Act*, the government may not collect personal information unless it relates directly to an operating program or activity of the institution (*Privacy Act*, s. 4). Moreover, the government may not use personal information without informed consent (*Privacy Act*, s. 7). There are, however, exceptions to the use limitation built into the statutes governing Canada's security intelligence agencies and the Canadian *Criminal Code*. These acts give the relevant agencies the legal authority to collect and use personal information in furtherance of their mandates

without notification or consent. For example, section 12 of the *CSIS Act* stipulates that

> The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

Second, some—but not all—personal information collected by a government agency is subject to privacy protections under section 8 of the *Charter*. Section 8 guarantees the right to be secure against unreasonable search or seizure. This has been interpreted to mean that the *Charter*'s protections are only triggered when there is a search or a seizure that is subject to "reasonable expectation of privacy" (REP) (*R v S.A.B.*, 2003 SCC 60 at para 38). For example, one cannot reasonably claim a privacy interest in the collection of their name, the address of their workplace, or their hair colour. Rather, personal information attracting constitutional protection is "information which tends to reveal intimate details of the lifestyle and personal choices of the individual" (*R v Plant*, [1993] 3 SCR 281 at 293).

Information collected by electronic searches and seizures or through electronic surveillance will almost certainly meet the REP threshold (Forcese and West 2021, 435). Indeed, almost thirty years ago, the Supreme Court recognized that "electronic surveillance is the greatest leveler of human privacy ever known" (*R v Duarte*, [1990] 1 SCR 30 at para 22). More recently, the Supreme Court recognized that a police request for an Internet user's subscriber information might engage section 8 of the *Charter* where the police seek to link anonymous online activities to that subscriber information (*R v Spencer*, 2014 SCC 43). Likewise, collecting subscriber information or location data either from a service provider or directly from a user that reveals their physical travel patterns and personal interactions would certainly trigger the *Charter*'s protections.

Once triggered, a government search or seizure must be "reasonable" to not fall afoul of the *Charter*. A search is presumptively unreasonable if it is not pre-authorized by a neutral and impartial arbiter capable of acting

judicially (*Hunter et al. v Southam Inc.*, [1984] 2 SCR 145). We typically conceive of this as the need to obtain a judicially authorized warrant. Alternatively, a warrantless search may be reasonable if it satisfies three criteria: (1) the search is authorized by law; (2) the law itself is reasonable; and (3) the search is carried out in a reasonable manner (*R v Collins*, [1987] 1 SCR 265 at para 23).

The statutes governing Canada's national security and intelligence agencies set out various criteria for obtaining prior authorization for highly intrusive searches (e.g., police wiretaps under part VI of the *Criminal Code*), and the legal parameters for conducting less intrusive warrantless searches (e.g., intelligence collection under s. 12 of the *CSIS Act*). None of these existing authorities permit the collection of personal information to conduct data analysis or electronic surveillance to stop the spread of a naturally occurring pandemic.

Before moving on, a note about the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). *PIPEDA* regulates private-sector organizations involved in commercial activities unless ousted by applicable provincial privacy legislation. Under the Act, consent is required for collecting, using, and disclosing a person's information, particularly where subsequent use and disclosure is for a purpose other than that for which the information was collected (Forcese and West 2021, 435). *PIPEDA* binds private-sector organizations even when information is requested by federal and provincial agencies like the RCMP or Public Health Ontario.

CSIS Act

CSIS may collect Canadian datasets under section 11.05 of the *CSIS Act*. A Canadian dataset is "a collection of information stored as an electronic record and characterized by a common subject matter" that "contains personal information, as defined in section 3 of the *Privacy Act*." This data "does not directly and immediately relate to activities that represent a threat to the security of Canada," and "predominantly relates to individuals within Canada or Canadians." Location data generated from cellphone users within Canada to conduct contact tracing satisfies each element of this definition.

However, CSIS may only collect this information if it contributes to CSIS's security intelligence mandate under section 12, its security threat

reduction mandate under section 12.1, or its foreign intelligence mandate under section 16 of the *CSIS Act*. The latter is not applicable to this discussion, as tracing the spread of the virus across Canada is also clearly not a foreign intelligence task.

Importantly, CSIS's security intelligence and threat reduction mandates are tied to the definition of "threats to the security of Canada." Section 2 of the *CSIS Act* defines which "threats to the security of Canada" may be investigated and reduced by CSIS. They include (1) espionage and sabotage; (2) foreign-influenced activities; (3) terrorism; and (4) subversion. Here lies the problem: the natural spread of a communicable illness does not fall into any of these categories, and therefore is not subject to investigation by CSIS.

