STANDARDS RESEARCH

Intelligent building systems and workplace privacy

May 2022

Author

Noah Zon, Springboard Policy

Alannah Dharamshi, Springboard Policy

Jasmine Irwin, Springboard Policy

Project Advisory Panel

Obhishek Bhattacharjee, Smith + Andersen

Christina Catenacci, Georgian College

Bala Ghanam, BOMA Canada

Clift Rondeau, CSA Group

Patricia Matthews, CSA Group

Helene Vaillancourt, CSA Group

Table of Contents

Executive Summary

Modern buildings are much more than bricks and beams. With the introduction of intelligent building systems, these spaces are digital environments as well as physical ones. Intelligent building systems use digital technologies and sensors to monitor and manage a building and its systems, such as lighting and ventilation. These technologies can make buildings more environmentally friendly, more comfortable, and less expensive to operate. However, in doing so, they also generate vast quantities of data about people spending time in these buildings, presenting a growing risk to digital privacy, especially for employees in the workplace.

Workplace privacy in intelligent buildings is a growing challenge

There has been a surge in adoption of intelligent building systems in workplaces in recent years. The number of connected building devices doubled in the past five years [1]. Adoption was accelerated by the pandemic; unoccupied spaces, public health measures, and concerns about liability changed the calculus in favour of investment. Intelligent building systems installed as part of pandemic responses have included HVAC upgrades [2]; temperature and distancing monitoring supported by infrared cameras and computer vision [3], [4], [5]; and contactless entry systems [6].

Intelligent building systems are a privacy risk for employees

These privacy risks apply to anyone passing through these spaces, but they are most significant for employees with intelligent building systems in their workplaces.

Employees are subject to significant data collection. Employees are monitored for most of their waking hours, often with systems installed by their employers explicitly to track their movements and behaviours.

Data in the workplace can have significant, long-lasting consequences for employees. The information collected about employees can influence their career prospects and reveal sensitive information to their employers

Current policy frameworks do not adequately protect employee privacy. Most protections hinge on employee consent — an unrealistic approach given the power dynamics of an employment relationship. Policies have also failed to keep pace with the evolution of monitoring technology.

There is a policy gap

Workplace privacy in Canada is covered by a loose patchwork of laws and policies. This patchwork leaves gaps in privacy protections for Canadian workers:

- Privacy protections include laws at the federal and provincial level. These laws have little to say about employee privacy and the power dynamics of workplaces.
- Employment frameworks are primarily in provincial jurisdiction and do not directly address electronic surveillance and privacy.
- International laws and standards influence the Canadian marketplace but do not provide direct accountability for Canadian workers.

Recommendations

The levers to protect employee privacy can be found in a range of hands. This report identifies a variety of potential responses, broadly grouped into three categories:

Reinforcing protections

- Legislative reform
- Strengthening enforcement
- Responsive regulation

Empowering workers

- Engage workers in policymaking
- Shared governance and decision-making
- Strengthen advocacy avenues for workers

Supporting industry leadership

- Standardization
- Capacity building and best practices

"Intelligent building systems — the digital management and monitoring of building systems that include heating and ventilation, lighting, security, and other operations — mean that physical workplaces themselves are sources of information."

Introduction

Our workplaces are changing. With a surge in remote and hybrid work there has been a great deal of media on the loosening connection between our employers and our places of work [7].

Even with these significant shifts, the majority of Canadian workers show up in person to their workplace all or most of the time — with three in five doing so even at the peak of pandemic restrictions [8]. These physical workplaces are undergoing their own quiet transformations that have significant implications for the relationship between employers and employees — especially for employee privacy.

Modern commercial buildings are much more than bricks and beams. Whether it's warehouses, retail, office or institutional spaces, there is increasingly a digital layer to our buildings. Intelligent building systems — the digital management and monitoring of building systems that include heating and ventilation, lighting, security, and other operations — mean that physical workplaces themselves are sources of information.

The accelerating adoption of intelligent building systems is being driven by a number of priorities. They allow effective energy management to support climate objectives, help manage costs, and can make for better operations and experiences for the people spending time in those buildings [9].

Many of these systems also collect personal information directly or indirectly about the people working in these spaces. This presents a privacy risk — one that is difficult to see or manage, but that is expanding with the increased adoption and sophistication of intelligent building sensors and systems.

The COVID-19 pandemic has accelerated the adoption of intelligent building systems in commercial settings. The global smart buildings market is expected to grow at a rate of more than 10 per cent per year in the first half of this decade [10]. The pandemic also led to new types of surveillance. Building owners and employers invested in a number of sensors and systems to manage public health measures, including computer vision systems to track social distancing, and thermal imaging to check temperatures. While this sensitive data collection began in the context of an emergency, it is not clear how it will be phased out or if it will normalize greater data collection for the long-term.

The privacy risks of intelligent building systems are more acute for employees than customers or occasional visitors. They face **greater data collection** because of the amount of time they spend in the spaces and the activities they do there. They have **less control** over their information because of the grey areas between employment relationships and privacy rights, and because it is difficult to have informed consent due to the power dynamic with employers.

Privacy risks for employees also have **greater impact** because the data collection and use can directly affect their livelihoods if used by current or prospective employers to make decisions about their career progression.

In the face of this growing challenge, Canadian workers, employers, building owners, and policymakers need solutions. Today, Canadian privacy policy frameworks remain an out-of-date patchwork. Intelligent building systems can manage safer, more sustainable buildings, but we need proactive responses to ensure that those do not come at the cost of employee privacy.

About this report

This objective of this project is to explore the implications of intelligent building systems for employee privacy. The research focuses on the privacy risks to employees working in a wide range of commercial building settings (including office, retail, industrial, hospitality and community/institutional buildings such as hospitals), and in the context of the Canadian policy environment. This report highlights the nature of those challenges and includes potential solutions that address the widening policy, regulatory and standards gap, including legislative and non-legislative responses. The solutions require leadership from a range of actors throughout Canada, including policymakers, building owners, employers, and employees themselves.

The research for this project took place in Fall 2021 and Winter 2022. It included a review of academic and grey literature, jurisdictional scans of policy responses, and insights from key informant interviews and an expert project advisory panel. The authors are grateful for all of those who contributed their insights and to Dana El-Chaer for research support.

1 Intelligent Building Systems in the Workplace

There is no one single definition of an "intelligent building"; intelligent buildings are made up of a range of technologies working together, with the makeup varying from building to building. The Chartered Institution of Building Services Engineers describes an intelligent building as "[a building] that provides a productive and cost-effective environment based on three basic elements: people, products, and processes" [11]. Interest and investment in intelligent buildings systems have surged in the last decade, with the growing capabilities of Internet of Things (IoT) technologies [11].

In some cases, intelligent buildings feature net-new innovations that would be unfamiliar in an office building or warehouse of 30 years ago — for example, computer vision systems that use artificial intelligence (AI) computing power to turn images into machine-readable data. Other components involve digitizing "legacy" systems (like lighting or heating, ventilation, and air-conditioning [HVAC]) through sensors and connections that collect data and automate processes [12]. Most of these systems are not visible to people moving through the building; they are either hidden behind walls or form a digital "layer" of data about how the building is operating and how people are moving through it.

In an increasingly enmeshed world of IoT, there are no firm lines of what technology is part of an intelligent building system and what is not. By being connected to hundreds of interconnected devices — including, sometimes, employees' personal smartphones — the rise in intelligent buildings can blur lines we use to make sense of work environments: between fixed and fluid architecture, between personal and professional information, and between public and private space.

