Pandemics and Privacy: Key Privacy and Information Security Considerations

By David Elder

April 2020

Amidst the many challenges and uncertainties presented by the COVID-19 pandemic, many businesses are also grappling with the application of privacy laws and related information security obligations to their efforts to continue to operate while minimizing the potential for the virus to spread.

Potential business responses to the pandemic can involve the collection of a range of personal information (from employees, vendors, clients and any other visitors to an organization's facilities), and the use and disclosure of that data for purposes and in contexts that are well outside the ordinary. In addition, business continuity plans often involve radically different ways of doing business, such as having all, or a majority of, employees work from their homes. These approaches can present significant challenges to the maintenance and oversight of existing privacy compliance procedures and information security management frameworks.

Privacy laws allow for greater flexibility during a public health crisis

The good news, for businesses grappling with the ever-changing implications of the current public health crisis is that during emergency situations, each of Canada's private-sector privacy laws can allow for the collection, use and disclosure of personal information for purposes and in circumstances that would not otherwise be permitted, including processing without the consent of the affected individuals. In addition, as several Canadian privacy commissioners have taken pains to point out, privacy laws should not be a barrier to appropriate information sharing.

In particular, all of the private-sector privacy laws allow for the processing of personal information, without consent, where required by law, such as where an organization is required to collect or disclose certain information by a government public health body with the legal authority to compel such behaviour (for example as empowered under the various states of emergency and states of public health emergency that have declared by provinces and municipalities across the country). Privacy laws also contain explicit statutory exceptions or other flexibility that can allow for the collection, use and disclosure of personal information by businesses, without consent, where necessary to respond to an emergency situation.

The less good news is that the nature and scope of the flexibility allowed under Canada's four private-sector privacy laws varies somewhat from jurisdiction to jurisdiction. In this regard, there are provincially-enacted private sector privacy laws for each of the provinces of Alberta, British Columbia and Québec, each of which applies to activities within that province, as well as a federal law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) that applies to the handling of personal information in the course of commercial activity in the remaining provinces. PIPEDA also applies to all federally regulated works, undertakings and businesses, regardless of the province or provinces in which they may operate.

Accordingly, in considering any pandemic responses that implicate personal information, organizations must carefully assess the exceptions and requirements of the law or laws to which they may be subject. Such assessments can themselves be challenging, since there is little precedent in Canada for the application of privacy laws to a public health emergency of the scope and severity of COVID-19, and there is therefore some uncertainty with respect to how these laws will be interpreted and applied by privacy commissioners during this pandemic.

However, privacy laws continue to apply

While privacy laws provide organizations with varying levels of flexibility during emergency situations, they do not provide businesses with *carte blanche*: not all activities and initiatives involving personal information will be compliant simply because they were undertaken in response to a pandemic. Rather, in implementing any new pandemic-related measures that involve the processing of personal information, businesses must continue to be mindful of the continued application of the basic principles and requirements of private sector privacy laws, including the following:

1. **Consent**

   First and foremost, all of the private sector privacy laws generally require the consent of an individual for any collection, use or disclosure of his or her personal information, subject to certain narrow statutory exceptions. Accordingly, to the extent possible, all pandemic-related initiatives that involve the processing of personal information should generally only be undertaken with the consent of the individuals concerned, unless an exception applies.

   While PIPEDA and the laws in Alberta and BC explicitly contemplate that in certain circumstances, the consent requirement may be met by the collection of implied consent (i.e. consent inferred through conduct), express or explicit consent is generally required with respect to the collection and handling of sensitive personal information. Since health-related data is generally considered to be sensitive, it is likely, in the context of an organization's response to COVID-19, that the form of consent generally required by privacy laws will be explicit.

2. **Appropriateness**

   Even where the required form of consent is obtained, each of the private sector laws includes an overarching requirement that any processing of personal information must be appropriate or legitimate in the circumstances. In determining whether any processing of personal information is appropriate, privacy commissioners have tended to take into account the following factors, which are not exhaustive:

   a. ***The sensitivity of the personal information at issue***. While determinations of appropriateness consider a balance between individual privacy rights and business needs, a more stringent standard for appropriateness is applied with respect to processing involving sensitive personal information, which effectively tips the balance further toward individual rights. As noted above, health-related information is generally considered to be sensitive.

