CANADIAN CIVIL LIBERTIES ASSOCIATION

2020

Privacy, Access to Information, and You: The COVID-19 Edition

DR BRENDA MCPHAIL; DIRECTOR OF THE PRIVACY, TECHNOLOGY, AND SURVEILLANCE PROGRAM
CARA ZWIBEL; DIRECTOR OF THE FUNDAMENTAL FREEDOMS PROGRAM
JIANYANG (JY) HOH; LAW FOUNDATION OF ONTARIO PUBLIC INTEREST ARTICLING FELLOW

Table of Contents

WHY PRIVACY? WHY NOW?

When we're in the middle of a global pandemic, why should we care about privacy? After all, everyone in Canada is facing extraordinary restrictions on our civil liberties at present, due to emergency measures that have been enacted federally, and in every province and territory. We're self-isolating. Those of us who can are working from home, and non-essential businesses have been ordered to close. We're limiting our trips out of the house to essential trips for groceries and prescriptions. When we make those trips, we're practicing physical distancing, and if we fail to do so, we risk a hefty fine if we get caught.

In this context, privacy might seem like the least of our worries. But consider this:

1) Health information is widely acknowledged to be one of the most sensitive categories of personal information. In the current health crisis, there are real tensions between the need for the public to have the information about how many people are sick in their city and province or territory to support their own efforts to stay safe and informed, and providing a level of detail that would permit identifying individuals;

2) There are widespread demands from the public, and intense interest from governments around the world, to use technology—to find a silver bullet app-- that will help in efforts to contain the virus. But many of the technologies being discussed, particularly those that are proposed to assist in contact tracing or risk assessment of individuals, require granular information about us which may include location information (about us and others we come into contact with), symptom information, and diagnosis information. And many of them involve public private partnerships which opens up questions about public health and profit motives potentially mixing;

3) Choices we make now about information sharing and encouraging the use of technologies for tracking humans as a way of tracking the spread of COVID-19 are going to have an impact on our privacy when the crisis is over—if there's one thing we know, it's that technology doesn't go backwards, and there's a real risk that if we take measures now that we consider necessary in the current state of emergency, it will be difficult to dial them back later unless the right legal, policy, and technical constraints are in place from the start;

4) Critical decisions are being made by governments, facilitated by emergency measures legislation. Privacy and Access to Information legislation complement one another. Access to Information gives us the ability to hold our leaders accountable for their decisions more important than ever. At the same time, our federal access to information system is, as described by the Information Commissioner of Canada in an open letter, "currently in a critical phase and may soon be beyond repair if certain ongoing and developing issues remain unaddressed." This potential failure affects the ability to acquire and evaluate documents that reveal government processes and the basis on which pandemic-related decisions were made, and is a real and present threat to transparency and accountability during and beyond the current crisis.

And all this is happening in a climate where people are afraid, and politicians are under intense pressure to do something—or many things—to ease that fear. But it is precisely when we're afraid that we might be inclined to offer up the rights we normally hold dear in exchange for safety—or even just feeling safer, which is not the same thing. That's why CCLA, with generous support from the **Ken and Debbie Rubin Public Interest Advocacy Fund**, has created this resource, "Privacy, Access to Information, and You: The COVID-19 Edition." It's going to grow, become more interactive, and be updated as privacy and access evolve during the current public health crisis, in an effort to provide information and encourage critical thinking and public engagement with issues of rights and state accountability during these turbulent times.

OVERVIEW OF PRIVACY LEGISLATION IN CANADA AND WHERE IT FALLS SHORT

Privacy law is generally divided into two types: **those that govern the private sector**, and **those that govern the public sector**. These types can be further subdivided into federal and provincial laws. These laws are overseen by federal and provincial privacy commissioners, which are independent bodies that answer to their respective legislatures and have a mandate to protect privacy.

The main federal privacy law for the private sector is the **Personal Information Protection and Electronic Documents Act (PIPEDA)**.