Criminal Code

Under the *Criminal Code* of Canada, law enforcement officers may apply to judges for orders to have third parties (namely, telephone service providers) produce large quantities of data. In particular, a judge or justice may issue orders for the production of (1) "transmission data," including information about telecommunications such as the type, direction, date, time, duration, size, origin, destination, or termination of the communication, but not including the content of communications; and (2) "tracking data," or data that relates to the location of a transaction, individual ,or thing (*Criminal Code*, ss. 487.011, 487.016, 487.017).

However, to issue these orders, a judge must be satisfied that there are reasonable grounds to suspect that "an offence has been or will be committed under this or any other Act of Parliament" (*Criminal Code*, ss. 487.016(2)(a), 487.017(2)(a)). In other words, the data can only be collected if an officer can establish that there are grounds to suspect a criminal offence has or will occur in advance of requesting the information. Thus, while such an order may produce evidence of prior violations of public health measures, they cannot be issued to proactively identify if or when individuals are breaching their quarantine, gathering in large groups, etc. Moreover, production orders may not be issued for the purpose of contact tracing.

CSE Act

There is little doubt that CSE has the technical capability to collect and analyze location data generated by Canadians' cellular devices. CSE also has a mandate "to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence" (*CSE Act*, s. 20). However, when CSE provides that assistance to these agencies and departments, they are bound by these bodies' legal authorities. Meaning, if CSIS or the RCMP cannot legally collect the information, neither can CSE. There is also no measure by which CSE could assist other federal or provincial agencies, (e.g., the Public Health Agency of Canada) with the collection of Canadians' personal information.

Having established that there are no regular legal authorities that would allow the federal government to leverage Canada's security and intelligence agencies' surveillance and analytical capabilities to stop the spread of an illness like COVID-19, we turn next to emergency legislation.

Part 3: Federal Emergency Legislation

This final part examines the federal *Quarantine Act* and the *Emergencies Act* and concludes that neither may be used to conduct electronic surveillance or order the requisition of location data or subscriber information from Canadians or service providers.

Quarantine Act

The federal *Quarantine Act* gives the Minister of Public Health the authority to conduct health screening when it is necessary to prevent the spread of a communicable disease. Under the Act, travellers have a duty to provide any information that a quarantine officer may reasonably require for the performance of their duties. Additionally, when the Governor in Council (essentially cabinet) issues an Emergency Order under the *Quarantine Act*, that order may subject anyone seeking to return to Canada from abroad to "any condition." Arguably, one of those conditions could be the mandatory download and use of an app that would allow quarantine officers to track travellers' movement to enforce compliance with any order issued under the Act.

Of course, there are several limits to data collection of this kind. First, it only impacts travellers coming into Canada from a foreign country. Second, collection would only be permitted for the duration of the order a traveller is subject to—for example, fourteen days from the date of their return to Canada. Third, the app would be ineffective for contact tracing as it could not capture the personal information of others in a user's vicinity who were not also subject to a quarantine order.

Emergencies Act

The *Emergencies Act* contains the stiffest government emergency powers of any emergency law in Canada. The statute defines a "national emergency" as "an urgent and critical situation of a temporary nature that . . . seriously endangers the lives, health or safety of Canadians and is of such proportions or nature as to exceed the capacity or authority of a province to deal with it, or . . . seriously threatens the ability of the Government of Canada to preserve the sovereignty, security and territorial integrity of Canada" and that cannot be addressed effectively under any other law of Canada (*Emergencies Act*, s. 3). Importantly, the caveat "any other law of Canada" means any other *federal* law (*Roberts v Canada*, [1989] 1 SCR 322).

The *Emergencies Act* anticipates four categories of emergencies: a public welfare emergency, a public order emergency, an international emergency, and a war emergency. As is the case with COVID-19, an emergency caused by "disease in human beings, animals or plants" falls within the definition of a public welfare emergency (*Emergencies Act*, s. 5). To trigger the wide-ranging powers under the Act, the Governor in Council must consult with the provincial cabinet in the affected provinces. Where the Governor in Council "believes, on reasonable grounds, that a public welfare emergency exists and necessitates the taking of special temporary measures," it may declare an emergency (s. 6(1)). At the time of writing, the Governor in Council had not declared the COVID-19 pandemic a public welfare emergency, although there is little doubt that the legal threshold has long been met. Certainly, the spread of the coronavirus disease seriously endangers Canadian lives, and the consequences, cost, and resources necessary to manage the pandemic have exceeded the internal capacities of the provinces. However, rather than invoke the Act, the Trudeau government chose not to take action that encroaches on the jurisdiction of the provinces and

instead passed new legislation to take measures within its federal jurisdiction to address the crisis.

