Deloitte.
Legal

Deloitte Legal alert

Striking the right balance: getting back to business without taking a step back on privacy

June 9, 2020

As workplaces begin reopening in the aftermath of COVID19 closures, employers across Canada are implementing return to work plans to protect the health and safety of their workers and their customers.

These plans include a workplace hazard assessment, and identification and implementation of various solutions to control or mitigate hazards, such as use

Contacts:

Olivier Fournier
Partner, National Leader,
Deloitte Legal Canada LLP
Tel: 514-393-8362

Hélène Deschamps Marquis
Partner, Data Privacy and Cybersecurity
Tel: 514-393-8300

Charif El-Khouri
Partner, Employment and Labour
Tel: 514-393-5581

of employee health status screening and/or contact tracing tools (for more information on occupational health and safety planning, please see our earlier bulletin).

However, because these potential solutions will include the collection, use and disclosure of personal information of employees and customers, including personal health information, businesses must consider applicable privacy legislation and governing principles in choosing, designing and implementing any given solution. In fact, following the World Health Organization's declaration of a global pandemic, federal, provincial, and territorial privacy commissioners reiterated that privacy legislation continues to apply during a pandemic, and that governments and organizations alike should respect the established framework,[1] especially with respect to contact tracing technology.[2]

Currently in Canada, there are four applicable privacy statutes. The *Personal Information and Protection of Electronic Documents Act* (PIPEDA) applies to any organization that collects, uses or discloses personal information in the course of commercial activities. Additionally, provincially regulated private sector organizations located in Quebec, British Columbia and Alberta are governed by provincial privacy laws.[3]

These four Canadian privacy statutes differ in form, but share core principles. Nevertheless, one of the exceptions in PIPEDA that distinguishes it from the three provincial laws is that – with regard to employees- it only applies to personal information of employees of a federally regulated business. In provinces without privacy legislation, such as Ontario, courts invoke torts or the common law to protect employee privacy. As such, this article will refer to Canadian privacy laws in general and highlight principles that are common across the country.

Overview of certain health and safety technologies

Depending on the nature of the workplace, businesses may wish to augment their return to work plans with technology-enabled solutions.

There are two broad categories of technology-enabled solutions that businesses may consider implementing to promote workplace safety:

- **Symptom screening** – the process by which either the employee (through self-assessment) or the employer estimates the risk of a given person's infection status; and
- **Contact tracing** – the process by which one (usually public health authorities) can trace who an infected individual has been in contact with.

Symptom screening

Symptom screening is intended to assess risk factors associated with infection. It can be conducted by employees or customers themselves (i.e., self-assessment), or by an employer or business, and usually involves a

[1] https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_covid/
[2] https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/
[3] Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*, Alberta's *Personal Information Protection Act*, and British Columbia's *Personal Information Protection Act*

Jessica Kearsey
Partner, Employment and Labour
Tel: 416-775-2302

Quebec
Philippe Ross
Lawyer, Employment and Labour
Tel: 514-393-9704

Nasim Ghasemi
Lawyer, Data Privacy and Cybersecurity
Tel: 514-369-9730

Nareg Froundjian
Lawyer, Data Privacy and Cybersecurity
Tel: 514-393-6506

Ontario
Alexis Lemajic
Lawyer, Employment and Labour
Tel: 416-874-3436

Related links:

Deloitte Legal Canada LLP

combination of (i) screening questionnaires and (ii) some form of symptom check, such as a temperature check to identify potentially symptomatic individuals.

Screening questionnaires – self or employer administered

To assess whether an *employee poses an infection risk*, a questionnaire may ask: (i) if an employee had travelled recently and not yet completed their mandatory quarantine, (ii) if an employee had been exposed to someone who either tested positive for COVID-19, or was recently abroad and in contact with the employee in the 14 days following their arrival to Canada, or (iii) if the employee is symptomatic themselves. Likewise, many partially open businesses have posted signs on storefronts asking customers some of the above questions, encouraging visitors to self-assess and asking anyone who answers "yes" to refrain from entering the premises.

On the other hand, to assess whether *infection poses a greater risk to the employee*, questionnaires may include questions about an employee's underlying medical conditions (e.g., immunocompromised or respiratory problems), if any, or other factors that public health authorities have identified as increased risks, such as smoking.

