COVID-19 and Cellphone Surveillance

Note: This was originally published on April 16, 2020 on ABlawg: Joel Reardon, Emily Laidlaw, and Greg Hagen, "COVID-19 and Cellphone Surveillance" (April 16, 2020), online: ABlawg, https://ablawg.ca/wp-content/uploads/2020/04/Blog_JR_EL_GH_COVID.pdf.

One of the authors has since discovered attacks on the decentralized version of contract tracing systems that may render it worse for privacy than the centralized model. More information can be found here.

Last week in Premier Kenney's address to the province, he announced (at approximately 10:29 of the video) that a central component of Alberta's strategy in relation to COVID-19 (and its related SARS-CoV-2 virus) could require the use of technology to enforce quarantine orders: "We will strictly enforce quarantine orders to ensure compliance, including using technology like smartphone apps." When a spokesperson for the Alberta Privacy Commissioner's Office raised privacy concerns about the use of a smartphone app to enforce quarantine, the *Calgary Herald* reported that Premier Kenney dismissed such concerns as "overblown", seemingly because only a small group of people would be tracked and only for the purposed of enforcing a valid quarantine order.

At this stage, however, we do not know precisely how the Alberta government will use technology to address COVID-19 issues. Premier Kenney's mention of technology was brief and only referenced enforcement of quarantine orders. There are other possible uses of location tracking technology, however, such as contact tracing to assess who might have been exposed to the virus. Once software is used to enable location tracking by the Government of Alberta for enforcing quarantines, it may be tempted to repurpose such software for contact tracing. Faced with the prospect of technology being used in these ways, we teamed up to provide readers with a cross-disciplinary commentary on the technological and privacy implications of cellphone surveillance and COVID-19.

The use of technology to either enforce quarantines or trace COVID-19 contacts has been deployed in numerous countries, including China, Israel, Taiwan, South Korea, Singapore (see here, here and here) and the United Kingdom, and current efforts are underway to develop apps by Google and Apple (an unlikely team), and MIT, among others. As the story goes, geodata enables tracing of SARS-CoV-2 contacts to assess who might be at risk of contracting the disease, to find unlawful public gatherings, and to enable authorities to track quarantine breakers and enforce stay at home orders. We are facing a health emergency of staggering proportions and infection data is valuable to assist in reducing the transmission and spread of the virus. All of this data might enable a more surgical approach to quarantine measures in the near future rather than the blanket approach necessary at this stage, thereby paving the way to re-opening our economy and our doors.

However, we must directly acknowledge the impact that smartphone location tracking has on personal privacy in order to do the hard work we need to do to ensure that appropriate privacy protections are put in place. The fact that location tracking is for the purpose of enforcing legally valid quarantine orders on a small number of individuals does not minimize the privacy risks. Rather, we must ensure that such tracking protects important privacy rights. The long and short of our message is that privacy rights are so important that they need to be preserved as much as possible during the fight against COVID 19. Indeed, we argue that new and more specific privacy safeguards need to be legislated prior to requiring the use of smartphones for quarantine enforcement or contact tracing. Of course, it is tempting to reduce privacy during a health emergency in order to further public health priorities. However, emergencies are precisely the moment when our commitment to fundamental rights like privacy are tested the most, and complying with that commitment has the multiple effects of better ensuring that the data that you want to rely on is in fact telling you accurate things, that the approach you want to take is proportionate, and that use of the technology in this way does not become normalized.

To begin to understand these issues, we will examine the technical aspects of smartphone surveillance, and the regulatory principles that should govern its use in a preliminary way. To be certain, there are more issues than we can explore in this short post, but our goal is to provide a legal framework to begin to think about these issues. Let's take a deeper dive.

Contact Tracing Introduced

Contact tracing is a method for public health authorities, where a person who has received a positive diagnosis for a disease such as COVID-19, to alert those with whom they have been in contact and are therefore also at risk. The risk posed by the underlying virus, SARS-CoV-2, has made contact tracing a useful tool to manage the outbreak, particularly as it may be transmissible by those not exhibiting symptoms.

