AIRD BERLIS

SPOTLIGHT
MEDIA, SPORTS AND COMMUNICATIONS LAW BLOG

Mar 27, 2020

Geolocation and the Fight Against COVID-19

Could the Emergencies Act Overrule Privacy Law Protections for Cellphone Location Data?

By Paige Backman and Stephanie D'Amico

(1) The longstanding tension between public safety and civil liberty

While COVID-19 is a "novel" coronavirus, the tension it stokes between public welfare and personal freedom is anything but new. In the 1970s, our nation had a divided response to the federal government's invocation of the *War Measures Act* to suppress terrorism during the October Crisis. More recently, the same themes emerged in debates about the controversial *Patriot Act* in the wake of 9/11 in the United States. The delicate balance between public safety and civil liberty is a fixture of democratic society and has, once again, come to the fore as the world grapples with a global pandemic for the first time in more than one hundred years.

Today, the battle is between public health and personal privacy. An increasing number of jurisdictions are leveraging geolocation data from cellphones to combat COVID-19, and many are wondering whether such extraordinary measures can or will be implemented in Canada to help "flatten the curve." Geolocation data tracks every person's movements, day and night, so long as they have their mobile phone with them and it's turned on. It can inform where you are and who you are with. In the ordinary course, mobile phone tracking and other digital surveillance activities would, at minimum, butt heads with both the Charter and Canada's existing privacy legislation. However, the extraordinary powers inthe federal *Emergencies Act* (the successor legislation to the repealed *War Measures Act*) could, in theory, empower the legal use of geolocation data to fight the pandemic.

(2) The use of geolocation data to prevent the spread of COVID-19

Globally, mobile carrier data has been used in a range of different ways to buttress health authorities' efforts to combat COVID-19. In general, geolocation data is typically used in three ways: (1) to ensure compliance with quarantine and social distancing protocols; (2) to retrospectively review the movements of those who have tested positive for the virus in order to prevent community spread; and (3) to provide real-time alerts to people in proximity to someone who has tested positive for the virus.

Taiwan, for example, has implemented an "electric fence" which collects geolocation data from cellphones to monitor and enforce quarantine. The system alerts law enforcement officials if citizens under quarantine leave their address or turn off their phones. Regular phone calls are made to ensure those ordered to self-isolate are not venturing out in public and leaving their phones at home. There are considerable fines for violating quarantine.

Singapore has developed the "TraceTogether" App which, among other things, allows the government to use retrospective location data to review the movements of citizens who have tested positive for the virus in order to track and reduce community spread.

The Israeli government drew attention last week for ordering hundreds of citizens to self-isolate via text message because location data collected by the ISS indicated they had been in proximity to a person who had tested positive for COVID-19.

Some of the most extreme and Orwellian uses of geolocation data have been seen in China, where citizens' access to checkpoints is restricted based on a colour-based QR code which corresponds to a person's health status. South Korea, Italy, Germany and Austria are among the other jurisdictions sharing

geolocation data with health authorities in an effort to help combat the virus. Discussion of technological intervention has begun in the United States.

(3) Protections for geolocation data under Canadian privacy law

The *Canadian Charter of Rights and Freedoms* (the "Charter") does not specifically mention privacy or the protection of personal information. However, Section 7 of the Charter states that an individual's right to life, liberty and security of person is a fundamental human right and Section 8 of the Charter similarly protects our fundamental human right to be free from unreasonable searches from the government. Further, the Supreme Court of Canada has expressly determined that the right to privacy, as set out in the *Privacy Act*, is a "quasi-constitutional" human right. The values set out in the *Privacy Act* have been found to be closely linked to those fundamental rights set out in the Charter as being necessary to a free and democratic society.

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. This includes telecommunications companies and mobile carriers which, for the most part, are the entities that collect and have access to the geolocation data that could be weaponized against COVID-19.

A fundamental purpose of PIPEDA and its provincial counterpart legislation across Canada is to formalize by statute applying to the private sector protections for "personal information" and to ensure that the collection, use or disclosure of personal information, including individuals' location and movement, occurs only with consent.

PIPEDA defines "personal information" broadly as "information about an identifiable individual." It includes information that can identify an individual directly or through reasonably available means. The geolocation data to be used by government to enforce quarantine protocol or to provide real time alerts would be considered personal information.

There are various provisions in PIPEDA which would arguably permit the disclosure of personal information – in this instance, geolocation data – to government institutions without the consent of the individuals. For example, Section 7(3) of PIPEDA provides that:

(3) an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is…

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,

(iii) the disclosure is requested for the purpose of administering any law of …

(d) made on the initiative of the organization to a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

...

(i) required by law.

(4) Use of the Emergencies Act to compel disclosure of geolocation data

Under the *Emergencies Act*, the federal Cabinet can proclaim a "public welfare emergency" in response to the COVID-19 pandemic. A public welfare emergency has not yet been declared, but the Trudeau government has indicated that the invocation of the Act is not off the table, particularly if the provinces support or request the declaration of a national emergency.

The *Emergencies Act* imbues the federal government with a broad swath of powers. If a public welfare emergency were declared, Cabinet may be in a position to pass regulations mandating the disclosure of mobile carrier data to aid in the fight against COVID-19. Subsection 8(1) of the *Emergencies Act* provides that during a public welfare emergency, the Governor in Council may make orders and regulations which are reasonably believed to be necessary to deal with the emergency. The subject matter for possible orders is expansive and includes powers for the requisition, use or disposition of property[1] and to regulate the distribution of essential goods, services and resources.[2] The broad wording and untested nature of these provisions are such that mobile carrier data could be considered "property" under paragraph 8(1)(c), or be declared an "essential resource" under paragraph 8(1)(e).

The *Emergencies Act* also includes the ability to impose fines and imprisonment for violation of orders and regulations created under the Act, measures which have already been implemented in jurisdictions with less robust human rights protections. The exercise of Cabinet's authority under the *Emergencies Act* is subject to limited judicial oversight.

(5) Conclusion

To date, geolocation data has not been overtly used in Canada to combat COVID-19. However, given the urgent need to respond to the pandemic, measures which would be unthinkable in normal times may be seen as viable options to help contain the outbreak. For some, the availability and use of geolocation data presents a techno-utopian resolution to a public health crisis; for others, it is a work of dystopian speculative fiction waiting to happen. No matter where one lands, the pandemic brings into sharp relief the need to evaluate whether and to what extent diminished data privacy and enhanced surveillance technologies should be tolerated in the context of a public health emergency.

Organizations with questions about privacy or data security can contact our Privacy & Data Security Group .

[1] *Emergencies Act*, R.S.C., 1985, c.22 (4th Supp.), s.8(1)(c)

[2] *Emergencies Act*, R.S.C., 1985, c.22 (4th Supp.), s.8(1)(e)

Authors

Paige Backman
Partner
T 416.865.7700
pbackman@airdberlis.com

Stephanie D'Amico
Student-at-Law
T 416.863.1500 x3317
sdamico@airdberlis.com