When collecting information about an employee's health status, employers should be very cautious not to ask for any more information than is necessary (e.g., "do you have an underlying health condition that may increase your risk for infection?" instead of "please list all health conditions and diagnoses.") and to clearly communicate to employees the purpose for which the information is collected. Employers should also ensure that any personal health information is kept strictly confidential, disclosed on a need-to-know basis only, not stored with or associated to personnel files and destroyed in accordance with applicable laws and policies.

Symptom check – self or employer administered

Widely known COVID-19 symptoms include elevated body temperature and decreased blood-oxygen levels. Therefore, a second aspect of at-home symptom screening may involve asking employees to take and report their body temperature or blood oxygen levels before coming into work.

Temperatures may be recorded using an over-the-counter thermometer, and blood oxygen may be measured using a pulse oximeter – a small, non-invasive and inexpensive device that sends pulses of light through the finger to determine oxygen concentration in the blood stream.

As home antibody testing kits may become more widely available, businesses may be tempted to ask their employees to monitor for the presence of SARS-CoV-2 (or COVID-19) antibodies. However, we do not foresee an extension of self-administered symptom checking to customers and members of the public.

In addition, businesses may adopt different on-site testing solutions to screen employees and customers. These may range from less intrusive means (e.g., using infrared imaging to monitor temperature) to more intrusive means (e.g., requiring thermometer and pulse oximeter testing). There is an abundance of guidance available on this topic from regulators and privacy watchdogs.

Contact tracing

Contact tracing is a process used by health authorities to identify, educate, and monitor individuals who have had close contact with an infected person. It is a critical component of pandemic containment and eradication measures.

To gather data that is needed for contact tracing, the current technology offerings usually (i) leverage a smartphone's Bluetooth technology to determine when two individuals came into close contact, (ii) allow an infected individual to voluntarily update their health status, and (iii) push notifications to everyone who came close to the infected individual.

Perhaps to avoid an employer accessing its employees' smartphones, or to make the technology more widespread (and thus, effective), one company is developing a bracelet leveraging Bluetooth technology similar to smartphones to create an employer-managed contact-tracing scheme.

Businesses may be tempted to request access to data from a contact tracing application and may contemplate requiring all employees and visitors to install a given application to gain entry to workplace premises. However, in our view, these measures are likely inconsistent with applicable privacy laws, as outlined below.

Most of the current generation of contact tracing applications do not appear to collect geolocation data and Apple and Google have been reluctant to allow their application program interface (API) to allow such collection. On the other hand, employer-provided and/or employer-managed devices can transmit geolocation data (from the smartphone's GPS). Employers may be tempted to use geolocation data they already collect (e.g., for tracking their fleet) for new purposes, such as contact tracing or individual infection risk assessment. However, using personal employee information for a purpose other than that for which it was collected raises privacy concerns, as outlined below.

Contact tracing applications usually rely on the principle of user consent. In fact, Google and Apple have stated they would disable access to their API in any jurisdiction that would make the use of an application mandatory. Some countries are even in the process of implementing statutory safeguards to protect the overarching requirement of user consent. For example, Australian draft legislation would make it an offence to make access to a place, a service, and for greater reason, employment, conditional on the use of a contact tracing application.

Applicable principles of Canadian privacy laws

Businesses that seek to implement any of the solutions described above to protect their workers or customers must (i) have a legitimate business purpose for doing so and (ii) use solutions that are reasonable having regard to that purpose.

Reasonableness is assessed on the necessity and proportionality of the solution. These considerations are fact- and context-specific, depending on the workplace, industry, and other workplace characteristics.

In light of the above, businesses must consider a three-step approach to determining which solution, if any, to implement, to manage workplace safety risks in relation to COVID-19.

1. Identifying a legitimate objective

The **first step** is to identify the objective for which a solution requiring the collection of personal information is contemplated. Legitimate business objectives include the protection of worker safety and, in some workplaces, the health and safety of clients, customers or patients.

This analysis will be case-specific and depends on the conditions of the workplace and also the availability of other solutions to protect worker safety, such as social distancing, infection control, and personal protective equipment (PPE).

The objective of any solution must be identified clearly, as it will directly impact the assessment of the legality of a given solution.

2. Reasonableness

The **second step** is to assess whether a potential solution is reasonable having regard to the objective sought, in light of the two principles of **necessity** and **proportionality**. In assessing the reasonableness of a solution, businesses should consider the following three questions:

(i) Is the solution involving personal information **necessary and effective** to achieve the stated objective?