Contact tracing can be implemented in non-technical ways. For example, an infected individual may inform co-workers, families, and friends that they may be at risk, ensuring those who have had lengthy or repeated recent contact with the individual may themselves get tested. Recollection-based contact tracing, however, is unable to identify strangers who may have unintentionally come into close contact with an infected individual. The high risk of SARS-CoV-2 contagion means that effective contact tracing must include these individuals as well.

Mobile phones have been proposed as a tool to implement a digital form of contact tracing that does not rely on memory of past social interactions. This works by having phones collect and report data that encodes when all pairs of people were in close proximity, and using that data to assess individuals' risk of contagion.

For example, suppose you happened to be at the same grocery store or on the same bus at the same time as someone who now tests positive. Recollection-based contact tracing is unlikely to identify you, but if it is known that both your mobile phones were physically proximate for an extended period of time then you can be promptly warned.

Centralized Location Tracking for Contact Tracing Creates Privacy Risk

Such a technology-aided contact tracing system can be implemented using the fact that most mobile devices are able to self-geolocate, either explicitly though GPS measurements or inferring location from nearby cell-phone tower identities and Wi Fi hotspot identities. A simple solution, which we can call "centralized," is to require everyone to give the government or some other authority their GPS locations at all times. This data is combined with information about who is infected, and determines and informs those who are at risk.

A centralized location tracking system creates a significant privacy risk. That is because it collects far more data than is actually necessary to implement the public health goals of contact tracing, and this data is deeply personal and private – including both locational and medical data. In doing so, it also violates the principle of minimizing the amount of personal data collected because the useful subset of data is only instances of pairs of people in close proximity, and even then only if one ends up being infected shortly after. As well, GPS location is not a reliable indicator since it is accurate to 5-20 metres (see here), which is farther apart than social distance guidelines, and it is even less reliable indoors.

Decentralized Proximity Tracing for Contact Tracing

To achieve a more robustly reliable and less privacy invasive proximity measure, we can use Bluetooth radio communication. Bluetooth is a commonly used technology for short range communication for many consumer electronics, such as wireless headphones or wireless game controllers. The observation here is that if two phones are able to "hear" each other via Bluetooth it means that the phones are nearby and we can infer that the phones' owners are currently in close proximity.

Bluetooth proximity is not foolproof. It could be that people are nearby but only briefly. We can address this by requiring an amount of time in which they keep hearing each other to count as a proximate encounter. Still, it could also be that they are mutually quarantined, such as by being in a sealed environment, like separate cars or adjacent rooms.

Bluetooth also does not provide secure distance bounding. When used normally it achieves its goals, but it is vulnerable to someone with a high-gain directional antenna to spy on Bluetooth signals from far away or with a powerful broadcasting antenna that can be used to make many people think they are close to someone when in reality they are not. These broadcasts could fool many listeners into falsely thinking that they are at risk.

TraceTogether App

Despite these issues, Bluetooth proximity has been used already. The TraceTogether app being used in Singapore is based upon the idea that everyone installs an app, TraceTogether, and that app sends out a *hello* message to everyone around them periodically. These *hellos* include a pseudonym for the user: not their actual name, but rather some random number that is associated with that person. Everyone's phone keeps a diary of all the *hellos* they heard over the last couple of weeks along with who sent them.

If a user is found later to be sick, then they can upload their pseudonym to a service that informs all other app users. All other users can then check to see the *hellos* they got and if they noticed enough, say five, from an infected person they may themselves *choose* to get tested and reveal their own identities if they are also infected.

This model is positive in that users have control over whether to reveal their pseudonym and *do not* have to reveal their location history. Data is stored only by the users themselves, making it a decentralized system. It has the unfortunate feature, however, that a person's pseudonym is fixed. Figuring out someone's pseudonym would be easy if you keep seeing the same pseudonyms when they are around. It also allows *hellos* sent by the same user to be linked over time: even if you don't know who they are, you can recognize when you see them again, allowing for long-term tracking of individuals.

The nature of Bluetooth being a public broadcast also means that other apps can collect these *hellos* and combine them with location information to send them off to ads and analytics companies. It is commonplace that apps include code written by third party companies that collect exactly this type of personal information, and app developers are paid for having their code run on each individual phone. The use of persistent pseudonyms would enable such a third party library to start tracking other people's locations by listening in on the same Bluetooth communication.

