David Young Law
Compliance Bulletin

March 2020

Privacy in a pandemic

The Coronavirus pandemic has thrust privacy to the front lines of responding to the health emergency. What is becoming clear is the risk that a "surveillance society" could be the new norm coming out of the global response.

On the public health level, information about individuals, both specific and aggregate, is understood to be a critical tool in identifying risk centres and taking protective measures – with the goal of slowing spread of the virus. Within the private sector, surveillance techniques also are being operationalized, mostly for transparent, properly-intentioned purposes, but also for less clear and sometimes undisclosed reasons. Screening of employees for entry to work-places is an example of the former; undisclosed recording of video conferences is potential example of the latter case.

Privacy concerns intersect with strategies to assist both counteracting the spread as well as enabling workplaces and the broader economy to function normally. However, it is important to understand that the rule of law – particularly as reflected in our privacy laws – continues to apply.

The privacy laws are not preempted by the health emergency. On the contrary, they are written to contemplate substantially all of the extraordinary measures now being considered.[1] Furthermore, providing a rights-based oversight of the privacy laws, as well as of the public health and emergency measures laws, are the protections contained in the *Charter of Rights and Freedoms*. It is important to recognize that while the laws enable extraordinary measures in emergency situations they also stipulate limitations and protections. These protections are inherently part of the rule of law.

What is required in these exceptional times is a rules framework to govern how the permissions contained in the privacy laws should be utilized – addressing critical criteria including legal authority, proportionality, necessity and limitations on data use and retention.

Public sector privacy – testing and tracking

The advance of the virus south of the border has some important insights for Canadian and for that matter global pandemic response. It appears that any serious commitment to initiate pervasive testing of the

[1] Of note is the GDPR's Recital 46, addressing epidemics specifically:
The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest ... for instance when processing is necessary for ... for monitoring epidemics and their spread.

population was delayed by at least a month – meaning that with the bottlenecks now being experienced there is likely a very large number of people who may have the virus and either have already been infected or are now infecting others but against whom no protective measures have been taken. If their status were known, both retroactive and going forward measures could be instigated to protect others. Conversely, persons who are not infected could be cleared for more normal activities including potentially return to workplaces. The key correlative to such a testing strategy is the ability to track – both the persons who have tested positive as well as others with whom they may have come into contact. Tracking the positives both retroactively and prospectively can enable public health authorities to identify other potential at-risk persons as well as to monitor the positives' compliance with quarantine going forward.

It is clear that location data – collected by many mobile phone devices – is the most readily available source of information regarding individuals' day to day activities and, potentially, interactions with other individuals.

There has been much controversy regarding the use of private mobile phone data to track individuals identified as having or potentially having the virus.[2] [3]

Any such collection and use of personal information by a government entity is controlled by the "public sector privacy laws" which apply federally and in all provinces and territories, including at the municipal level.[4] The key requirement for such collection by a government entity is lawful authority – in other words specific legislation either permitting or requiring such collection. It is unlikely that authority for collection of phone location data would be found in existing laws; however it can be provided for in an emergency measures law.[5]

Linking location data to persons' medical record information also requires authority for disclosure of the medical record to the (presumably government) entity performing any analysis. Such authority - in circumstances involving health and safety - typically exists under the personal health information laws in most provinces and territories and in their applicable public health legislation.[6]

The public sector privacy laws do not require the consent of individuals for collection and use of their information, requiring instead, as noted, lawful authority and additionally, that the individual be notified of the

---

[2] See: https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

[3] While specific legislation could require telecommunications providers to disclose such data, the privacy policies of the telecoms that hold the location data typically contain provisions permitting disclosure in such circumstances as a term of their use of the provider's service. Consent per se is not required.

[4] At the federal level the relevant legislation is the *Privacy Act* and in the provinces and territories, legislation similar to the Ontario *Freedom of Information and Protection of Privacy Act* or the Yukon *Access to Information and Protection of Privacy Act*.