1.1 The Rapid Growth of Intelligent Building Systems

The share of workplaces featuring intelligent building systems is growing quickly. There has been an estimated doubling in the number of connected building devices between 2018 and 2022 [1]. This push is being driven by a number of factors:

- **Energy and resource management:** An estimated 30% of the energy used by commercial buildings is wasted [13]. By optimizing systems like lighting, HVAC, and water usage, companies can both save costs and have greener operations. Sensors and

automation can turn off systems in unused areas, adjust ventilation to suit room size and the number of occupants, and conserve energy use.

- **Asset management and predictive maintenance:** Through usage data and sensors, intelligent building systems can anticipate maintenance needs and cleaning, keep track of needed stock, and prevent equipment failures [14].
- **Occupancy & space optimization:** Intelligent buildings can help monitor person-traffic, allocate space, and streamline facility booking processes.
- **Security:** Digitized/individualized building systems can help improve building security and detect threats of concern. By having more IoT enabled tools in intelligent buildings, it can be easier to "securitize" spaces in a workplace; for example, elevators that require personalized Bluetooth to move, or door locks with voice recognition [9].
- **User/worker experience:** Intelligent building systems can increase convenience, comfort, and useability for employees. In some intelligent buildings, workspaces can be automatically personalized to anticipate individual worker preferences, including desired temperature, noise level, lighting, and positioning [15]. IoT security systems — like facial recognition systems — could mean employees no longer need to worry about losing their ID badge [16].

These ongoing trends have been accelerated by the pandemic. As part of the COVID-19 response, some features of intelligent buildings have become increasingly sought-after, including tracking occupancy levels, and the ability to monitor temperature and other public health factors like distancing (see box on p. 14).

Even if the motivation is not to track people, facility-focused data can capture a great deal of information about employees. Tracking parking flow, bathroom use (for maintenance), or room booking requires collecting vast amounts of employee data. While aggregation and anonymization can mitigate privacy risks, effective oversight and governance can be challenging.

1.2 Intelligent Building Systems as Workplace Monitoring and Surveillance

Some intelligent building systems are directly designed to monitor employees in the workplace, bringing important privacy implications. These intelligent building technologies are used to monitor employees, make decisions about them, and optimize their performance. For example, some employers use video surveillance combined with AI computer vision or other types of sensors to monitor employee productivity — how workers spend their time, where they are within a space, and how long they take to finish tasks [17].

These new systems are being used in a variety of settings to bring information collected from building sensors directly into workplace operations and people management. In some cases, this is done at an aggregate level for process improvement — for example, to learn how one configuration of an assembly line tends to help workers move faster than another. In other cases, systems are used to directly monitor employees' real-time actions or monitor their performance over time. Insights from smart light-emitting diode (LED) systems can help employers optimize lighting for maximum worker happiness and productivity across an office building; the same technology could also be used to track when an individual worker turns off their light and leaves for the day [18].

Within intelligent buildings, it can be very difficult for employees to understand *both* **what data is being collected from them** and **how that information is used to make decisions** about them or their work. This lack of transparency is a concern, as Intelligent building technologies are being adopting across many industries and types of workplaces as described in Figure 1. In particular, employees often express concern that hidden surveillance could be used for disciplinary reasons [19].

Intelligent buildings are also the building blocks of a broader trend towards smart cities [9],[26]. Some of the most significant testing grounds for the possibilities of smart cities are, in fact, workplaces. Corporations

like Alphabet and Qualcomm are developing smart campuses for employees that act as mini-communities, linking intelligent buildings with each other and other services like shuttles and garbage disposal [27],[28]. Greater interconnection between smart buildings can mean scaling up the benefits described above: creating greener, more convenient, data-driven spaces for entire communities. However, smart cities can also intensify the privacy and security risks of a smart building by orders of magnitude — a prominent concern for the proposed Sidewalk Toronto smart city district in Toronto's Quayside neighbourhood.

2 Privacy in the Workplace

Concerns about privacy in the workplace are nothing new. From timecards to managers roaming the floor – there has long been a tension between the interests of organizations to monitor their operations and employees' privacy. However, modern electronic surveillance has dramatically increased the scale and scope of employee monitoring [31]. Electronic surveillance now goes beyond the bounds of human supervision through continuous, and often hidden, data collection and analysis about the most minute details of workers' behaviours, activities, and interactions [20], [32]. This ability has shifted the balance of power more heavily in favour of employer interests.

Intelligent building systems add another dimension to the electronic surveillance landscape. The distinct privacy implications of intelligent building systems have three main dimensions: the magnitude and sensitivity of data; the use and misuse of information; and power dynamics and consent in the workplace.

Figure 1: Intelligent buildings as supervisors

In restaurants

Some restaurants are using Presto computer vision systems that, among other capabilities, can identify if a table has not been cleared or customers have been waiting a while for their food or to be seated [20],[21]. These systems have explicitly been used for employee performance monitoring and employees reported knowing little about it.

In healthcare

Some hospitals use hand-hygiene monitoring, where health care workers can be told to wash their hands based on their movements [20].

Electronic visit verification is mandated for Medicaid-funded services in US, where health providers need to be able to prove a home care service visit has been made, often by GPS-tracking employees [22].

In warehouses

Warehouses are increasingly adopting "lead me" carts that both give workers directions and monitor their performance [20]. In some warehouses, conveyor belt scanners produce data to track productivity and speed [23],[24]. At Amazon warehouses, the drive to find efficiencies and optimize worker performance has led to machine-led supervision, including auto-generated employee reports and self-service "HR kiosks" [25].

In offices

Office buildings can collect data on occupancy and worker movement to help employers manage their building systems and personnel. However, this "incidental" mass information collection can capture data points like coworker interactions, bathroom usage, and other sensitive location information [20].

Beyond the building: Employee monitoring and remote workers

The COVID-19 pandemic accelerated the adoption of remote work, especially for those workers who might normally be commuting into office buildings. In 2016, 1 in 25 Canadian workers did the majority of their work from home; in August of 2021, that number was close to 1 in 4 (down from a peak of about 40% of workers in April 2020) [8].

In response to this massive shift, many companies have implemented workplace surveillance software to track their employee's activities when they are no longer in physical proximity [29]. These tools use things like computer activity, keystroke tracking, and webcams to report on what employees are doing and when. One survey indicated that the use of employee surveillance software jumped 50% in 2020 and continued to grow through 2021 [30].

Because this document's focus is on intelligent building systems in workplaces, monitoring of remote workers is not part of this report. Remote worker monitoring does, however, reflect many of the same trends: a rapid acceleration in adoption spurred by the pandemic; greater electronic surveillance of employees; and a policy gap that leaves employees with few protections. Changing attitudes around how and in what ways employers track their workers as a result of remote work could have spillover effects into the perception of monitoring and tech-enabled supervision within in-person environments.

2.1 Data Magnitude and Sensitivity

To improve operations and create adaptive environments, intelligent buildings need vast quantities of data about occupants [33], [34]. Even before the rise of intelligent buildings, workers were already concerned about the volume of information that their employers collect [31], and innovations like intelligent buildings expand the scale and pace of this practice [35].

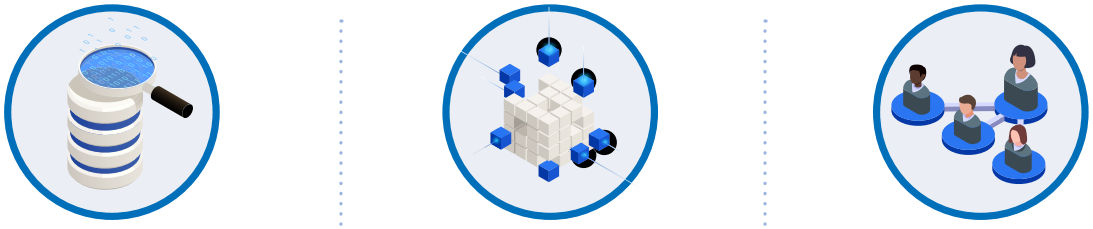
The data generated in intelligent buildings may be particularly sensitive or personal [36]. Data collected by intelligent buildings could even cross into potentially revealing information employers are legally prohibited from asking about because of potential for discrimination, including disabilities [20] and health-related behaviours [37]. For example, systems that track location in the building might identify that someone has a health issue because of their time spent accessing washrooms.