Adding Unlinkability

An obvious improvement to the Singapore model is to prevent linking of previous *hellos* to a current *hello*. That is, every time you send a *hello*, you simply pick a random number and send it instead, and later report all the random numbers you ever sent. Now, every time you send a *hello* it is not linkable to any other *hello* you have ever sent. Now, everyone remembers all the *hellos* they hear, and if someone is sick they publish all the *hellos* that they ever sent.

Without getting too deep into cryptographic details, it turns out that the pretty basic techniques we use in cryptography can make this approach very efficient and also prevent people from claiming that they send *hellos* that they never really did. The trick is to use a *keyed pseudorandom number generator*. These random number generators produce a long list of numbers that look random – one cannot guess the next one by looking at the list – but which become predictable if you know a small secret key that is used to generate them. To reveal all your *hellos*, all you need to do is publish the key and anyone else can reconstruct all the random numbers. Without the key, the numbers themselves look simply random and so the *hellos* cannot be linked. It also means that you cannot claim an arbitrary number you did not actually send – you can only claim numbers that the key generates. As long as the key remains secret, other users of the system do not have their *hellos* linked up.

This unlinkable, Bluetooth-based contact tracing is the main proposal made by a large team of European Researchers as well as another team of MIT researchers. Both proposals have their own additional ideas, such as techniques to thwart those with powerful antennas and annotation of received *hellos* as low risk for contagion based on geolocation metadata. It

also appears to be the current working draft of the proposed Google and Apple partnership for their contact tracing mobile phone update.

Individuals would opt-in to notify a health app that they have tested positive, and any phones that have recently be in close proximity would be alerted. The contact tracing feature would be "baked" into the operating system, which will be rolled out in the next few months. The opt-in nature relies on a consent-based model to preserve privacy, but the lack of compulsion means it will not be as widely effective to combat the spread of the virus. As it is embedded into the operating system, the degree to which it is opt-in depends on how it is ultimately deployed. There is a further issue of the data now being in the hands of a private sector entity, in particular Google, which built its business on collection and use of user data.

Additional Privacy Principles

So, far we have highlighted that a centralized contact tracing system does not comply with the principle of minimizing the collection of personal information, but decentralized, proximity testing software also raises privacy issues. We want to emphasize here that the technology that is used to combat the spread of SARS-CoV-2 – whether contact tracing or to enforce quarantines or social distancing – should comply with all privacy principles. These principles are embodied in provincial and federal privacy legislation, and many of them stem from the *National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (Schedule I of the Federal *Personal Information and Protection of Electronic Documents Act*, SC 2000, c 5). Some of the relevant principles from the model code are that the collection, use and disclosure of personal information should only be done if it is for a reasonable purpose. Usually, consent must be provided in a meaningful way, although consent is not possible for many of the uses explored in this post. The data collected and used should be limited to that which is necessary, and there should be no creeping use beyond this scope, such as repurposing the data for other uses or sharing the data with third parties. Data should not be retained for longer than necessary. Reasonable security safeguards should be used. And a justifiable worry with this data is accuracy. We should have access to the data to challenge its accuracy.

Based on these principles, the proposed uses of technologies to combat COVID-19 raise many questions, including, but not limited to:

- **What data will be collected?** Will individuals be identifiable? Will information be aggregated or anonymized? What data minimization techniques will be used?
- **Is the data accurate?** How will the accuracy of the data, or limits about its accuracy, be accounted for?
- **Who will have access to the data?** What limits will be in place about who has access to the data and who they can share it with?
- **How will the data be used?** Will decisions be made about an individual

based on data, e.g. to impose a fine for breaching a quarantine order, to limit a person's access to certain places?

- **How will the data be secured?** What security measures are used to protect the data?
- **How long will the data be stored?** What will the data retention period be?
- **What requirements will be imposed on individuals related to their devices?** For example, will users be required to keep their phones on, take them when they leave the house, enable Bluetooth or download an app? What if you do not own a smartphone?
- **Who is accountable?** Who has oversight? Ultimately, there will potentially be cross-pollination between public sector bodies (e.g. law enforcement, health sector) and private sector (if private sector designs the tracking app).