Nevertheless, the Trudeau government could have, and could still, invoke the *Emergencies Act* in response to the pandemic. Should such a declaration be made, the Governor in Council must identify the state of affairs constituting the emergency, the special temporary measures anticipated, and the area affected by the emergency. The government may only implement measures believed necessary on reasonable grounds to deal with the situation. Those orders or regulations may only pertain to a closed list of matters set out in section 8 of the Act.

Those matters include:

> (a) the regulation or prohibition of travel to, from or within any specified area, where necessary for the protection of the health or safety of individuals;
>
> (b) the evacuation of persons and the removal of personal property from any specified area and the making of arrangements for the adequate care and protection of the persons and property;
>
> (c) the requisition, use or disposition of property;
>
> (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;
>
> (e) the regulation of the distribution and availability of essential goods, services and resources;
>
> (f) the authorization and making of emergency payments;
>
> (g) the establishment of emergency shelters and hospitals;
>
> (h) the assessment of damage to any works or undertakings and the repair, replacement or restoration thereof;
>
> (i) the assessment of damage to the environment and the elimination or alleviation of the damage; and

(j) the imposition

(i) on summary conviction, of a fine not exceeding five hundred dollars or imprisonment not exceeding six months or both that fine and imprisonment, or

(ii) on indictment, of a fine not exceeding five thousand dollars or imprisonment not exceeding five years or both that fine and imprisonment, for contravention of any order or regulation made under this section.

Notably absent from this list is the authority to mandate the disclosure of personal information by individual Canadians, Canadian entities regulated by *PIPEDA*, or other government departments. The Act also fails to give the government any additional authority to collect personal information from individuals or third parties.

Some have argued that the government can collect location and subscriber data from telecommunication service providers under section 8(c): "the requisition, use or disposition of property" (Flood and Thomas 2020, 112). Flood, Scassa, and Robertson suggest that this provision could be used to "access data held by telecommunications companies" (2020). Nevertheless, they note that an order or regulation made under the *Emergencies Act* issued to requisition that data would be insufficient both to overcome the protections afforded by *PIPEDA* and comply with section 8 of the *Charter*. As such, even if the government were to rely on this novel interpretation of "property" to collect the data, a new law is necessary to give service providers the authority to share the requested data.

There are three issues with the above argument.

First, while it is true that any order issued under the *Emergencies Act* for the seizure of property that is subject to a reasonable expectation of privacy must comply with section 8, and by consequence, the three criteria for warrantless searches set out by the Supreme Court in *Collins*. This much is clear from the statute's preamble.[1] However, it is not true that additional legislation is necessary to overcome the limits set out in *PIPEDA*.

When it comes to sharing or disclosing personal information, there are two key questions. First, does the entity with the desired information have the legal authority to share it? Second, does the entity requesting the information have the legal authority to collect it? If the answer to either question is "no," the information may not be shared.

Under the argument advanced by Scassa and Flood, the lawful authority to collect would be an order issued under the *Emergencies Act* to administer the Act or any number of provincial emergency regulations issued to manage a major health crisis. What they appear to overlook is that *PIPEDA* sets out several exceptions where private-sector organizations may disclose personal information without notification and consent. For example, under section 7(3)(c.1)(iii), an organization may disclose personal information to a government institution that identifies its lawful authority to obtain the information and indicates that the disclosure is requested for the purpose of administering any law of Canada or a province. This exception is the authority to share; it has already been built into *PIPEDA* for situations exactly like Scassa and Flood describe. Consequently, new legislation would not be required.

Second, under existing law, individuals do not "own" information about themselves that third parties physically compile. In *McInerney v McDonald*, the Supreme Court of Canada determined that doctors, not patients, own the physical copies of a patient's medical records ([1992] 2 SCR 138). The paper records or hard drives on which a doctor stores a patient's information are the physician's property. Therefore, a patient does not have the right to demand access to or receive copies of those records. The Court noted that, "while the doctor is the owner of the actual record, the information is to be used by the physician for the benefit of the patient," thereby giving "rise to an expectation that the patient's interest in and control of the information will continue" (para 22). Scassa herself explained that "although *McInerney* dealt with personal health information, there is no reason to expect that a Canadian court's decision would be different with respect to other types of personal information" (2018, 13).