Some technologies in intelligent buildings might even capture biometric data including fingerprints, eye movements, facial expressions, and tone of voice [23], [35], which can uniquely identify an individual worker. For instance, sensitive fingerprint data is being collected as part of systems that let retail employees clock in at stores [37], and agricultural workers enter greenhouse facilities [38].

Even without direct collection of this type of information, sensitive and personal inferences about workers could be drawn from seemingly innocuous information [39]. Data could be linked to identify workers, infer their relationships, and track their location [40]. Take the use of sensors [9] — from indoor environmental quality sensors, to smart utility meters, to surveillance cameras — a large amount of data can be collected about workers and be revealed to employers and building managers [41]. For example, data from occupancy sensors installed for energy efficiency could be combined with other information to infer occupancy and activity patterns [39].

Workers are concerned: a recent study of preferences about working in smart buildings found that individuals were wary that these types of sensors could enable workplace monitoring on an outsized scale to business need [41].

Figure 2: Employee privacy implications of intelligent buildings



2.2 Information Use and Misuse

Interviewees for this report explained that while workers are concerned about the collection of their information, they are much more concerned with how that information might be used or misused by their employers.

Pervasive electronic surveillance can constrain the ability of individuals to freely move, associate, and express themselves in the workplace [42], and could even be used to erode worker benefits and protections [35]. For instance, time and activity tracking systems have been used to reduce wages by identifying "unproductive" periods as unpaid down-time during work hours [37].

These types of technologies might also be used to assess them and make managerial decisions [32]. Electronic surveillance can feed algorithmic management systems that partially or fully automate management and decision-making about workers – from performance assessments and behaviour predictions to even decisions about promotions and firing [43], [44]. These types of tools, however, can be inaccurate and biased [45], reinforcing patterns of discrimination and making unfair assessments in consequential decisions that affect the trajectory of workers' lives. For example, some offices have implemented thermal cameras to monitor workers for high body temperatures as a potential sign of COVID-19 but since the technology cannot distinguish fevers caused by the virus from other causes of high body temperature like pregnancy or menopause, individuals could be falsely identified [46].

Excessive monitoring has been shown to lead to stress and anxiety on the job [47]. It can also be a safety hazard, causing individuals to overwork or cut corners leading to injury in order to meet data-driven targets [48]. Ironically, productivity monitoring can lead to decreased output [49] affecting workers' sense of autonomy and discretion [20]. Because privacy and information sharing depend on trust, a lack of trust can create a vicious cycle undermining workplace relationships [48], [50], [51].

Beyond workplace applications of data in intelligent buildings, there is also the potential for function creep where information can be repurposed or shared. In an intelligent building context, information related to workers can flow between companies, building operators, and third-party service providers. There is potential that any of these stakeholders could then share or sell this data to other actors outside the ecosystem, including data brokers, advertisers, and urban planners [52]. For instance, sharing data about smart meter usage with third parties is already commonplace in many North American jurisdictions [39]. Most employers do not own their buildings, and the monitoring technologies used in these spaces might include a mix of systems purchased and managed by either the employer or the building operator. The data management is more likely to be governed by commercial leases or informal arrangements than a data privacy policy.

The implications of cybersecurity for workplace privacy in intelligent buildings

Intelligent buildings may have cybersecurity vulnerabilities that could allow for outside access to employee information. For instance, attackers could inject spyware into building systems to gather sensitive information or could gain remote access to surveillance cameras to monitor the building [40]. These types of cybersecurity vulnerabilities are diverse and could occur throughout many of the different parts of an intelligent building – from the physical sensors and devices to the digital software and networks [53], [54]. Data breaches are becoming increasingly costly (an average of more than $5 million CAD per incident) and harder to detect and address [55], with the Canadian Centre for Cyber Security highlighting ransomware as an increasing organizational threat [56]. Since the different parts of an intelligent building require integration and communication to function cohesively, unintended pathways could arise that are vulnerable to attack and any one system or device could become a weak point for the whole ecosystem [53], [57].

Given this range of technologies, creating secure intelligent buildings is a complex task, even for cybersecurity professionals. Yet many intelligent building systems are designed and installed by building engineers and procured and operated by building managers with limited expertise in the field [53].

2.3 Power Dynamics and Consent

Power dynamics in workplaces also cause issues. Electronic surveillance practices are often opaque, difficult to understand, and lack transparency, making it difficult for employees to influence and interrogate their use [35]. Intelligent buildings only make this more challenging as surveillance and data collection can be less intuitively visible [58], making it harder for workers to perceive the technologies they interact with in the workplace. The Privacy Commissioner of Canada has issued guidance that hidden or "covert" surveillance is an "extremely privacy-invasive form of technology" and should be approached with an additional level of safeguards [59].

A lack of understanding and awareness about the monitoring practices and privacy risks in intelligent buildings undermines meaningful consent. At the same time, the unequal balance of power between employers and employees can make free and informed consent impossible in workplace contexts [23], [50]. Given that many workers do not have the luxury to walk away from their jobs, they are often not in a position to make a choice about the use of data-driven technologies and could feel compelled to accept terms they would not otherwise agree to [48]. What's more, privacy statutes in Canada contain a number of exceptions to consent that could apply to an intelligent building used as a workplace. For instance, consent is often not required under private sector privacy laws if the purpose of data collection, use, or disclosure is necessary to establish, manage, or terminate an employment relationship [60].

As a result, workers may be left with little recourse than to accept surveillance, data collection, and other privacy intrusions within intelligent buildings. Employers stand to gain significant information advantages from these practices, leaving workers with even less bargaining power than ever before [35]. Technologies could even be used to inhibit collective organizing by workers, directly through anti-union surveillance or indirectly through chilling effects on behaviour [37]. This type of intense 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 [23].

COVID-19 and intelligent workplaces

COVID-19 has changed the expectation of both employees and employers about what information is shared at work. After years of pandemic protocols, it has become routine for employees to disclose information to their employer that they might have previously kept private: explicit details about their own health information, the health information of their family members, their travel plans, and other information well beyond what was common before the pandemic. Employees have also come to expect more workplace supervision and monitoring as a result of the pandemic, including detailed information about where they are and who they are in contact with when doing their jobs.

COVID-19 mitigation and response has already accelerated the adoption of smart building technologies across industries, a trend that will likely continue as more employees return to in-person work. Intelligent building technologies may have been appealing to many employers before 2020, but the cost or complexity of implementation could outweigh the perceived benefits. COVID-19 changed the incentive equation for smart buildings. Intelligent building technologies — ubiquitous, networked, automated, and responsive — are uniquely equipped to help workplaces carry out pandemic safety protocols and best practices, enabling safer in-person work and associated gains in productivity. Intelligent building features can enable:

Improved air circulation: Smart HVAC systems can track air quality and use occupancy data to manage optimal air circulation [61]. Some believe that sensors in HVAC systems could someday detect pathogens and help with monitoring infectious spread [2].

Contactless tech: To avoid employee contact with traditionally high-touch surface areas like buttons and doors, workplaces can use touch sensors, voice recognition, or phone apps as a replacement [6].