PIPEDA covers private sector organizations that handle personal information in course of commercial activity, such as airlines or banks. For example, a bank handles your personal information when it asks for your name and address in the course of setting up your savings account. Businesses that are based in Canada but handle personal information across national borders are also subject to PIPEDA. At the provincial and territorial level, three provinces (Alberta, BC and Quebec) have privacy laws that are substantially similar to PIPEDA; the organizations that are subject to these provincial laws are exempt from PIPEDA. Organizations in all three territories are federally regulated and are thus covered by PIPEDA. Several other provinces (Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador) have health privacy laws which provide substantially protections, similar to PIPEDA, specifically to health information.

The main federal privacy law for the public sector is the **Privacy Act**. The Privacy Act sets out your rights in relation to your personal information when it is handled by federal government bodies – for example, the Canada Revenue Agency has your name and address on your tax return. Each province also has different public sector privacy laws that set out your rights in relation to your personal information when handled by provincial (and sometimes municipal) government agencies, such as Alberta's Freedom of Information and Protection of Privacy Act and Ontario's Municipal Freedom of Information and Protection of Privacy Act. A full list of privacy laws by province can be found here.

These privacy laws are long overdue for an overhaul - the Privacy Act is ***more than 35 years old***. The outdatedness of the legislation is compounded by the exponential pace at which modern technology develops. PIPEDA is focused on data protection – trying to make sure that companies that collect, use or store your personal information, which can include anything from your name to your picture to your genetic code, follow fair information practices. Data protection is important but ill-suited to protect against other kinds of threats to privacy and other human rights. For example, data protection rights are not a good fit for corralling facial recognition technology, which enables surveillance that poses an unprecedented threat to privacy rights. PIPEDA and other privacy legislation should be updated to adopt a rights-based approach, which will grant privacy law the flexibility to protect Canadians in the face of constantly metamorphosing privacy threats.

Another shortfall in the current law is that **most privacy commissioners do not have the authority to enforce their recommendations**. Breaches of privacy law must often be dealt with under lengthy criminal prosecutions, which require discharging a higher burden of proof. In March 2020, however, Ontario empowered its privacy commissioner to issue administrative fines for infringements under its health privacy statute, a first in Canada. Ontario's example should be followed by the other provinces and the federal government so that the guardians of privacy have robust powers to do their jobs.

WORDS IT HELPS TO KNOW WHEN DISCUSSING PRIVACY

While privacy laws may vary by municipality, province, or country, certain privacy concepts are common to most locations. This section provides brief explanations of consent, surveillance, and data collection.

Consent

Consent is a foundational principle of PIPEDA. PIPEDA requires organizations that wish to use, collect, or disclose your personal information to first obtain your consent. Consent must be meaningful, which means that organizations must provide you with clear information about why they are using, collecting, or disclosing your personal information. Consent is usually express (actively given) but can sometimes be implied (inferred from the circumstances).

One example of consent is when you are prompted to agree to a privacy policy before you install a new application on your phone. As anyone who has ever "agreed" without reading the full privacy policy might understand, consent may never be truly meaningful in the digital age.

Privacy policies are often incredibly long and drafted in unreadably technical language – but if you do not agree to them, you cannot access the software. Suggested fixes for these problems include using shortened privacy policies or seeking consent at the time the information is collected, rather than at the installation phase.

Surveillance

Simply put, surveillance refers to "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (a definition from surveillance studies scholar David Lyon). Surveillance is a tool used in a variety of contexts. A lifeguard at a pool surveils swimmers to prevent drownings. Police surveil protesters and activists. Companies surveil our browsing activity online to decide how to market to us, what to market to us, and sometimes how to make decisions about us.

The first two examples might both sound like positive, protective forms of surveillance to some, while others, including CCLA, would worry about harms to free expression, association and open political discourse caused by surveillance of dissent.

Online tracking feels innocuous, maybe even beneficial to some (get ads that interest you!) but carries risks we're just beginning to understand for social sorting, hidden forms of discrimination, and behavioral manipulation.

Surveillance (continued)

There are many technologies of surveillance: surveillance cameras, satellite imagery, and geolocation tracking are some of the more familiar kinds. However, new technologically-mediated forms of surveillance are quickly emerging – facial recognition, which is currently used by Canadian police, and social media surveillance, such as the kind that was exposed in the Cambridge Analytica scandal.

Data collection

Data collection occurs whenever an organization gathers information of any kind. Thus, data collection is happening whenever you fill out a driver's license application form, withdraw money from an ATM, or indicate that you are attending an event on Facebook. Canadian privacy law imposes some requirements on organizations that collect your data.