What does this mean in the context of the location data generated by subscribers so that Rogers, Bell, and Telus can bill customers and provide them with various GPS-enabled services? For one, it means that the personal information generated by users and compiled by service providers is

not the property of individual subscribers. Moreover, while Rogers, Bell, and Telus may be the physical owners of the hard drives on which they store our personal information, they do not "own" the information itself to do with it as they please. The limitations imposed by *PIPEDA* on the selling, sharing, and use of personal information held by the private sector reinforces this fact.

Even before *McInerny*, in *R v Stewart* ([1988] 1 SCR 963), the Supreme Court considered whether confidential information qualifies as property, such that it could be the subject of theft. The Court held that for anything to be property, someone must "own" it, and it must be capable of being taken or converted in a manner that results in a deprivation of its use or possession by the owner (para 35). The Court held that "except in very rare and highly unusual circumstances," information could not be taken or converted.[2] Arguably, one such exception is a trade secret. However, the accumulation of subscriber information or location data is not a trade secret, nor any other form of intellectual property. It does not satisfy the criteria to be a trade secret under IP law; it is not a plan or process, tool, research mechanism, or compound known only to the service provider and valuable only insofar as it remains a secret (Canadian Intellectual Property Office n.d.). Nor does the compilation of facts collected by service providers into an ever-changing database qualify as a copyrightable work (Scassa 2018, 7–8).

What is more, Parliament chose to amend the *Criminal Code* to capture the taking of trade secrets in 2020. However, rather than amend the *Code* so that information would qualify as "property" capable of theft, Parliament added a separate provision making it an offence to "obtain a trade secret" by deceit, falsehood, or other fraudulent means (s. 391). Here, too, bulk subscriber or location data does not satisfy the *Criminal Code* definition of "trade secret."[3]

Third and finally, any move to recognize property rights in personal information should not be undertaken lightly. This issue is subject to a long-standing debate and has wide-ranging implications for our modern, data-driven economy. Currently, none of Canada's privacy or data-protection laws expressly define who owns personal information, let alone the vast amounts of data we generate simply by living in the modern world. Before we accept that a new property right exists, numerous questions need

to be considered. As Ritter and Mayer (2018) ask: When does ownership attach to data? What are the rights, privileges, and constraints vested in the owner of personal data? Can any of those rights or controls be transferred, licensed, or sold? These questions demand the full consideration of Parliament. They should not be brushed aside for the sake of expediency by fitting the square peg of electronic surveillance into the round hole that is the requisition of property.

If, however, I am wrong, and location data is property and may be requisitioned through an order issued under the *Emergencies Act*, that order would still need to comply with section 8 of the *Charter*. This is extremely complicated. We only need to look to the complex legislation surrounding the collection and use of datasets under section 11 of the *CSIS Act* for a sense of what would be required to ensure the reasonableness of collecting, retaining, and analyzing highly revealing information about an entire population. Whether such a scheme should or could be implemented via an emergency order issued by the Governor in Council is highly questionable. Moreover, it is arguable that without some sort of prior judicial authorization, the collection and use of bulk location information to enforce public health orders would never satisfy section 8 of the *Charter*.

Conclusion and Recommendations

The preceding discussion establishes that the Government of Canada has no existing legal means of leveraging the electronic surveillance and data analytics capabilities of its security and intelligence agencies to conduct contact tracing to stop the spread of a communicable illness like COVID-19. Moreover, only very narrow authorities allow for the collection and use of personal information to enforce public health measures. And, to date, reliance on a voluntary application has proven ineffective. Even if incalculable, the economic and public health costs of this choice are substantial.

In the aftermath of the pandemic, lawmakers may ultimately determine that it is appropriate to leverage the tools and techniques developed by Canada's security agencies to limit the effects of a global health crisis in a manner compliant with the *Charter*. If so, the following recommendations could serve as a starting point for a discussion on legislative reforms.