Temperature monitoring: Fixed infrared cameras can monitor occupancy through "heat mapping" bodies in a building. Infrared cameras could also be used to flag people who may have a fever: such cameras have been used in some high-traffic spaces like airports and sports stadiums, despite experts decrying their ability to detect illness [3], [4].

Occupancy management: In offices or work facilities with COVID-informed capacity limits, intelligent building systems can help assess how many people are in a building, who are using high-traffic areas like washrooms, and can make recommendations on cleaning and scheduling [61].

Worker density/spacing: Even more granular than occupancy, some technologies can monitor how close individual employees are to each other in real time, either through workplace "wearables" or through camera monitoring [5].

Contact tracing: By tracking what individual employees move in and out of workspaces, employers can monitor and notify close contacts and mitigate the effects of outbreaks.

Preventing COVID-19 transmission has not been the only factor driving the growth of intelligent building adoption during the pandemic. For employers with a large share of employees working remotely, COVID-19 also presented an unusual opportunity to re-think and reconfigure their physical work environment. Before the pandemic, installing intelligent building systems meant possibly disrupting the flow of in-person work: both the hassle of renovations and the difficulty of adjusting employee expectations and habits. COVID-19 changes have spurred many companies to make huge shifts in how and where employees do their work, including the adoption of smart building technologies to support hot-desking and hybrid work models [62], [63].

COVID-era "smart workplace" technologies may represent a massive shift in the amount of data collected from employees, but many have the stated purpose of improving workplace safety (COVID transmission) or worker well-being (flexibility, workplace satisfaction). Existing legislation acknowledges that health priorities can take precedence over privacy priorities: there are public health emergency exceptions to both the Privacy Act and PIPEDA [64]. There may also be a deliberate trade-off on the part of some employees, who are willing to make defined privacy concessions in order to do in-person work safely. Distinguishing between informed consent and the false choice is difficult in the short-term. For the long-term, there are risks that COVID safety measures will further normalize surveillance in [65]. Even as the risk of COVID-19 transmission subsides, it will be difficult to walk back systems that have become part of a building's networked infrastructure and give employers access to valuable data.

3 The Public Policy Landscape

Workplace privacy in Canada is covered by a loose patchwork of laws and policies. While potentially covered by both privacy and employment laws, the issue is largely overlooked in both cases. Protections in privacy laws generally do not account for the power dynamics of workplaces [60]. Employment policies and regulations are relatively silent on data protection [66]. Where protections exist, they vary depending on jurisdiction, sector, and unionization status. To the extent that protections explicitly covering workplaces exist, the policies have generally emerged from case law.

These gaps have left employees with piecemeal electronic privacy protections in the workplace, while leaving employers with limited guidance on monitoring practices [23]. The result is a framework that serves no one well, but is generally tilted in favour of employer business interests over the privacy interests of workers [60].

The digitization of our workplaces makes these gaps more significant. Today's technologies enable more widespread surveillance and increased capture of sensitive data, which can be combined to form profiles and used for AI and analytics [67]. This information can form a detailed and long-lasting record of individuals, with implications for their present and future opportunities.

The most important areas of the public policy landscape for employee privacy in intelligent buildings are privacy laws and employment law frameworks. While data collection and management in intelligent buildings can also be shaped by other policy such as building codes, telecommunications law, or landlord and tenant statutes, these only come into play in some specific uses of intelligent building systems. International policies and standards are also influential as technology vendors tend to design for the dominant expectations in a global marketplace.

"Today's technologies enable more widespread surveillance and increased capture of sensitive data, which can be combined to form profiles and used for AI and analytics."

3.1 Privacy Frameworks

Canada has a number of laws that govern privacy in both the public and the private sectors. Some of these are federal, such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) which covers most of the private sector and the *Privacy Act* (covering the federal public sector), and others are provincial, often focusing on public sectors and healthcare. While these laws differ in some important ways, they share a very limited consideration for employee privacy.

3.1.1 The Personal Information Protection and Electronic Documents Act

PIPEDA is the main federal legislation that applies to private sector data collection [68]. Generally, PIPEDA focuses on the data of consumers, but it also applies to employees in federally regulated organizations like airports or banks [69]. While the law does not spell out a clear framework for handling employee privacy, it does limit data collection to purposes a reasonable person would consider appropriate [70], and some boundaries have been established through a combination of case law, guidance from the Privacy Commissioner of Canada, and amendments to the Act.

PIPEDA generally relies on the premise of consent, including in workplace contexts. However, power dynamics in workplaces make truly meaningful and voluntary consent difficult [23], making this protection less effective. The law also provides some broad exceptions to consent in workplace contexts, for example, if the information was produced by an individual "in the course of their employment" or if the information is necessary to "establish, manage or terminate an employment relationship" [71]. Given these and other shortcomings, there have been calls and efforts to modernize PIPEDA for the digital age, with a renewed commitment to reform or replace the legislation in 2022 [72], [73].

3.1.2 The Privacy Act

The *Privacy Act* governs personal information collected by federal institutions in Canada [76]. While the law covers individuals employed by these public sector entities, it does not offer a clear, specific framework for handling their privacy in the workplace. The broad direction of the Act is to limit the information collected about individuals — including workers — to that which "relates directly to an operating program or activity of the institution" [76]. The law also contains a requirement to inform individuals of the purpose of collection, but there are a number of exceptions to this rule [67].

Like PIPEDA, there have been calls and efforts to reform the *Privacy Act* to be responsive to today's technologies. Recently, public consultations were held on modernizing the legislation [77], and amendments are on the government agenda for 2022 [78].

The four-part Reasonableness test

While Canadian privacy legislation does not outline explicit conditions for data collection from employees, there is an overarching principle that data collection and use is reasonable. Under PIPEDA, "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances" [71]. While vague, this has been clarified through litigation (Eastmond v. CP Railway & Privacy Commissioner of Canada) and guidance from the Commissioner into a four-part test of reasonableness, along with some "no-go zones" [74]. To be considered appropriate, data collection and use from employees must be:

- **Necessary:** the data collected is required to meet the organization's operational needs.
- **Effective:** the data collected is empirically effective at meeting the desired goal or need.
- **Proportional:** the trade-off between privacy and the benefit gained is proportional.
- **Minimal:** the data was collected using the least invasive method available.

While the four-part test does set a higher bar to allow for data collection, because they are ambiguous and subjective it makes it difficult in practice to demonstrate unreasonableness in a work-related environment [75].

3.1.3 Provincial and Territorial Legislation

Provinces and territories have a number of laws related to privacy that compliment and overlap with federal legislation. Where provinces have private sector privacy laws that are 'substantially similar' to PIPEDA, those provinces are considered exempt from PIPEDA and these workers would be covered by provincial law instead [69]. This is the case for Quebec, British Columbia, and Alberta. Quebec has recently passed privacy legislation requires disclosure of electronic monitoring in most settings [79]. Similar to the federal level, provinces also have privacy laws that would apply to provincial and local public sector workers [80]. Some provincial privacy laws are specifically targeted at both employee information and health information [80].

Provincial privacy laws follow similar approaches to federal frameworks — leaving similar gaps. Provincial policies also generally rely on notice and consent with some broad exemptions where that might interfere with doing business [67]. However, provincial courts have laid out some expanded protections. For example, protections have been extended in Quebec based on the privacy rights in the *Quebec Charter of Human Rights and Freedoms* [60], and in Ontario through the common law tort of "inclusion upon seclusion" related to harmful invasions of privacy [67]. Similar to the Privacy Commissioner of Canada, provincial privacy guardians have also built on the legislation with privacy guidance. For example, British Columbia's Information and Privacy Commissioner found that some workplace technologies were excessive and provided recommendations on workplace surveillance, including providing notice, training, logging employer activity, and ending the use of certain technologies such as keystroke logging [81].