[5] To be noted, the City of Toronto's order declaring an emergency did not provide for the collection of cell phone data; see:https://www.toronto.ca/wp-content/uploads/2020/03/95d7-covid-19-order-mayor-chapter-59-2020-03-23.pdf

[6] See for example, Ontario's *Personal Health Information Protection Act, 2004*, subs. 40(1) and *Health Protection and Promotion Act*, s. 77.6

collection. A government entity also may *disclose* personal information if for a purpose for which it was initially collected, or in compelling circumstances affecting health or safety.[7]

The key points to understand are that **there must be *lawful authority*** for any collection of personal information – and that, if collected for example under an emergency or public health law, it may be used or disclosed but only for the purposes for which it was collected.

While the privacy laws provide the basic threshold requirement for any such linking – that data may only be collected and used for the stipulated, authorized purposes – they are thin on the ancillary rules that should accompany any such extraordinary new uses of personal information.

For example, typically, they do not expressly stipulate time limitations on retention of data, or provide for accountability and monitoring rules - in contrast to Canada's private sector privacy laws which do address such requirements.[8] For this reason, any authorization, whether it be pursuant to an emergency measures law, or in separate legislation, should provide for a clear and rigorous rules framework for such data collection.[9] Such a rules framework should be informed by societal and ethical standards reflecting the context of the current emergency.

Providing such a rules framework has another important purpose – to ensure compliance with the ultimate protective law against which any such health data use must pass scrutiny – the *Charter* right of individuals to be free from unreasonable search. This right, as articulated in numerous cases,[10] comes down to protecting an individual's "reasonable expectation of privacy"- characterized as embodying the personal goals of dignity, integrity and autonomy. Compliance with this requirement involves establishing that the law in question is reasonable, meaning that it recognizes the need for privacy intrusion and authorizes the least intrusion necessary. So clearly limiting both the purpose of the data collection and its retention will respond to this requirement.

Private sector privacy issues

Separate from the public sphere issues, privacy implications are relevant to remote working and learning, screening of employees, and generally, the burgeoning collection of data inherent in electronic interactions. These issues also extend to virtual health care provided by employers, as well as remote learning systems for children.

Guidance for compliance includes transparency – meaning clear notification to users – regarding collection, use, disclosure and retention/deletion rules as well as satisfying the criterion of "reasonableness". Employers must be mindful of the constraints under both the privacy laws and the *Charter* governing monitoring of employees.

---

[7] Or if otherwise required or permitted by law.
[8] For example Schedule 1 to the *Personal Information Protection and Electronic Documents Act*.
[9] See: *How invoking the Emergencies Act could help Canada better track, contain COVID-19*, CBC Opinion, March 27, 2020, Colleen M. Flood, Teresa Scassa, Dr. David Robertson.
10 See for example, *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at 159; *R. v. Gomboc*, [2010] 3 S.C.R. 211.

Particular attention should be paid to any further, secondary uses that might be made of information collected beyond the immediate purpose – such as unrelated workplace uses or future marketing. In this regard, organizations using new remote working tools should review carefully the privacy policies of their service providers and stipulate opt-outs for information use not directly related to providing specific service.

The global issue – do we want a surveillance society?

All of these instances of new or expanded data use in responding to the COVID19 pandemic entail more extensive – or new – modalities for collecting, using and disclosing personal information, in most instances relying on electronic systems and databases that collect and retain information as their default setting. As a general proposition, many more interactions are now being "documented" electronically, and potentially retained for future use, than was the case previously.

Public health applications to combat the emergency, with proper authority and appropriate protections, may be developed using personal information in ways not previously contemplated. However such uses must be clearly identified and limited to the purposes of fighting the pandemic.

Compliance with our accepted civil society and personal privacy norms – as reflected in the rule of law – behoves governments and businesses alike to observe a minimalist approach – the least invasion of personal privacy required for the objectives at hand. Electronic data applications and remote interactions can assist in both combatting the virus as well as making life as "normal" as possible. However they should not be an opening to a different, post-pandemic "big brother" world.

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.