Data collection (continued)

However, these laws are outdated and cannot account for the speed and scale at which data collection is conducted today, or the ways in which it can be used. Tech giants such as Google or Facebook harvest vast amounts of data from their users to sell to advertisers, which has become their core business model.

So much data is collected from you that tech companies are able to use it to construct extensive personal profiles; it has been said that these companies know us better than we know ourselves. Massive amounts of data are also necessary to train algorithms, which are essentially sets of rules for computer processing; algorithms are used for everything from assessing job applicants, to immigration applicants, to facial recognition.

The new normal of data collection not from individuals directly, but behind the scenes from their behaviour and activities online, combined with new incentives to maximize such collection, demands new privacy rules to keep up.

WHY DOES PRIVACY MATTER DURING A PUBLIC HEALTH CRISIS? FREQUENTLY ASKED QUESTIONS

Q1: Why should I care about privacy when the pandemic is threatening my life? The government can track me and my contacts if it wants to protect public health – I don't have any use for privacy if I'm dead!

A: It is a myth that we must choose between privacy and public health (or privacy and almost any other public good). It is often entirely possible to accommodate both. And let's be clear, no one is saying that if we were to give up all our medical and location and contact information we'd be safe—at best, the arguments for trading privacy for health purposes focus for the moment on better tracing the disease's progression through our communities. It's about better managing risk, which is important, but no silver bullet guaranteeing anyone's absolute safety.

Caring about privacy does not mean that we must always reject public health measures such as technologically-assisted contact tracing—assuming they are actually driven by explicit, documented public health needs. It simply means that we should ask questions about whether such measures are necessary as per the scientific evidence, if they can be effective (and that's a big unknown at this time), and if they can be shown to meet both those criteria, how they can be crafted to ensure the best possible public health and privacy outcomes.

It's also important to consider proportionality: basically, are the privacy risks, and other risks that come from surveillance that people are being asked to accept worth it when compared to the potential benefits to individuals, and/or to society? Those other risks include risks of discrimination, if apps result in people being denied access to essential services, stigmatized because of their health status, or being asked to give up liberty and quarantine based on incorrect information.

It's no wonder, given these real risks, that around the world and here in Canada, rights protection is big concern for people when it comes to potentially using such apps. Only if these tools can be shown to be likely effective under current conditions, designed with strong technical privacy protections built in and strong privacy safeguards in the policies and protocols for their use to mitigate knock-on effects of surveillance, will enough people consider voluntarily downloading them to make a real difference.

Governments know that times of fear provide the best cover to restrict fundamental rights like privacy. By surrendering our freedoms because we are scared, we play right into their hands. After the pandemic ends, we will still have to deal with the surveillance systems and privacy restrictions that have become normalized. We must therefore fight for the best possible outcome: a healthy populace that has its privacy intact.

Q2: Do I have to tell my landlord if I or someone I live with has COVID?

A: You are under no legal obligation to inform anyone of your COVID status. Your personal health information is only one person's business – your own. While landlords can request that residents tell them if they contract COVID, it is illegal for landlords to force you to reveal COVID status information or treat you differently, whether you refuse to do so or you disclose that you do have COVID.

Q3: What steps can I take to protect my privacy during the pandemic?

A: You can ask your elected representatives about the many laws, regulations, and orders that are passed every day. Ask them whether each measure is supported by public health evidence and about the steps they have taken to ensure that each measure violates privacy as minimally as possible.

Avoid engaging in privacy-violating activities such as calling in snitch lines to report what may seem like violations of social distancing guidelines. When we create a culture of fear-based reporting on others, public trust plummets, and nobody wins.

And think about your choices when it comes time to download new technologies. Take a second to look up a review, or a few minutes to glance through the privacy policy. In many cases, there are different options to accomplish the same task, pick the one that works for you AND offers the privacy protection you deserve, if you can.