With the increasing importance of data privacy, provinces are also becoming more active in updating or expanding their privacy legislation. For example, Quebec's new *Act Respecting the Protection of Personal Information in the Private Sector* establishes a number of new practices and protections — though the law does not deal directly with workplace privacy [82].

3.2 Employment Frameworks

Experts interviewed for this report highlighted that privacy laws alone are not sufficient for managing workplace privacy employee data; employment frameworks also need to be part of the equation. While privacy laws address the data management most directly, labour laws deal with the most significant consequences for the use — or misuse — of data captured by intelligent building systems for employees. Labour laws also generally have much more significant enforcement capacity and penalties associated.

Canada has a number of employment laws that apply to employees in an intelligent building workplace. Provincial legislation such as the *Alberta Employment Standards Code* apply to over 90 per cent of employees [83], while limited sectors including airports and banks are covered by the federal *Canada Labour Code* [84]. These laws and regulations set standards on the basic terms of workers' relationships with their employers and minimum protections, such as minimum wage.

Canadian labour legislation does not have a lot to say about the boundaries between personal information and business operations [66], [85]. However, they do offer protections against discrimination and unfair dismissal that are affected by the privacy risks of intelligent buildings. For unionized employees, collective agreements may also include some protections related to workplace surveillance [86], but these provisions are not particularly common and are rarely prioritized during negotiations [87], [88], [89].

The Government of Ontario recently proposed changes to the *Employment Standards Act* that would establish some explicit workplace rights and responsibilities around electronic surveillance that would apply to intelligent buildings systems. If passed, the legislation would require that employers with 25 or more employees have a written policy that governs electronic monitoring [90].

3.3 International Context

Policy made beyond our borders can also shape how data from intelligent building systems in workplaces are managed. Because data crosses borders, some standards and policies are set internationally. At the same time, companies often design their products and policies to comply with regulations in leading or large jurisdictions. For example, the European Union (EU)'s General Data Protection Regulation (GDPR) and California's Consumer Privacy Act have been influential well outside their borders [91].

3.3.1 International Frameworks

Canada has signed international laws that include privacy. For instance, Article 12 of the *Universal Declaration of Human Rights* [92], and Article 17 of the *International Covenant on Civil and Political Rights* [93], include privacy as a fundamental right. The UN Human Rights Council has affirmed that this right applies in digital contexts [94]. The UN system includes a Special Rapporteur on the right to privacy, who provides guidance to states [95].

Other international frameworks provide specific guidance on employee privacy: the International Labour Organization has a code of practice for the protection of workers' personal data [96]. International standards development organizations have also created privacy standards for the digital age. For example, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created a development program for information security, cybersecurity and privacy protection, ISO/IEC JTC 1/SC 27 [97]. From this program ISO/IEC 27701 [98] has been adopted for Canada [99] and ISO/IEC 27400, which covers IoT privacy and security, is under development [100].

3.3.2 European Policy

The European Union's GDPR has been one of the most influential policies on digital privacy around the world [101], and features some of the most stringent privacy requirements anywhere. The GDPR provides individuals with the right to some information about their personal data and the right to access, rectify, erase, and reuse it [102]. Unlike Canadian laws, the GDPR does not rely as heavily on consent, especially in an employment setting. Given the power asymmetry between employers and employees in the workplace, the policy is explicit that companies cannot rely on informed consent in this context [23].

"The acceleration of intelligent building systems adoption combined with changing work patterns and pandemic-driven surveillance interact with one another to expand the scope and impact of privacy risks to employees."

Other European jurisdictions similarly have privacy laws that provide stronger protections for workers. For instance, the United Kingdom's *Data Protection Act,* which is aligned with the GDPR, requires that employers ensure worker data is processed in a fair and lawful way, and provides employees with rights to ask about their information and how it is used [103], [104]. Norway and France also have specific requirements to notify and involve workers in decisions about data collection and surveillance technologies that impact workers, such as through co-determination processes and mandatory conciliation procedures [48].

3.3.3 American Policy

The United States has relatively weak privacy protections for workers. Existing employment laws in the United States (US) [105] have been found to be "inadequate to the task of protecting workers in the data-driven workplace" [20]. At the same time, the US has no federal law that directly addresses employer surveillance of workers and the main national privacy law, the *Electronic Communications Privacy Act,* does not provide workers, or other individuals, with significant protections [106]. However, some states have developed new privacy laws with stronger protections. Most notably, California has developed a modern consumer privacy law, the *California Consumer Privacy Act,* which also applies to employees in covered workplaces [107]. A number of other states have considered and debated privacy legislation in recent years.

3.3.4 Australian Policy

The Australian state of New South Wales has a unique piece of legislation that specifically governs workplace surveillance that could apply in an intelligent building context. This law, entitled the *Workplace Surveillance Act,* regulates the use of overt and covert surveillance including through camera, computer, and geo-tracking technologies, effectively proving employees with enhanced privacy protections from these types of practices [108], [109]. The Act prohibits surveillance of employees without notice.

4 Recommendations

A combination of patterns has transformed a policy and regulatory gap on employee privacy into a growing chasm. The acceleration of intelligent building systems adoption combined with changing work patterns and pandemic-driven surveillance interact with one another to expand the scope and impact of privacy risks to employees. To support employees, employers, and building owners in effective adoption, we will need a multifaceted set of responses.

The levers to protect employee privacy can be found in a range of hands. Potential solutions can broadly be grouped into three categories of response: reinforcing protections, empowering workers, and supporting industry leadership. These recommendations are intended to apply throughout the Canadian employment context to people working in different jurisdictions and different types of employment relationships.

Table 1: Recommendations at a glance

Reinforcing protections	▪ Legislative reform ▪ Strengthening enforcement ▪ Responsive regulation
Empowering workers	▪ Engage workers in policymaking ▪ Shared governance and decision-making ▪ Strengthen advocacy avenues for workers
Supporting industry leadership	▪ Standardization ▪ Capacity building and best practices

4.1 Reinforcing Protections

A major challenge to protecting employee privacy in workplaces with intelligent building systems is the lack of clarity in what is expected of employers, employees, and building owners. As other research on the digital age has highlighted [110], [111], this is a common challenge when the adoption of new technologies and practices moves faster than policymakers can react. It also reflects a longstanding area of uncertainty around privacy expectations in an employment setting.

4.1.1 Legislative Reform

The gaps in employee privacy protections have existed for decades in Canada — they are simply more prominent and important as the risks have grown in scope and scale. Neither labour nor privacy laws in any jurisdiction in Canada have direct responses to the distinct questions of digital tracking in workplaces. While there has been a broad wave of reform to update labour and privacy legislation for the digital age at both the federal [112], [113] and provincial [114], [115] levels, no proposal to date has addressed this gap.

Instead, legislative frameworks leave protections up to an interpretation of the balance between broad protection principles and vague exemptions for necessary collection in the workplace. It is clear that more surveillance may be appropriate in a workplace for basic safety reasons, but there is an absence of clear guidance of where that ends. In that grey area, data collection has surged with few checks or balances.

While uncertainty has the greatest impact on employees, it is also harmful to employers and building owners. Reducing that uncertainty needs to start with legislative reform that makes clear how employees' privacy rights are to be protected in the workplace and how data collected about employees can be used and managed. That is both a question of privacy and rights in the employment relationship.