   b. ***The legitimacy of the objective of the measure undertaken***. Legitimacy could arise from a valid business interest or from a broader public interest; however, where sensitive information is implicated, privacy commissioners will also look to whether the initiative in question addresses a pressing or compelling need. It would appear likely that objectives relating to "flattening the curve" or otherwise minimizing the spread of the virus in or through a business facility would generally be viewed as both legitimate and compelling, although other objectives, such as managing corporate reputations, may not be, where they rely on additional collection or use of personal information, and particularly personal health information.

c. ***The effectiveness of the measure***. As part of their analysis, commissioners will assess the extent to which the measure in question achieves, or is likely to achieve, its objective. For example, initiatives undertaken to reduce the spread of the COVID virus within a workplace will be reviewed based on the likelihood that such initiatives are rationally connected to achieving that objective. Accordingly, if the objective is to reduce "community spread", is the initiative likely to have a material impact on virus transmission, taking into account a range of factors including available scientific data and public health agency guidance?

d. ***Whether less invasive solutions exist***. In determining the appropriateness of pandemic response initiatives involving additional processing of personal information, commissioners will also assess the extent to which there may be less invasive means of achieving the same ends at comparable cost and with comparable benefits. In this context, regard may also be had to the practices of comparable organizations.

e. ***Proportionality***. Finally, privacy commissioners will consider whether, considering all relevant factors, the intrusion on personal privacy arising from a particular response initiative is proportional to the perceived benefits of that initiative.

3. Minimization

A fundamental principle underlying privacy laws is data minimization, requiring that organizations collect only the personal information that they reasonably need, use it only for the purposes for which it is reasonably required, and retain it for only as long as is necessary to fulfill those purposes. The principle also encompasses the requirement that personal information should only be accessible by employees of an organization on a "need-to-know" basis, i.e. where reasonably required for them to perform their job function. Similarly, where an organization engages a third party to provide a service on the organization's behalf, the third-party should receive/have access to only the personal information required to provide the service for which it was engaged, and to restrict access by its own employees to a "need-to-know" basis. The minimization principle is particularly important when dealing with sensitive personal information, such as health-related data.

4. Confidentiality and Security

Even in times of emergency, where a privacy law may authorize additional collection, use or disclosure of personal information without consent, an organization's statutory obligations respecting confidentiality and security continue in full force – and apply with respect to <u>all</u> personal information retained and used by an organization, not just information collected as part of a business's response to the COVID-19 virus. Unfortunately, a sudden move to a work-from-home model can present significant challenges to meeting these obligations.

Privacy laws require that organizations maintain the confidentiality of all personal information under their control, preventing access to that data by any unauthorized parties. Organizations are further required to protect all personal information under their control with physical, organizational and technological safeguards appropriate to the sensitivity of the information. The rapid movement from operations conducted at a company-controlled and secured facility to a work-from-home business model can present many challenges to continued compliance with these obligations.

Some organizations will already have had in place secure remote access solutions for employees working remotely. Others will have had to scale up existing solutions rapidly, and some may have been starting from scratch – but all need to give careful consideration to ensuring the continued confidentiality and security of personal information in a widely dispersed, home-based work environment. This is particularly the case for businesses without existing remote access solutions, which may have made the cut-over to a work-from-home model virtually overnight. The many potential compliance issues with remote access can include the following:

- **Insecure physical environments**. Depending on their living arrangements, the premises from which employees may be accessing or storing personal information may not be physically secure, increasing the risk of unauthorized access and use. In addition, even within the premises, room-mates, family members and other unauthorized persons may have unrestricted access to an organization's systems or hard-copy documents, or may inadvertently overhear conversations in which personal information of a customer or employee is discussed. Care should be taken to remind new home-workers of their confidentiality and security obligations, and they should receive training about secure home-working.

- **Insecure processing and communication devices**. In some cases, employees may be using their home or other personal computers, tablets, smartphones and other devices to access and work on material that includes personal information. These devices may not have adequate password, firewall or malware protection, and may already carry malware or be subject to known vulnerabilities. All work-related tasks should ideally be carried out on employer-provided devices, or at least on employee devices that the business has taken steps to ensure are secure.

- **Insecure communications channels**. Workers may be using their personal email and social media accounts to communicate with co-workers, clients and suppliers. Such channels may not provide an adequate level of security. Workers may also be using unsecured home WiFi connections, or may be accessing employer networks based on inadequate authentication controls. Workers should be provided with secure encrypted channels through which to communicate for business purposes and access employer systems, and such system access should be secured by multifactor authentication solutions.