PRIVACY AND THE PANDEMIC

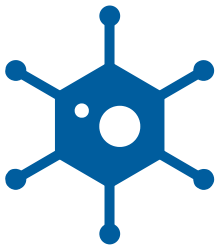
An ongoing compilation of current issues, with explainers and links to media stories

Technology and cellphone companies handing over consumer data to governments for surveillance or contact tracing

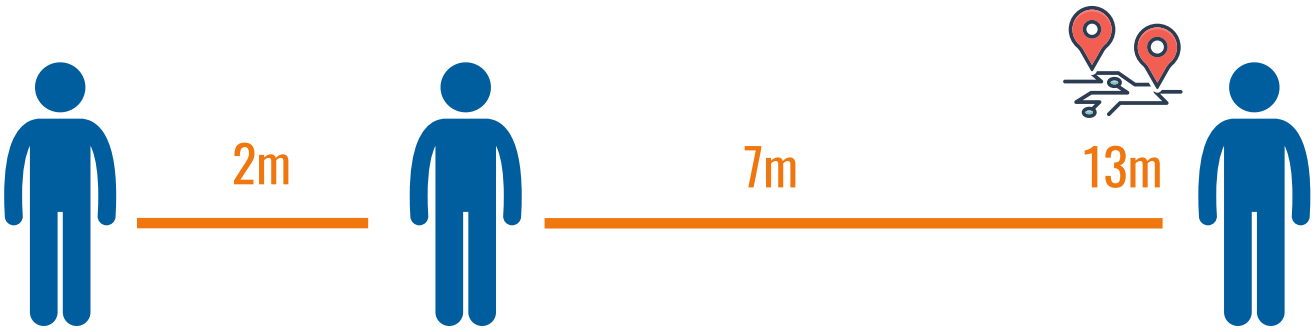
Ever since countries such as Taiwan and South Korea have used advanced technology to trace those who have contracted the coronavirus (a process known as “contact tracing”), there have been calls for Canada to do the same. Technology-assisted contact tracing, it is suggested, may assist Canadians to return to a semblance of normalcy, and privacy does not require that such technologies be avoided altogether – it is a myth that privacy and public health must be at odds.

However, there is a real debate to be had over whether technologically assisted contact tracing will actually work under current conditions (which include limited testing capacity), and over the form that it should take. If respect for human rights is built into the system's design, then the tool may be acceptable to enough people to encourage voluntary use.
If governments capitalize on the crisis to expand the technological surveillance state, then the tool deserves to fail due to public mistrust, and the damage to privacy will likely last long after the public health emergency ends.

One frequently discussed but dangerous model would be the government tracking of mass location data. Under this model, the government would collect citizen cellphone location data from cellphone companies. The government would then use the location data of someone who has tested positive for the coronavirus to identify who else has come near that person. Anyone who has been contacted would then be ordered to come in for testing or potentially subject to quarantine orders. Location data could also be used to determine compliance with quarantine orders once they have been issued. This model was approved in Israel, to be executed by their internal security police, the Shin Bet. The Israeli Supreme Court recently sent the emergency legislation back to the drawing board, saying it failed to sufficiently protect citizen privacy rights.



This model would be problematic for numerous reasons. First, it is unclear whether it would even be effective because cellphone location data is often not precise enough to correctly identify potential virus transmission. Coronavirus transmission is believed most likely to occur within a 2 metre radius, and global positioning system (GPS) location data is rarely that accurate - one study has found an average accuracy rate of 7 – 13 metres. The relative inaccuracy of GPS should be evident to anyone who has tried using Google Maps near large buildings only to find their location pin bouncing erratically. The other option, cell tower location tracking, is even less accurate than GPS. China, no stranger to surveillance, investigated and rejected location-based tracking because it was too imprecise.



More importantly, however, governments that create large surveillance systems are unlikely to relinquish them – especially a geolocation-based system, which would be very useful for surveillance. While GPS tracking is not precise enough to identify virus transmission, it is certainly precise enough to place people at anti-government protests or the scenes of alleged crimes. Generally, when governments propose such systems, they seek to normalize their use amongst the populace. Then, they can be used for surveillance purposes other than public health, such as law enforcement. Without the proper privacy safeguards and oversight, allowing these systems to be used even over a short period will tempt governments to cling on to them after the crisis is over.