This clarity cannot be achieved with a single piece of legislation. That is because, in Canada, effective protections need to rely on action in both federal and provincial jurisdiction. While a federal *Employee Privacy Protection Act* — like the one proposed by legal expert Ifeoma Ajunwa for the US [116] — could establish a clear set of policy principles and amend relevant federal legislation (i.e., the *Privacy Act*, PIPEDA and the *Canada Labour Code*), more than 90% of Canadian workers are governed by provincial labour standards rather than federal one [83]. Many Canadian workplaces are likewise governed by provincial privacy legislation, particularly in provincial and local public sectors or healthcare.

There are instead a set of principles and considerations that should be considered in legislative reform across privacy and employment legislation, and across federal and provincial jurisdiction. Principles in the CSA Group Model Code for the Protection of Personal Information developed in the 1990s similarly filled a gap and informed legislative reform [117].

- **Clear limits:** In light of the power imbalance in an employment relationship and the significant risks to livelihood, there should be clear limits on data collection from intelligent building systems in workplaces — rather than relying on consent. These limits could include narrow definitions of the information that can be collected [20], limits on the use of specific technology (such as facial recognition)[118], and limits on how data is stored and transferred [119].
- **Clear disclosure:** In order to advocate and make informed decisions about their interests, employees need to be made aware of how their information is being collected, stored, and used. This is a principle that applies across data collection in the workplace

[20] but is particularly important in the context of intelligent building systems where sensors may not be visible. This should include understandable explanation about who has access to the information (e.g., supervisors) and any use of algorithms [20]. Targeting this disclosure requirement to employees (rather than all visitors to commercial buildings) would reduce compliance costs for employers and building owners and target to areas of higher risk.

- **Right to access:** For effective protections, it is not enough for employees to know that information is being collected about them; they need to be able to access the data record itself. Without that access, they can't contest inaccurate information that might be used to evaluate their performance or have impacts beyond the workplace [120], [121]. Access is also a pre-condition for real choice and control over information collection, rather than an unrealistic opt-in or opt-out for all data collection and use drawn from intelligent building systems.

Together, these three principles of legislative reform would shift from an environment where most data collection and use is permitted — either through pro forma consent or broad exemptions — to one with clear "guardrails" [91] of protections. Yet legislative reform on its own is not enough to strengthen protections — it needs to be paired with appropriate enforcement and responsive regulation.

4.1.2 Strengthening Enforcement

The lack of meaningful enforcement as a deterrent is a long-established gap in protecting privacy for employees and more generally [122]. The potential economic benefits of data collection and the potential costs of compliance have increased with technological development, and enforcement is largely stuck in the Windows 95 era of computing. For effective protections, oversight bodies need the capacity to investigate potential breaches and to levy penalties with teeth.

To be effective, workplace privacy enforcement should be easily accessible and have accountability channels that allow for employees to report breaches while having their identity protected from their employers. Individual employees are unlikely to risk raising complaints where they can expect it to negatively affect their livelihoods [123]. While legal whistleblower protections can play a role, the best protection against reprisal is to shield identities.

Stronger enforcement goes hand in hand with legislative reform. Changes to laws would be needed to allow for stronger penalties and binding orders, and to allow for additional activities such as proactive investigations [124]. Proposed federal privacy reform in 2021 included changes to the structure of enforcement bodies, including a new tribunal [91]. Quebec's new privacy legislation also introduces stronger enforcement, modeled off Europe's GDPR [125].

4.1.3 Responsive Regulation

The gaps in workplace privacy protections for intelligent buildings exist because the design of those protections have largely stood still while digitization increased exponentially. While PIPEDA was designed with a requirement to be reviewed and refined every five years [116], that process has been effectively abandoned.

To keep up with evolving technologies and business practices, our policy frameworks do not just need to be updated today — they need to continue to adapt. One way to ensure that parliamentarians are more responsive to this task than they were for PIPEDA was to ensure that exemptions that allow for data collection and use "sunset" or expire every five years — a common review period used in other legislation such as the Bank Act — unless they are reviewed and renewed. This would ensure more engagement by policymakers and ensure that a gap does not penalize employees.

Another driver of gaps in the policy and regulatory landscape is the fact that policymakers lack the technical capacity to make informed decisions about approaches to fast moving technology. Governments need to better develop, attract and retain technology policy expertise, and make it available to both government and parliamentarians. A dedicated institution, like the US White House Office of Science and Technology Policy, could convene relevant and up-to-date technical advice to help policymakers

understand how technology is being implemented and the implications for Canadians [126]. This work can also be supported within existing institutions — for example, the US Equal Employment Opportunity Commission launched its own initiative to assess how AI used in hiring could affect civil rights and anti-discrimination laws [127].

4.2 Empowering Workers

The outsized risk to employees when it comes to their privacy in workplaces with intelligent building systems stems in large part from the power imbalance. In turn, there is significant opportunity to build constructive solutions to workplace privacy for intelligent building systems by empowering employees.

There are opportunities to involve employees more actively in data management and governance throughout the "life cycle" of data collected by intelligent building systems: at a foundational level by engaging workers in policymaking; in the active management and governance of data; and in systems of accountability and oversight.

4.2.1 Engage Workers in Policymaking

Decision-makers shaping privacy and employment policies that govern data collection and management from intelligent building systems are unlikely to have experience with the harmful effects of surveillance in the workplace or to hear actively from those who do. The voices of these workers tend to be left out of discussion and policymaking — and the results are policies that don't reflect their needs and interests [128], [23].

To overcome this gap, policymakers should consider more creative and proactive forms of engagement that bring employees' perspective into policymaking. This means going beyond traditional consultation processes, which are likely to be dominated by industry voices with vested interests. Collaborative models that engage employees on policy questions could include focused processes such as citizens' assemblies or juries that bring ordinary people into policymaking processes [129], or more formal ongoing advisory bodies that bring in people's real-life experiences, like the Canada Revenue Agency's Disability Advisory Committee [130].

4.2.2 Shared Governance and Decision-making

Another opportunity to empower workers is to create shared governance models where employees have a say in how data is managed — and even a stake in its benefits.

Shared decision making over some aspects of how the workplace is managed is not new to Canada. Joint health and safety committees are a feature of labour regulations in most provinces and provide a venue for employees and management to meet and make plans to protect health and safety in the workplace [131]. This is a model that could be expanded or used as a model to manage data collection about employees in intelligent buildings. For example, a joint data governance committee could require co-chairs from employees and management and be responsible for reviewing an organization's electronic monitoring policies and any new technology instalment or data use.

Other models of shared governance include new organizational approaches such as data trusts that allow for access to deanonymized data with safeguards for purposes with broader benefits [132]. Shared ownership in data could be about a stake in direct economic benefits [121] but it can also include empowering employees in their own work. For example, some groups of workers using gig work platforms have created initiatives to pool and share their own data to help them approach their work on the platforms [133]. This model could be translated to other employee data (including the data generated from intelligent building systems) to empower employees to learn and benefit from data they generate in their work.

4.2.3 Strengthen Advocacy Avenues for Workers

Even if upstream initiatives to engage workers in policymaking and data governance were in place, employees still need better channels to advocate for their interests. This includes both the ability to address individual privacy risks and to advocate collectively.

To understand how their privacy rights may have been affected and to advocate for their interests, employees need to navigate complex technical and legal

"Privacy is not just an individual right — it's a collective right, and individuals are not much better off if they opt out of data collection while their peers do not."

information or invest heavily in legal representation. This is an unrealistic pathway for most employees, especially lower-income workers who are more likely to face invasive surveillance. One potential model is to fund specialized workplace privacy legal clinics to provide resources and advice, similar to some of the specialty legal clinics that exist in other fields.