The Temptation to Route Around Privacy Protections in a Pandemic

These issues take on a greater urgency as a result of the existing public health emergency that has been declared under the *Public Health Act*, RSA 2000, c P-37. It may be tempting for the Government of Alberta to rely upon the fact that existing privacy legislation allows for weaker privacy protection during public health emergencies. For example, according to the Alberta Privacy Commissioner's interpretation, the three pieces of Alberta privacy legislation – the *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, the *Health Information Act*, RSA 2000, c H-5, and the *Personal Information Protection Act*, SA 2003, c P-6.5 – each permit the collection of personal information without consent from a person when that collection is expressly authorized by an Alberta enactment. On this reading, a "centralized" public body could collect, use and disclose personal location information through a smartphone if an enactment made during an emergency authorized such collection.

More radically, s 52.21(2)(a) of the Alberta *Public Health Act* permits the minister responsible for a particular enactment (or if unavailable, the Minister of Health) to order, without the need for consultation, the suspension or modification of the operation or application of an enactment that would unreasonably delay or hinder action necessary to protect public health. Hence, the minister responsible for the *Freedom of Information and Protection of Privacy Act,* for instance, may suspend or modify provisions of that enactment that protect personal privacy, paving the way for automated location tracking that need not protect privacy. Further still, the recently-passed *Public Health (Emergency Powers Act, 2020),* SA 2020 c5, amends the *Public Health Act* by allowing that same minister, under s. 52.21(2)(b), to *create* new provisions either in addition to, or instead of, an existing provision in an enactment of the provincial legislature (more generally on the new Act, see Shaun Fluker's recent post). As a result, that minister now has the power under the

amended *Public Health Act* to order Alberta residents to download software to their smartphones in order to send the Government of Alberta real-time continuous location information without the benefit of privacy protections otherwise contained in the *Freedom of Information and Protection of Privacy Act*.

Additional Privacy Safeguards

In our view, there are at least two important preconditions to the government requiring the use of any software or other technology to enforce quarantines or enable contact tracing. The first is technological: safeguards need to be baked into the design of such technology in a way that it ensures the minimum privacy invasiveness. Closely related, if there is a choice of technologies, the most privacy-preserving technology must be chosen. At the time of writing, contact tracing through Bluetooth-enabled devices that use decentralized, unlinkable, proximity testing is the best route forward in comparison to centralized location tracking systems. But the use of such technology is not the end of the story, as even those Bluetooth systems carry privacy risks. Further, a particular technology solution is not a "rhetorically powerful enough solution to reassure and empower the public." (see *Coronavirus Safeguards Bill* at p 2, discussed next)

Thus, the second precondition is key: it is urgent that a legislated privacy safeguards framework for smartphone apps be implemented if the Alberta Government is considering using them for contact tracing or quarantine enforcement. In the United Kingdom, where the government is said to be developing its own contact tracing app, several scholars drafted model legislation for the purpose of safeguarding privacy: *The Coronavirus Safeguards Bill 2020* (see also comments of the lead drafter here). These safeguards include some existing privacy safeguards, but also include new safeguards and safeguards that are designed to apply to smartphone contact tracing explicitly. In particular, the model legislation draws from human rights, where the question is whether the types of cellphone tracking proposed are prescribed by law with a legitimate aim, and complies with principles of necessity, proportionality, transparency, accountability and due process.

In our view, *a similar model should be legislated in Alberta prior to the use of any location tracking or proximity detection for the purposes of contact tracing or quarantine enforcement*.

Michael Geist has suggested several important safeguards for the Canadian context. Our privacy commissioners, provincial and federal, should be involved in an ongoing way in the development and implementation of these safeguards, but with a recognition that their role is limited to the specific legislation within their remit. In this unprecedented emergency, broader privacy and technology issues should be considered which requires a broader group of specialists at the table.