Another model is contact tracing by Bluetooth. Bluetooth is a widely available technology that enables phones to wirelessly exchange data with other phones in proximity. Apple and Google have announced that they are developing an app that would emit random numbers that change at intervals. If users of the app walk within a prescribed range of other users, their phones would exchange the numbers to create a record that is devoid of directly identifying information. If someone tests positive for COVID, they can upload their app's numbers to a centralized database, which will enable other users to check if they had exchanged numbers with the infected person because they were within proximity.

Advocates of a Bluetooth-based system, such as the American Civil Liberties Union, argue that it is superior to a location-based system both in terms of effectiveness and privacy. It is less vulnerable, so the argument goes, to government overreach; even if they could access the database, they would only be privy to a set of meaningless numbers. However, even a Bluetooth-based system has flaws. Data can never be truly anonymized, even if directly identifying information is removed; a determined surveillance specialist could cross-reference the numerous associations between phones with other data to identify individuals. Furthermore, Bluetooth-based location tracking has, like cellphone location tracking, also produced false positives. False negatives are also a risk. For example, many contact tracing apps base part of the risk assessment on duration of contact, and set a time frame ranging from 5-30 minutes for a contact to be recorded. Spending 30 minutes 6 feet apart from someone in a grocery lineup, both wearing masks, would register on most apps as a contact yet be relatively low risk, while a passing encounter where a maskless bypasser sneezed towards you could carry more risk, yet fail to register as a contact. The former example might register a false positive if one of the two shoppers reported a positive covid test, while the latter would be a false negative if the sneezer turned out to be carrying the virus.

Whatever form contact tracing takes, it should accord with the following privacy principles. First, government contact tracing that relies on data should be a last resort. It should only be used if public health evidence demonstrates that it is necessary because traditional contact tracing cannot work to satisfactory effectively. The privacy-invasive aspects of the measure should be proportionate to the evidence-based public health benefit. Consent should be paramount – no one should be compelled by law to download contact tracing apps. The government must also ensure that independent bodies review any such measures to provide oversight of the measures' effects on vulnerable populations, to ensure that the data is not used improperly, and to adjudicate complaints and report them to the relevant legislative body. CCLA's full set of recommendations on technologically-assisted data surveillance during the pandemic are here.

Recent Ontario order authorizing first responders to pull any Ontarian's name, address, date of birth, and COVID test status

How would you feel if complete strangers could find out whether you or anyone in your family has or had COVID-19? What if that information, along with your address and other personal data, was stored and shared over the internet or downloaded onto computers accessed by first responders? That has been the reality in Ontario since the provincial government passed Regulation 120/20 (also called "O Reg 120/20") on April 6, 2020.

O Reg 120/20 was intended to allow first responders such as firefighters, police officers, or paramedics to check, for example, whether a residence's occupants have COVID-19, so that they can take the necessary precautions before they show up.

O Reg 120/20 empowers these first responders to ask for a person's name, address, date of birth, and whether they have positive COVID-19 test results. While privacy law would normally prevent medical personnel from revealing such sensitive personal health information, O Reg 120/20 overrides that principle to protect first responders. It's not clear how it is necessary, however; surely first responders should be taking universal precautions on the grounds that anyone they come into contact with may be infected—particularly given the paucity of testing, and the reality that individuals are likely infectious well before showing symptoms, never mind having a positive test.

An additional problem is that the regulation is sloppily worded, any first responder could pull the COVID status of any person in Ontario, regardless of whether the first responder will even be making a call at that person's house. The only restriction is that the data must be used to "prevent, respond to or alleviate the effects of the emergency". The law does not provide any penalties for a first responder who uses or discloses the data for other purposes; abusers will get away scot free. The regulation also places no time limit on pulling information – but why would a first responder need to know that someone tested positive for COVID-19 30 days ago, when the virus' incubation period is 14 days?

There are numerous ways these loopholes could be abused, especially considering the irrational human tendency to stigmatise those who have contracted infectious viruses. If your vengeful ex happens to be a firefighter, they perhaps might find out if you have or had COVID and publicize that information to try to shame you. A racist police officer could collate COVID-positive test data from persons of Chinese descent to support the narrative of a Chinese virus and that Chinese persons should be avoided.

None of this is to say that first responders are especially prone to misbehavior – far from it. But first responders are human, too, and humans make errors of judgment. Privacy-implicating regulations should therefore be carefully drafted to ensure that such errors are not accidentally authorized.