Privacy is not just an individual right — it's a collective right, and individuals are not much better off if they opt out of data collection while their peers do not [123]. Collective bargaining can play a role — though a 2004 study found that only one per cent of collective agreements contained provisions related to electronic surveillance [122], they can provide advocates for employees and mitigate the use electronic surveillance in the workplace for purposes such as performance management or dismissal.

Another avenue is the creation of ombuds offices, either within larger organizations or created jointly by employers across a sector with a common code of conduct [123]. In an intelligent buildings systems context, these joint approaches could also be facilitated by large property managers as a service to their tenants where there are similar work environments and monitoring systems in place. These voluntary approaches would be established to build trust and common expectations between employees and employers and allow employers to jointly resource this responsibility.

4.3 Supporting Industry Leadership

While some adoption of intelligent building systems is done explicitly with employee monitoring and surveillance in mind, most building owners and employers are motivated by other factors including energy efficiency, security, and comfort. During the COVID-19 pandemic, many building operators and employers were asked to take on new public health monitoring responsibilities without notice and with little guidance on appropriate technologies or data management practices for this new sensitive data. One element of a cohesive policy response is to support best practices by industry, including technology providers, buildings owners and managers, and employers.

4.3.1 Standardization

Intelligent building systems face a general gap in standards related to consistent definitions, cybersecurity, and interoperability [9]. While some standards exist for the interoperability of components such as lighting systems (e.g., IEEE 802.3 [134] and CSA C22.2 No. 250.2[135]), more focus is needed on these standards that can be applied to intelligent buildings at a systems level [9]. One such example is the CSA information and communication technology code for building, currently under development, which will standardize the information communication technology (ICT) infrastructure and its data related component within an intelligent building.

Development of a suite of standards related to the security, privacy, and data management of personal data captured by intelligent building systems could support employers and building owners to make informed privacy-friendly purchase decisions in deploying technology. These standards could also provide a common set of principles to support shared governance decisions between employees and employers, and broader efforts like ombuds offices.

A common set of established standards may also be useful for practices intended to help protect workplace privacy rights. For example, third-party audits or impact assessments are an increasingly common approach to provide all parties with confidence that data is being managed appropriately and algorithms used to process it are free of bias. However, as an emerging practice with multiple professions involved, there is a lack of consistency in how these reviews operate and whose interests are represented. A set of standards or practice guidelines could provide consistency and confidence to employers and employees alike.

Because many of the systems in intelligent buildings are installed by the building owner, their use and the data they generate are generally managed in commercial lease clauses. The creation of model commercial lease clauses around the use of intelligent building systems and the data they generate based on strong principles of clear limits, disclosure and access rights could support industry leadership and promote strong workplace privacy norms. For example, in England and Wales, a set of Model Commercial Leases were commissioned by the British Property Federation to support ease of transactions in the industry [136]. Many provinces provide standard forms of residential leases, either on a voluntary or mandatory basis [137], [138].

4.3.2 Capacity Building and Best Practices

Designers and managers of intelligent building systems are often navigating new territory without a map. Better information about risks and best practices can support better outcomes. One model is the Canadian Centre for Cybersecurity — a federal agency with a mandate that includes information, training, and resources to encourage stronger cybersecurity practices and to monitor potential vulnerabilities in Canada's critical infrastructure, regardless of who owns and manages it [139]. Given the close relationship between cybersecurity of critical infrastructure and privacy of data collected by sensors, this function could be developed as part of the Centre's mandate or through a dedicated initiative building on the Centre's model.

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" [140]. This approach could align well with the practices of larger firms that include a Chief Data Officer role but also risks creating further regulatory confusion with a large number of regulatory and quasi-enforcement bodies [91].

Documenting and sharing best practices does not need to be government-led. Industry coalitions and non-profits can also collaborate to identify best practices and share information. Employer groups and industry associations can play a leadership role by bringing together lessons from across a variety of settings to document and share lessons quickly.

Conclusion

As intelligent building systems become increasingly common, these spaces are increasingly sources of information about the people who spend time in these buildings and their work. Deployed responsibly, these systems can make our workplaces more sustainable, safe, and comfortable. However, without an appropriate management framework in place, the personal information that intelligent building systems capture can present significant privacy risks to employees.

In recent years, the digitization of the economy has prompted a significant rethink of both privacy and labour standards, both in policy and legislative frameworks and directly in the relationship between companies, consumers, and workers. To date, the proposed reforms have largely overlooked the question of workplace privacy and how data records could affect livelihoods or facilitate discrimination.

This gap has grown through the course of the COVID-19 pandemic. The public health crisis has prompted an acceleration in the adoption of intelligent building systems, both as part of an asset management strategy for owners of underused commercial spaces and as a direct response to the emergency. The result is an increasing scale and scope of sensitive data being captured about employees in the absence of consistent safeguards for employees or guidance for building managers or employers.

Decision-makers across sectors have a role to play in implementing these safeguards to support the use of intelligent building systems in a way that benefits everyone. Leadership from government is needed to reduce regulatory uncertainty and to strengthen labour and privacy protections. Renewed policy frameworks should be grounded in principles of clear limits, clear disclosure, and a right to access. Employees can play a role in shaping and implementing practices, including through shared governance models like data trusts. Industry leaders from technology providers to employers can set in place strong privacy practices by designing systems for privacy and sharing best practices.

As we look past the emergency response of the pandemic, it is imperative to look ahead to what our workplaces will look like going forward. While many organizations are focusing on the balance between remote and in-person experiences for their employees and customers, there are also significant changes happening to workplaces themselves — often literally hidden from view. Proactive approaches can ensure that emergency measures do not have negative effects on workplaces for the long-term.

References

[1] Infineon Technologies, "Smart Buildings: Definition & Creation," https://www.infineon.com/cms/en/discoveries/smart-buildings/ (accessed Feb. 09, 2022).

[2] S. Sousan, M. Fan, K. Outlaw, S. Williams, and R. L. Roper, "SARS-CoV-2 Detection in Air Samples from Inside Heating, Ventilation, and Air Conditioning (HVAC) Systems – COVID Surveillance in Student Dorms," Am. J. Infect. Control, vol. 0, no. 0, pp. 1-6, 2021, doi: 10.1016/J.AJIC.2021.10.009/ATTACHMENT/43E455C8-3DE1-4088-A4DF-9B7636BD94BB/MMC1.DOCX.

[3] Kate Connolly, "Disinfection Robots and Thermal Body Cameras: Welcome to the Anti-Covid Office," The Guardian, 2021. https://www.theguardian.com/money/2021/aug/21/covid-free-office-h3-bucharest-disinfection-robots-thermal-body-cameras (accessed Feb. 10, 2022).

[4] Grace Woodruff, "COVID Screenings: Why Your Temperature Reading Might Be Inaccurate," Slate, 2021. https://slate.com/technology/2021/07/temperature-covid-check-inaccurate-theater.html (accessed Feb. 09, 2022).

[5] A. Nguyen, "New Digital Infrastructures of Workplace Health and Safety," Oct. 2020. Accessed: Nov. 19, 2021. [Online]. Available: https://www.mediatechdemocracy.com/work/new-digital-infrastructures-of-workplace-health-and-safety.

[6] Akshay Thakur, "Smart Buildings Set to Be A Staple In Post-Pandemic World," https://www.workdesign.com/2021/04/smart-buildings-set-to-be-a-staple-in-post-pandemic-world/ (accessed Feb. 09, 2022).

[7] L. Saad and B. Wigert, "Remote Work Persisting and Trending Permanent," Gallup, Oct. 13, 2021.

[8] T. Mehdi and R. Morisette, "Working from Home: Productivity and Preferences," Apr. 2021. Accessed: Jan. 31, 2022. [Online]. Available: https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00012-eng.htm.