1. Expand the definition of "threats to the security of Canada" under section 2 of the *CSIS Act* to include the outbreak or spread of deadly epidemics. Such an amendment would broaden CSIS's section 12 mandate and allow for the collection of datasets to assist CSIS in fulfilling that expanded mandate.
2. Amend the *Criminal Code* to authorize the issuance of a transmission or tracking data production order to assist in the enforcement of public health measures. The threshold would need to be sufficiently circumscribed to satisfy section 8 of the *Charter* while removing the need for suspicion of a particularized offence.
3. Expand CSE's assistance mandate to include provincial health authorities where the Minister of Public Safety makes a written request to the Minister of National Defence. This request could be triggered when a province declares a provincial emergency and requests federal assistance. Under the federal *Emergency Management Act*, the Minister's responsibilities include "providing assistance other than financial assistance to a province if the province requests it" (s. 4(1)(i)).
4. Amend section 8 of the *Emergencies Act* to include a measure related to the disclosure of personal information. Currently, the measures listed in the federal *Emergencies Act* largely mirror those available to provincial governments under provincial emergency legislation, with one notable exception. Ontario's *Emergency Management and Civil Protection Act* uniquely stipulates that the Lieutenant Governor in Council may issue an order "that any person collect, use or disclose information that in the opinion of the Lieutenant Governor in Council may be necessary in order to prevent, respond to or alleviate the effects of the emergency" (s. 7.0.2(4)(13)).

Each of these recommendations comes at a cost, and that cost is the privacy of Canadians. Whether the loss of privacy resulting from enhanced surveillance and contact-tracing capabilities is worth it to stop the spread of a future pandemic is a question Canadian law and policy-makers should carefully contemplate.

NOTES

1 The text of the preamble reads: "the Governor in Council, in taking such special temporary measures, would be subject to the Canadian Charter of Rights and Freedoms and the Canadian Bill of Rights and must have regard to the International Covenant on Civil and Political Rights, particularly with respect to those fundamental rights that are not to be limited or abridged even in a national emergency."

2 The Court only considered this question in the context of criminal law. But as Scassa notes, "While the court did not consider whether it might be property in other contexts, it seems unlikely" (2018, 12).

3 *Criminal Code*, s. 391 (5). For the purpose of this section, "trade secret" means any information that (1) is not generally known in the trade or business that uses or may use that information; (2) has economic value from not being generally known; and (3) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

REFERENCES

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Canadian Intellectual Property Office. n.d. "Trade Secrets Factsheet." Government of Canada, accessed 21 June 2021. http://publications.gc.ca/collections/collection_2018/opic-cipo/Iu71-4-39-2017-eng.pdf.

Canadian Security Intelligence Service Act, RSC, 1985, c C-23.

CCLA (Canadian Civil Liberties Association). 2020. *Privacy, Access to Information, and You: The COVID-19 Edition*. Toronto: CCLA. https://ccla.org/cclanewsite/wp-content/uploads/2020/05/Privacy-Access-to-Information-and-You_-The-COVID-19-Edition.pdf.

Criminal Code, RSC, 1985, c C-46.

CSE Act (*Communications Security Establishment Act*), SC 2019, c 13, s 76.

Daigle, Thomas. 2020. "Open the Covid Alert App to Make Sure It Works, Says Developers." *CBC News*, 11 December 2020. https://www.cbc.ca/news/technology/covid-alert-app-bug-persists-on-iphone-1.5836604.

Dangerfield, Kate. 2020. "'The Big One': WHO Warns Future Pandemics Could Be Worse than Coronavirus." *Global News*, 29 December 2020. https://globalnews.ca/news/7545830/coronavirus-pandemic-big-one-who/.

Doffman, Zak. 2020. "COVID-19 Phone Location Tracking: Yes, It's Happening Now—Here's What You Should Know." *Forbes*, 27 March 2020. https://www.forbes.com/sites/zakdoffman/2020/03/27/covid-19-phone-location-tracking-its-moving-fast-this-is-whats-happening-now/.

Emergencies Act, RSC, 1985, c 22 (4th Supp).

Emergency Management Act, SC 2007, c 15.

Emergency Management and Civil Protection Act, RSO 1990, c E.9.

Forcese, Craig, and Leah West. 2021. *National Security Law*. 2nd ed. Toronto: Irwin Law.

Flood, Colleen M., Teresa Scassa, and David Robertson. 2020. "How Invoking the Emergencies Act Could Help Canada Better Track, Contain COVID-19." *CBC News*, 27 March 2020. https://www.cbc.ca/news/opinion/opinion-covid-coronavirus-emergency-measures-act-tracking-1.5510999.