Once the information has been harvested, however, the manner of its storage also raises privacy issues. O Reg 120/20 is silent on how long authorities are allowed to retain the COVID status information. Thus, once collected, the information could theoretically be kept indefinitely, which renders it vulnerable to data privacy breaches. Even if the first responders do not misuse the data, storing it for too long creates the risk of other malicious actors accessing the data for their own ends. This is not mere theoretical risk; government data breaches are common in Canada.

Thus, the regulation should be narrowed so that such information can only be pulled if the first responder is about to come into close contact with the person in question for the purposes of discharging their first responder duties. The regulation should also prevent the first responder from disclosing the information to anyone, and the data should be destroyed after the 14-day coronavirus incubation period has expired. To ensure that there is effective oversight, the system that contains the data should feature a log that tracks which first responder accessed data COVID status data, when they did so, and for what purpose. This will ensure that there is accountability for abuse and that data is destroyed promptly when it is no longer relevant.

Ontario's Pandemic Threat Response (PANTHR) - health data sharing initiative

Ontario recently announced a new health data-sharing initiative, the Pandemic Threat Response, abbreviated PANTHR. Pandemics require responses, and it may well be appropriate to use health data to address a public health crisis. But health data is also sensitive, and PANTHR, however well-intentioned, could lead to Ontarians' health data falling into the wrong hands. The basic intention behind PANTHR is to help the provincial government coordinate its pandemic response by pooling different types of citizens' healthcare data. Some examples of this data include the Ontario Health Insurance Plan (OHIP) billings that result whenever you visit your doctor, or the summaries of your discharge from the emergency room if you were unlucky enough to visit. Before PANTHR, that information was scattered in different locations. PANTHR will collect all that information and put it in one place, to be used by researchers to create models that predict where outbreaks are likely or how to optimally distribute healthcare resources.

The problem is that the data that PANTHR would collect is sensitive because it pertains to health – for example, not many people would want strangers to know that they contracted a sexually transmitted disease, or that they use anti-anxiety medication. And realistically, most patients would not expect that by seeing a doctor, they are agreeing to sharing that information for research purposes. That data should be private, and it is troubling to think of it all concentrated in one place for government researchers to pore over.

Ontario's solution is that the health information will be "de-identified", an oft-misunderstood term. De-identification is the process of stripping data of directly identifying information such as

names or addresses in an attempt to make the data untraceable to individuals. The confusion over de-identification is that it is often assumed that once data has been de-identified, there is no risk of re-identification. However, it has been repeatedly proven that no de-identification process can completely remove that risk – external data can be cross-referenced with allegedly de-identified datasets to reveal individual identities. In one experiment, researchers used cross-referencing to glean the identities of persons who had taken certain taxis in New York City, even though the researchers were only provided with the trip routes and no other identifying information.

Another concern is an assumption that once de-identification occurs, the data is no longer protected by privacy law because it is no longer personal—but increasingly in the privacy community, this assumption is being questioned. De-identification is a use of personal information, and uses of personal information (particularly in light of the re-identification risks) are arguably under the purview of our privacy regulators. PANTHR's application is still shrouded in secrecy. It is therefore important for citizens to remain informed and to ask their elected representatives for answers; this is even more crucial considering that these changes are often passed secretly and obfuscated by technical language. It is crucial for Ontarians to clearly assess each new initiative dreamt up by the government. Data sharing to improve a pandemic response may be necessary. Data sharing that leads to surveillance or data leaks however, is unacceptable.

Law enforcement officers demanding identification and collecting information about journeys to assess if they are 'essential travel'

Imagine you are driving from Montreal, QC to Bas-Saint-Laurent, QC. As you near the region, you slow down for one of the recently established roadblocks. A police officer stops your car and asks for your identification and the purpose of your travel. You are there to bring some supplies to your disabled grandmother, and you have heard that interprovincial travel is permitted for "humanitarian reasons." The police officer scribbles down some notes but denies you entry – your reason is not humanitarian enough because your grandmother may be disabled, but she is not sick with the coronavirus. You try to protest, but there is nothing you can do, so you turn around.

