

Intelligent Building Systems and Workplace Privacy

Summary for Policymakers

Intelligent building systems are being installed in Canada at a rapid pace, driven by environmental and economic considerations and accelerated by the pandemic. These systems consist of the digital management and monitoring of buildings that includes heating and ventilation, lighting, security, and other operations. They can improve energy efficiency, simplify business operations, lower costs, provide security, and improve employee experience.

Intelligent building systems can also collect considerable personal information, posing privacy risks that are growing as their adoption is increasing as well as their sophistication. This is particularly true for employees. Some systems are explicitly designed to monitor employees, and others capture this information indirectly. New CSA Group research identifies the workplace privacy implications of intelligent building systems, describes widening gaps in Canadian policy, regulation, and standards for workplace privacy, and provides potential solutions to these gaps.

Intelligent buildings systems for employee monitoring



In restaurants

Some restaurants use computer vision systems that can identify if a table has not been cleared or customers have been waiting to be served. These systems have been used for performance monitoring with employees reporting knowing little about it.



In healthcare

Some hospitals use hand-hygiene monitoring, where, based on their movements, health care workers can be told to wash their hands. Other systems are used to verify homecare visits.



In warehouses

Warehouses use “lead me” carts and conveyor belt scanners that give workers directions and monitor their performance.



In offices

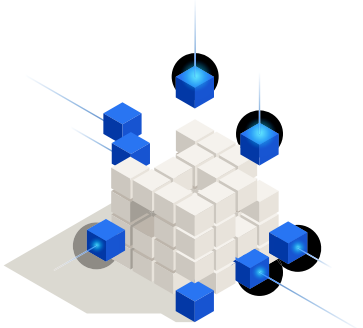
Office buildings can collect data on occupancy and worker movement to manage building systems and personnel, capturing sensitive personal data directly and indirectly.

Intelligent building systems can challenge workplace privacy

Workplace monitoring is not new, but modern technologies — including those used in intelligent building systems — have increased the scale and scope of privacy implications. Intelligent building systems present three main types of privacy risk for workers:









Data magnitude and sensitivity

Intelligent buildings can generate vast quantities of data about occupants. This poses concerns because data may:

- Be particularly sensitive or personal
- Include legally protected information (e.g., about disability) that could lead to discrimination
- Allow for re-identification of anonymized data given the scale of tracking

Information use and misuse

Workers are concerned about how their data might be used or misused. This is because employee data can:

- Be used to influence promotion, dismissal, and other workplace outcomes with little transparency or accountability
- Feed algorithmic management systems, which can be inaccurate and biased
- Be repurposed, shared with third parties, or exposed through cybersecurity vulnerabilities, leaving workers with little information about how their data is used

Workplace power dynamics and consent

Worker privacy issues posed by intelligent building systems can be further complicated by workplace power dynamics:

- **An unequal balance of power between employers and employees makes informed consent impossible** in most workplace contexts. Privacy laws in Canada also contain a number of broad exceptions to requirements for consent in the workplace.
- **Workplace surveillance often targets low-wage and hourly jobs** — workplaces where employees generally have less bargaining power and where many workers are immigrants, women, and/or racialized individuals.

The current policy landscape

Workplace privacy in Canada is covered by a loose patchwork of laws and policies that can vary by jurisdiction, generally favouring employer interests. **The two primary areas of policy that influence workplace privacy are privacy law and employment law, but neither provide significant workplace privacy protections.** Increasing workplace digitization furthers the need for privacy and employment policy that protects Canadian workers digital rights.



Canadian privacy laws provide little distinct consideration for employee privacy:

- **The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA)** covers the largest share of employee data in Canada. It focuses largely on consumer data, and relies on consent, which is generally ineffective in a workplace context. ***The Privacy Act*** governs the federal public sector and takes a similar approach. There have been recent proposals from the federal government and elsewhere to reform federal privacy laws and new proposed legislation is anticipated in the current parliament.
- **Provincial and territorial** legislation covers provincial public sectors, healthcare, and in some cases private sector. These laws generally follow similar approaches to federal frameworks, leaving similar gaps. Nonetheless, provincial courts in Quebec and Ontario have substantively expanded privacy protections through precedent in case law.

Employment laws are mostly silent on workplace privacy and monitoring

- Provincial legislation applies to more than 90 per cent of workers, while limited sectors including airports and banks are covered by the federal *Canada Labour Code*. While in comparison to privacy laws, labour laws have more enforcement capacity, there have been nearly no provisions related to electronic monitoring. The Government of Ontario recently proposed employment law reform that would, if passed, require employers to have formal electronic monitoring policies.

The international context also shapes workplace privacy in Canada

- **Companies often design their products and policies to comply with regulations in leading or large jurisdictions.** The European Union's General Data Protection Regulation (GDPR), which has very stringent privacy requirements, has been influential around the world. Canada is also party to international privacy laws like Article 12 of the *Universal Declaration of Human Rights*.

Recommendations to promote privacy

The growing policy and regulatory gap for workplace privacy calls for responses to support employees, employers and building owners. This report identifies a variety of potential responses, broadly grouped into three categories:

Reinforcing protections

- **Legislative reform:** Updates to privacy and labour legislation across jurisdictions can be approached with a common set of principles, including ensuring clear limits on 1) data collection; 2) clear disclosure to employees; and 3) a right to employee access to data.
- **Enforcement:** Legislative reform needs to be backed by stronger enforcement capacity. This includes channels for employees to report breaches while protected from reprisal.
- **Responsive regulation:** Mechanisms and expertise should be developed in a way that makes it easy to adapt regulations to future technological and social change.

Empowering workers

- **Worker engagement:** Policy should reflect workers' perspectives. This could include collaborative engagement like citizens' assemblies or worker-led advisory bodies.
- **Shared governance and decision-making:** Shared governance models where employees have a say in how data is managed — or even a stake in its benefits — could benefit employees and employers.
- **Strengthen advocacy avenues for workers:** Workers' ability to advocate for their own privacy can be supported by specialized workplace privacy legal clinics, collective bargaining, or ombuds offices.

Supporting industry leadership

- **Standardization:** Development of standards could support employers and building owners to make informed decisions in deploying technology and could strengthen audits and impact assessments and promote strong privacy norms. This could include standards or practice guidelines that could ensure confidence and consistency in third-party audits and impact assessments intended to ensure that data is being managed appropriately and algorithms used to process it are free of bias.
- **Capacity building and best practices:** Better information about privacy risks and best practices can support better outcomes. For example, the Canadian Centre for Cybersecurity could develop a dedicated intelligent building initiative, or industry coalitions or non-profits could share best practices. In its 2021 budget, the federal government proposed to create a new Data Commissioner with an advisory mandate to inform government and business approaches to data-driven issues to help protect people's personal data and to encourage innovation in the digital marketplace.

© 2022 CSA Group Testing & Certification Inc. All Rights Reserved.
05/2022