Flood, Colleen M., and Bryan Thomas. 2020. "The Federal *Emergencies Act*: A Hollow Promise in the Face of COVID-19?" In *Vulnerable: The Law, Policy, and Ethics of COVID-19*, edited by Colleen M. Flood, Vanessa MacDonnell, Jane Philpott, Sophie Thériault, and Sridhar Venkatapuram, 105–14. Ottawa: University of Ottawa Press.

Geist, Michael. 2020. "Why I Installed the COVID Alert App. *Michael Geist* (blog), 2 August 2020. https://www.michaelgeist.ca/2020/08/why-i-installed-the-covid-alert-app/.

Haggart, Blayne. 2020. "Canada's COVID Alert App Is a Case of Tech-Driven Bad Policy Design." *Conversation*, 13 August 2020. https://theconversation.com/canadas-covid-alert-app-is-a-case-of-tech-driven-bad-policy-design-144448.

Hunter et al. v Southam Inc., [1984] 2 SCR 145, 11 DLR (4th) 641.

ISED (Innovation Science and Economic Development Canada). 2021. *First Interim Report of the COVID-19 Exposure Notification App Advisory Council*. Ottawa: Ministry of Industry. https://www.ic.gc.ca/eic/site/icgc.nsf/eng/07716.html.

Landau, Noa, Yaniv Kubovich, and Josh Breiner. 2020. "Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens with the Data." *Haaretz*, 18 March 2020. https://www.haaretz.com/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383?v=1613647214246.

McInerney v McDonald, [1992] 2 SCR 138, 93 DLR (4th) 415.

Ng, Yixiang, Zongbin Li, Yi Xian Chua, Wei Liang Chaw, Zheng Zhao, Benjamin Er, Rachael Pung, Calvin J. Chiew, David C. Lye, Derrick Heng, and Vernon J. Lee. 2020. "Evaluation of the Effectiveness of Surveillance and Containment Measures for the First 100 Patients with COVID-19 in Singapore—January 2–February 20, 2020. *Morbidity and Mortality Weekly Report* 69, no. 11 (2020): 307–11. https://www.cdc.gov/mmwr/volumes/69/wr/mm6911e1.htm.

PIPEDA (*Personal Information Protection and Electronic Documents Act*), SC 2000, c 5.

Privacy Act, RSC, 1985, c P-21.

Quarantine Act, SC 2005, c 20.

R v Collins, [1987] 1 SCR 265, 74 NR 276.

R v Duarte, [1990] 1 SCR 30, 65 DLR (4th) 240.

R v Plant (1993), 157 NR 321, [1993] 3 SCR 281.

R v S.A.B., 2003 SCC 60.

R v Spencer, 2014 SCC 43.

R v Stewart, [1988] 1 SCR 963, 50 DLR (4th) 1.

Ritter, Jeffrey, and Anna Mayer. 2018. "Regulating Data as Property: A New Construct for Moving Forward." *Duke Law and Technology Review* 16, no. 1 (2018): 220–77. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1320&context=dltr.

Roberts v Canada, [1989] 1 SCR 322, 57 DLR (4th) 197.

Sahin, Kaan. 2020. "The West, China, and AI surveillance." Atlantic Council, 18 December 2020. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance/.

Scassa, Teresa. 2018. "Data Ownership." *CIGI Papers* no. 187. https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf.

Shwartz Altshuler, Tehilla, and Rachel Aridor Hershkowitz. 2020. "How Israel's COVID-19 Mass Surveillance Operation Works." *TechStream* (Brookings Institute), 6 July 2020. https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/.

Turnbull, Sarah. 2020. "COVID Alert App Nears 3 Million Users, but Only 514 Positive Test Reports." *CTV News*, 29 September 2020. https://www.ctvnews.ca/health/coronavirus/covid-alert-app-nears-3-million-users-but-only-514-positive-test-reports-1.5125256.

WHO (World Health Organization). 2020. "The Best Time to Prevent the Next Pandemic Is Now: Countries Join Voices for Better Emergency Preparedness." World Health Organization, 1 October 2020. https://www.who.int/news/item/01-10-2020-the-best-time-to-prevent-the-next-pandemic-is-now-countries-join-voices-for-better-emergency-preparedness.

Yang, Myungji. 2021. "Behind South Korea's Success in Containing Covid-19: Surveillance Technology Infrastructures." *Items*: *Insights from the Social Sciences*, 21 January 2021. https://items.ssrc.org/covid-19-and-the-social-sciences/covid-19-in-east-asia/behind-south-koreas-success-in-containing-covid-19-surveillance-technology-infrastructures/.