- **Insecure data storage**. Workers may be storing personal information on personal portable devices or free "cloud" accounts, both of which may provide inadequate security. Any electronic storage should be encrypted. For material in paper form, workers might leave sensitive material out for others in the household to view, or they may not have a means of physically securing such material. Handling of paper documents should be minimized, and where home-working employees require access to paper files containing personal information, locking filing cabinets should be provided.

- **Higher risk of scams and malware threats**. Particularly in unfamiliar and high-stress situations, workers can be vulnerable to phishing attempts, or malware installation through email attachments, etc. A number of such current threats have been identified. Employees should be reminded of protocols and tips for recognize scams and malware installation attempts.

Some privacy commissioners, such as the Information and Privacy Commissioner for British Columbia, have also issued tips and guidance for organizations setting up remote workspaces.

5. Employees

Private sector privacy laws tend to treat the personal information of employees differently from other types of personal information, with such treatment varying across the country.

Each of PIPEDA and the Alberta and BC private sector laws explicitly provides broad exceptions that allow an organization to collect, use and disclose the personal information of its employees without consent, where such processing is necessary to establish, manage or terminate that employment relationship and employees are provided with notice of the purposes for processing their data. It is not entirely clear how far "managing the employment relationship" would be interpreted to extend, but it seems likely that it would extend to collection and use of employee personal information to follow health authority guidance and reduce the spread of the COVID virus at the workplace or otherwise among employees and customers.

It is worth noting that while PIPEDA applies to the processing of personal information in the course of commercial activity in provinces other than Alberta, BC and Québec, it does not apply with respect to employee personal information in the remaining provinces, unless the employer in question is a federally regulated business.

The Québec law does not include an explicit exception for employee personal information, which is subject to the same statutory obligations and consent standard as consumer personal information.

Of course, in addition to privacy law concerns, the collection and use of employee personal information and related pandemic responses may also raise important issues under employment laws. Businesses may also want to consult the firm's COVID-19 Employment Resources in this regard.

6. **Transparency**

Since private-sector privacy laws are fundamentally consent-based statutes, it is important for businesses to provide adequate and ongoing disclosures to individuals with respect to the purposes for which their personal information may be collected, used and disclosed. Even where exceptions exist for employee personal information, notice to employees with respect to such purposes must be provided. More practically speaking, being transparent about how a business will use personal information during the current pandemic helps avoid misunderstandings, lack of cooperation, ill-feeling and complaints.

7. **Accountability**

Finally, a fundamental tenet of privacy laws is that organizations are responsible at law for the proper handling of all personal information within the organization's control, including when in the hands of a third party for processing. This includes a legal obligation to implement the necessary measures, including contractual restrictions, to ensure that such third parties use and protect the personal information to which they may have access.

Accordingly, during the COVID crisis, organizations must not only ensure that their own home-working frameworks comply with privacy law obligations, but that any vendors handling personal information on the organization's behalf do the same. To the extent that businesses seek the assistance of third parties in the implementation of their business continuity plans, such as licensing new remote networking solutions, the vendors in question, their products and the contractual terms for use of those products all need to be carefully assessed

Conclusion

As summarized by the Privacy Commissioner of Canada, during the COVID-19 outbreak, all organizations must continue to operate with lawful authority and exercise good judgment. Businesses will need to carefully consider how their response to the pandemic may affect their statutory obligations respecting the processing of personal information, both with respect to ensuring that any new collection or use of personal information is "appropriate" as well as ensuring that all personal information continues to be properly used and protected in a work-from-home environment.

About Stikeman Elliott

Stikeman Elliott is a global leader in Canadian business law and the first call for businesses working in and with Canada. Our offices are located in Montréal, Toronto, Ottawa, Calgary, Vancouver, New York, London and Sydney. We provide clients with the highest quality counsel, strategic advice, and workable solutions. The firm has an exceptional track record in major U.S. and international locations on multijurisdictional matters and ranks as a top firm in our primary practice areas including mergers and acquisitions, securities, business litigation, banking and finance, competition and foreign investment, tax, restructuring, energy, mining, real estate, project development, employment and labour, and pensions. For more information about Stikeman Elliott, please visit our website at www.stikeman.com.

For further information, please contact your Stikeman Elliott representative or the author:

David Elder
delder@stikeman.com

Subscribe to updates on a variety of valuable legal topics.
Visit Stikeman Elliott's Knowledge Hub at stikeman.com/kh.