Some initial ideas about the key safeguards for such a model law, and influenced by the work in the United Kingdom, include:

- **Transparency**

    - This should be an overarching requirement that follows the lifecycle of data – what is collected, by whom, for what purpose, shared with whom
- **COVID-19-Specific Data Safeguards**
    - There should be clearly defined limitations on the collection, use and sharing of data, which should all be for the purposes of COVID-19 reduction only, limitations on the decisions that can be made on the basis of the data, about who can demand that a user provide the data (e.g. law enforcement), the imposition of a short data retention period, and the requirement to delete or anonymize the data.
- **User Empowerment**
    - Users should not be subject to liability of any sort, or be penalized because they did not have a smartphone, do not have their phone turned on or with them, did not download an app, or enable Bluetooth or similar unless any of these requirements can be demonstrably justified (e.g., through familiar human rights tests) and these privacy safeguards are in effect.
- **Oversight**
    - There needs to be active oversight of the deployment of this emergency system through the privacy commissioner's office or a similar deputized commissioner. There should be public reports about the activities related to COVID-19, and there should be an avenue for an individual to be able to challenge that their rights have been infringed in a timely way (i.e. provide due process).
- **Privacy by Design**
    - Software or technology used for contact tracing or enforcing quarantined must be designed so as to preserve privacy. It is a consequence of this requirement that centralized location tracking should not be used because it does not protect privacy as much as alternatives.
- **No Contracting Out of Privacy Rights**:
    - Neither the Government of Alberta, nor the licensor of the software or technology can require that, as a condition of using the technology, the user contracts out of their privacy rights and remedies, agrees not to sue, indemnifies the licensor and/or Government, or releases them from liability for privacy

infringements.

To be clear, while we recommend that special privacy safeguards be provincially legislated for the use of contact tracing or quarantine enforcing software, the provincial government and its officials will also have to comply with federal legislation that protects privacy, such as provisions in the *Criminal Code*, RSC 1985, c C-46 and *Canada's Anti-Spam Legislation*, SC 2010, c 23, where applicable.

Charter Rights in an Emergency

It needs to be kept in mind that governmental powers to require the downloading and use of smartphone apps are inherently limited by the (constitutionally protected) human right to privacy. The *Public Health (Emergency Powers Act, 2020)* may make it seem that a ministerial order that requires the downloading and use of smartphone apps would be automatically valid law. But since privacy rights are protected under s 8 of the *Canadian Charter of Rights and Freedoms*, s 1 of the *Charter* requires that "reasonable limits prescribed by law" must be "demonstrably justified in a free and democratic society." Without going into a full analysis, this means that any departures from the safeguards provided by privacy law must be justified in order to be valid law. Such a justification would likely preclude the use of centralized contact tracing software because it does not impair the right to privacy "as little as possible": See *RJR-MacDonald Inc. v. Canada (Attorney General)*, [1995] 3 SCR 199 at para 60. Of course, a provincial government can invoke the notwithstanding clause in the *Charter*, allowing it to legislate notwithstanding the infringement of guaranteed privacy rights (see s 33), but to do so would likely undermine public confidence in the government's efforts to limit the spread of the SARS-CoV-2.

Conclusion

The use of contact tracing apps has become increasingly common during the global COVID-19 pandemic. Recently, the Premier of the Government of Alberta said that the Government will use smartphone apps or technology to enforce quarantines. Given the widespread use of location tracking software and a potentially successful use of it to enforce quarantines in Alberta, the Government of Alberta may be tempted to require the use of that tracking software for contact tracing. We have argued that the human right to privacy is valuable, that privacy should be protected as much as possible during this pandemic, and designed into contact tracing software.

But the use of centralized tracking software does not protect privacy as well as decentralized proximity testing using Bluetooth enabled devices. Moreover, the Government should consider developing draft legislation of the kind suggested in this post in order to protect privacy during the pandemic, if it uses technology to enforce quarantines and do contact tracing. Protecting privacy in this way will instill greater confidence in the public to use technology that assists in diminishing the transmission of the SARS-CoV-2.

[*] Joel Reardon is an Assistant Professor in the Department of Computer Science at the University of Calgary. Emily Laidlaw is an Associate Professor in the Faculty of Law at the

University of Calgary. Greg Hagen is an Associate Professor at the Faculty of Law at the University of Calgary.