It is important to understand that some of the new emergency orders and rules that are in place are without precedent in Canadian history and have not been tested before our courts. It is an open question whether restrictions on travel within a province and restrictions on interprovincial travel would be considered justifiable by a court if challenged. And challenges to laws that may be unconstitutional are difficult to mount at a time when courts are not sitting regularly and are focused on hearing urgent cases. Even if we are willing to accept that there will be some possibly unfair restrictions on our rights during a pandemic, what if the consequences of those restrictions live on well after the emergency is over?

What happens to the officer's notes of your having attempted to enter Bas-Saint-Laurent on that day, and the reason that you did it? What happens to that record establishing that your grandmother is

disabled, which is tied to your identification? Unfortunately, none of the emergency orders that authorized the police to establish roadblocks and ask these questions contain any privacy protections. The police could create a database of what they have learned from this questioning and use it to inform future law enforcement and crime prevention efforts. That information could sit in a police databank for years, and could also result in public disclosure in the event of a data breach.

The privacy intrusion of police officers asking after and recording police information is not the only disturbing thing about the interprovincial barriers. These orders were hastily drafted and give police and bylaw enforcement officers a lot of discretion. For example, are police really equipped to adjudicate whether someone's travel counts under "humanitarian reasons"? Clearly there was an attempt to make sure that some travel could continue despite the circumstances. But the provinces should also have taken privacy into account so that the information that arose from that questioning could not be used for improper ends or retained indefinitely.

OVERVIEW OF ACCESS TO INFORMATION

Access to information laws (also called freedom of information laws) are intended to do what you might expect – to provide individuals with access to information that is held, and often created, by the government. The idea underlying this kind of law is simple: governments are acting for the people they represent and using their tax dollars to create and collect information. Viewed this way, the information doesn't belong to government – it belongs to all of us and therefore should be made available to us.

Access to information laws can be used to better understand the process of government decision-making, to get at the data that governments hold, and to help hold the government accountable. It is a tool that is often used by journalists and academics but can also be used by the general public – we have the right to request government information for our own interest and purposes. For example, you may wish to know whether your local police force is using a controversial new facial recognition technology. An access request can help you find out.

Canadian courts have recognized that accessing government information can be crucial to allowing us to exercise our freedom of expression, which is a right protected by the *Canadian Charter of Rights and Freedoms*.

This does not mean that there is a right to all information held by government, but it does acknowledge that if we don't know what government is doing and aren't able to make informed assessments of their policies and approaches, our democracy suffers. As you might have guessed, access to information laws themselves don't always work in an easy or straight-forward way. Canada's access to information laws allow governments to refuse to provide access to information on a wide variety of grounds, and sometimes these exceptions seem so broad that the purpose of access to information laws is frustrated. For example, under Canada's *Access to Information Act*, access to records may be denied if their disclosure could be considered harmful: to provincial-federal relations, to international affairs, to the financial interests of the country or a government institution, and on and on. Refusals to provide information can be based on a significant number of broad categories. There are freedom of information/access to information laws in place in all of the provinces and territories as well as at the federal level. Many jurisdictions combine access to information with protection of privacy legislation. For example, Ontario has the *Freedom of Information and Protection of Privacy Act (FIPPA)* to deal with matters of personal privacy and access to information held by government departments at the provincial level. It also has the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* which deals with the same topics at the local level.

At the federal level, Canada's *Access to Information Act* was seen as groundbreaking legislation when it was passed in 1983 and was used as a model for other countries. Unfortunately, the law is now quite outdated and there have been lots of calls for reform. Some of the shortcomings of the Act and recommendations for its reform were highlighted in a March 2015 Report by the Information Commissioner of Canada, and a June 2016 Report of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

These reports and recommendations were made prior to changes to the Access to Information Act that were made in 2019. At that time, Canada's Parliament amended the law. Some of the more significant changes now require that government proactively disclose certain types of records without receiving a request. For example, travel expenses incurred by members of the House of Commons and Senate must be proactively disclosed within a certain period, as do contracts which they have entered. Certain briefing materials prepared for Ministers are also required to be proactively disclosed within a certain period, although the government has stated that proactive disclosure may be delayed because of operational constraints in place while Canada is dealing with the pandemic. Although some of the changes made in 2019 are positive, there are still many parts of the law that need reform. The federal government has committed to conducting a full review of the Act but it is not clear when that review will be complete.