A solution is **necessary** if it is rationally connected to the purpose for which it is designed. For example, a privately managed contact tracing application may be deemed unnecessary and ineffective, especially if public authorities have already implemented such a system. Similarly, continuously monitoring all employees' vital signs may also be unnecessary.

In addition, a solution is **effective** if it is evidence-based and functional. The accuracy, efficacy and efficiency of any solution must be evaluated, with regard to guidance from external sources such as health authorities, as may be necessary. For example, infrared imaging or mercury thermometer testing conducted in combination with a symptom screening questionnaire may increase accuracy of results and effectiveness of the solution. In contrast, a system that collects personal information but predicts an inaccurate risk score (resulting in turning healthy individuals away or allowing infected ones on site) is not an effective solution. While no solution is perfectly accurate, associated accuracy rates, including false positives and false negatives, will affect the analysis of a given solution's effectiveness.

(ii) Is the solution involving personal information **proportionate** with respect to the stated objective?

A solution is **proportionate** if its benefits outweigh the costs. For example, a contact tracing scheme involving Bluetooth-enabled wearables, which does not store personal information about an individual is likely a more proportionate solution than one seeking access to a variety of unrelated information stored on a smartphone. Similarly, it may be sufficient to verify symptoms or risk factors

verbally, or through a temporary alert to relevant individuals, without capturing personal information or without creating a temporary or permanent record.

(iii) Is the solution involving personal information **minimally intrusive** with respect to the stated objective?

A solution is **minimally intrusive** if it is necessary, effective, proportionate, and also results in the *least* invasion of an individual's privacy compared to other solutions. For example, it may suffice to know if an employee has low blood oxygen levels rather than the exact blood oxygen level, which may reveal other unnecessary details about their health. Finally, businesses will also need to justify why they are screening on-site, rather than relying on employee or visitor self-assessments, which can be collected in a less intrusive manner, in the comfort and privacy of their own homes.

3. Privacy design principles

The **third step** of a business' analysis of a given solution is to consider and effect **privacy design principles**. Even where the solution may be reasonable, a business must respect a number of privacy considerations when actually implementing the solution. Here are a few considerations:

(i) Businesses must obtain **consent** for the collection, use, and disclosure of employee or customer personal information. To be clear, the requirement of consent is distinct from a business' right, in certain circumstances, to deny workplace entry to individuals who will not consent to the data collection necessary for the solution.

(ii) Subject to limited exceptions, businesses can only use or disclose the information they collect for the **purpose** for which they obtained employee or customer consent.

(iii) Where possible, businesses should consider **anonymizing and de-identifying** collected information, so as to achieve the stated objective without identifying the employee or the customer. Businesses should also purge all personal information records that are no longer required to achieve the stated purpose, subject to retention requirements at law.

(iv) Businesses are responsible for implementing reasonable **security safeguards** to protect the collected information. Access to personal information collected should be limited to only those people within the organization with a "need to know" to meet the stated purpose (e.g., an HR manager, a workplace health and safety specialist, a risk assessment specialist, etc.).

(v) Businesses should regularly assess and reassess a given solution for effectiveness (accuracy, false positives and negatives), and redesign processes, as may be required, to meet the stated purposes. Businesses should consider both internal and external controls to audit and assess.

(vi) Employees and customers have the **right to know** how the personal information will be used, who will have access to it, where it will be stored, how it will be securely retained, and when it will be destroyed, as well as the **right to access** and challenge the accuracy of such

information. Business should expect questions and have a designated privacy contact who can provide answers.

(vii) Businesses remain at all times liable to employees and customers for any personal information they collected, including when they transfer such personal information to third parties (e.g., subcontractors and service providers) who use, host, or disclose such information. A number of Canadian jurisdictions have specific requirements for employee personal information stored outside Canada or outside the relevant province.

Finally, when it comes to employees, employers should consider broader workforce morale issues to ensure that they have a clear and effective communication plan for rolling out any proposed solution. When it comes to customers, businesses should remember that trust is the cornerstone of getting back to business as usual and engage proactively with customers to create a healthy and safe space for all involved.

For any questions about reopening your doors while being mindful of the privacy of those who enter, please do not hesitate to reach out to members of our Privacy Law team or our Employment and Labour Law team.

Deloitte Legal Canada LLP
Bay Adelaide Centre, East Tower
8 Adelaide Street West, Suite 200
Toronto ON M5H 0A9
Canada