MAKING AN ACCESS TO INFORMATION REQUEST

The process of making an access to information request will vary depending on which government institution holds the information. For now, let's assume that you want to access information held by a federal government institution. Your request will be dealt with under the federal Access to Information Act. Canada recently introduced a way to submit access requests online for some government departments. You can find out which departments are accepting online requests and complete a form to submit a request. In completing the online form you will also be able to find out if someone else has previously requested the same information and, if it has been released, you can also get access to it. If the relevant federal department is not accepting an online request, you can submit a request in writing and mail it to the department. There is a $5 application fee when you submit a request.

Under the federal law, the department that received the request for information is supposed to respond within 30 days, but these timelines can be, and frequently are, extended by significant periods of time. The institution may also decide, with the Information Commissioner's permission, to decline to act on the request if they think it is made in bad faith or is an abuse of the right to request access to records. If the institution does deal with your request and you are refused access to a record or parts of a record, or you think the delay in getting records to you is unreasonable, or you have been given a fee estimate for getting the information that you think is unreasonable, you can make a complaint to the Information Commissioner of Canada. This office has information about how to file a complaint, including the types of complaints it can consider, and a helpful list of FAQs. There is also a database of prior decisions that the Information Commissioner has made, which may help you decide whether to pursue a complaint.

If you submit a complaint, the Information Commissioner can choose to investigate it or decline to do so. If the complaint is declined, you should be given reasons in writing. If the complaint is investigated, you may be asked for more information or for representations (something setting out your position) on the complaint. If you receive a decision or report from the Information Commissioner about your complaint and you think there are reasons it should be reviewed, you can apply to the Federal Court of Canada. The government institution that received your request also has this right if they disagree with the Information Commissioner's report. Generally, these requests to the Federal Court must be made within 30 business days after the day the report was received by the government institution.

The specific rules in place for making access requests and complaints will differ by province or territory, but all jurisdictions have an information commissioner (often a combined information and privacy commissioner) or an ombudsman that can consider complaints regarding access to government information.

ACCESSING PERSONAL INFORMATION

Including health information

There is a difference between accessing general government information and accessing personal information that the government may hold about you. Generally, you have a right to request personal information that institutions have collected about you and to correct it if it contains mistakes.

You can reach out to the institution that has the information and request it. For example, if you want to find out what information a public health authority has collected about you, you should make a request to that institution directly. If you are not satisfied with the answer you get, or are struggling to get access to the personal information you want, there are bodies that oversee the operation of Canada's privacy laws that can help. There is a federal Privacy Commissioner and similar offices in each province and territory.

Requests for personal information are covered by privacy laws rather than access to information laws. In Canada, there are three kinds of privacy laws that might apply to personal health information:

1) health information privacy laws;
2) private sector privacy laws; and
3) public sector privacy laws.

Most provinces and territories in Canada have specific privacy laws that apply to the health sector or a private sector privacy law that has some application in the health information sphere; only Prince Edward Island and Nunavut have no such laws. Even in provinces that have health-specific laws, there may be some requests for health information that would come under a private sector or public sector privacy law.

The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* is an example of a private sector privacy law. It applies to non-government entities engaged in a commercial enterprise. It might apply to a private health care practitioner or institution in some provinces/territories. In some jurisdictions, PIPEDA and a provincial or territorial law will both apply.

The federal *Privacy Act* is an example of a public sector privacy law – it applies to information held about you by federal government departments. Personal information held by the Public Health Agency of Canada, for example, would fall under the Privacy Act.

Because of the overlapping nature of some of Canada's privacy laws, it may be hard to know where to go to request your information. The Office of the Privacy Commissioner of Canada has a helpful interactive tool to help you determine which law related to health information applies to you and which privacy commissioner's office could help deal with any complaints.

RESOURCES

If you want to request your personal health information from a specific institution, you can use this link to determine which law applies. We have also pulled together some resources in each jurisdiction that may be useful:

Canada
British Columbia
Alberta
Saskatchewan
Manitoba
Ontario
Quebec (English resources available)
New Brunswick
Nova Scotia
Newfoundland and Labrador
Prince Edward Island
Yukon
Northwest Territories
Nunavut