[9] D. Labonte et al., "Intelligent Buildings: Layout and Relevant Standards," CSA Group, Toronto, ON, Canada, Dec. 2021. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Intelligent-Buildings-Layout-and-Relevant-Standards.pdf.

[10] "Global Smart Buildings Market (2021 to 2026) Technology, Infrastructure, Solutions and Deployment Models," Research and Markets, Jun. 13, 2021. https://www.globenewswire.com/news-release/2021/07/13/2261658/28124/en/Global-Smart-Buildings-Market-2021-to-2026-by-Technology-Infrastructure-Solutions-and-Deployment-Models.html (accessed Dec. 01, 2021).

[11] O. Omar, "Intelligent Building, Definitions, Factors and Evaluation Criteria of Selection," Alexandria Eng. J., vol. 57, no. 4, pp. 2903–2910, Dec. 2018, doi: 10.1016/J.AEJ.2018.07.004.

[12] Juan Pedro Tomas, "The Impact of IoT in Smart Buildings," In-Building Tech, 2020. https://inbuildingtech.com/smart-buildings/the-impact-iot-smart-buildings/ (accessed Feb. 09, 2022).

[13] "About the Commercial Buildings Integration Program," US Department of Energy. https://www.energy.gov/eere/buildings/about-commercial-buildings-integration-program (accessed Feb. 10, 2022).

[14] "Smart Buildings: Enabling Predictive Maintenance," Iota Communications, 2020. https://www.iotacommunications.com/blog/smart-building-predictive-maintenance/ (accessed Feb. 10, 2022).

[15] Daisuke Wakabayashi, "Google's Plan for the Future of Work: Privacy Robots and Balloon Walls," The New York Times, 2021. https://www.nytimes.com/2021/04/30/technology/google-back-to-office-workers.html (accessed Feb. 09, 2022).

[16] Ross Miller and Julie Miner, "Even in Tech-forward Buildings, the Focus is still on the People," 2019. https://www.cohnreznick.com/insights/even-in-tech-forward-buildings-the-focus-is-still-on-the-people (accessed Feb. 09, 2022).

[17] Darrell M. West, "How Employers Use Technology to Surveil Employees," 2021. https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/ (accessed Feb. 09, 2022).

[18] Jeff Gavin, "Smart Lighting From 9 to 5: Office Lighting," Electrical Contractor Magazine. https://www.ecmag.com/section/lighting/smart-lighting-9-5-office-lighting (accessed Feb. 10, 2022).

[19] E. P. Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance," Feb. 2004. Accessed: Mar. 02, 2022. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf.

[20] A. Bernhardt, L. Kresge, and R. Suleiman, "Data and Algorithms at Work: The Case for Worker Technology Rights," Berkeley, CA, USA, Nov. 2021. [Online]. Available: https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf.

[21] L. Matsakis, "At An Outback Steakhouse Franchise, Surveillance Blooms," Wired, Oct. 19, 2019.

[22] A. Mateescu, "Data & Society — Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care," Nov. 2021. Accessed: Nov. 18, 2021. [Online]. Available: https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care/.

[23] A. Nguyen, "The Constant Boss: Work Under Digital Surveillance," New York, NY, USA, May 2021. [Online]. Available: https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf.

[24] "Powering the Smart Factory with the Internet of Things," The Possibility Report. https://www.theatlantic.com/sponsored/vmware-2017/iot-manufacturing/1751/ (accessed Feb. 09, 2022).

[25] Jodi Kantor, Karen Weise, and Grace Ashford, "Inside Amazon's Employment Machine," New York Times, Jun. 15, 2021. https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html (accessed Feb. 09, 2022).

[26] "Can Smart Buildings Lead to Smart Cities?," Wired, 2019. https://www.wired.com/wiredinsider/2019/11/can-smart-buildings-lead-smart-cities/ (accessed Feb. 09, 2022).

[27] Jack Kelly, "Google Has Master Plan to Build A Massive Corporate Town For Its Employees," 2020. https://www.forbes.com/sites/jackkelly/2020/09/04/google-has-master-plan-to-build-a-massive-corporate-town-for-its-employees/?sh=1b0ee00f2d78 (accessed Feb. 09, 2022).

[28] Nate Berg, "Qualcomm Turns Its Corporate Campus Into a Mini Smart City," Fast Company. https://www.fastcompany.com/90583927/this-corporate-campus-is-now-a-mini-smart-city (accessed Feb. 09, 2022).

[29] M. J. Masoodi, N. Abdelaal, S. Tran, Y. Stevens, | Sam, and A. | Karim Bardeesy, "Workplace Surveillance and Remote Work," 2021, Accessed: Nov. 06, 2021. [Online]. Available: https://www.cybersecurepolicy.ca/workplace-surveillance.

[30] Jennifer Alsever, "Use of Employee Surveillance Software Has Jumped Over 50% Since the Pandemic Started," 2021. https://fortune.com/2021/09/01/companies-spying-on-employees-home-surveillance-remote-work-computer/ (accessed Feb. 09, 2022).

[31] A. M. Townsend and J. T. Bennett, "Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy," J. Labor Res., vol. 24, pp. 195–205, 2003, doi: 10.1007/BF02701789.

[32] T. Scassa, "Privacy in the Precision Economy: The Rise of AI-Enabled Workplace Surveillance During the Pandemic," Centre for International Governance Innovation, Jun. 08, 2021. https://www.cigionline.org/articles/privacy-in-the-precision-economy-the-rise-of-ai-enabled-workplace-surveillance-during-the-pandemic/.

[33] A. Albrechtslund and T. Ryberg, "Participatory Surveillance in the Intelligent Building," Des. Issues, vol. 27, no. 3, pp. 35–46, 2011, [Online]. Available: http://www.jstor.org/stable/41261942.

[34] C. Pathmabandu, J. Grundy, M. B. Chhetri, and Z. Baig, "An Informed Consent Model for Managing the Privacy Paradox in Smart Buildings," in 35th IEEE/ACM International Conference on Automated Software Engineering Workshops, 2020, pp. 19–26, doi: 10.1145/3417113.3422180.

[35] A. Mateescu and A. Nguyen, "Explainer: Workplace Monitoring & Surveillance," New York, NY, USA, Feb. 2019. [Online]. Available: https://apo.org.au/sites/default/files/resource-files/2019-02/apo-nid218571.pdf.

[36] R. Barrette, "Privacy in our Smart Cities," Toronto, ON, Canada, Jun. 2018. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/2018/06/2018-06-20-its-privacy-and-smart-cities-web.pdf.

[37] K. Zickuhr et al., "Workplace Surveillance Is Becoming the New Normal for U.S. Workers," 2021.

[38] C. Ramsaroop, "Reality Check 101: Rethinking the Impact of Automation and Surveillance on Farm Workers," Data & Society: Points. https://points.datasociety.net/reality-check-101-c6e501c3b9a3 (accessed Jan. 27, 2022).

[39] K. Grieman, "Smart City Privacy in Canada," Ottawa, ON, Canada, Jan. 2019. [Online]. Available: https://iapp.org/media/pdf/resource_center/Smart_Cities_OPC_2019.pdf.

[40] A. Qureshi, S. M. Afaqui, and J. Salas, "IoTFC: A Secure and Privacy Preserving Architecture for Smart Buildings," in Security and Privacy in New Computing Environments, D. Wang, W. Meng, and J. Han, Eds. Cham, Switzerland: Springer, 2021, pp. 102–119.

[41] S. Harper, M. Mehrnezhad, and J. C. Mace, "User Privacy Concerns and Preferences in Smart Buildings," in Socio-Technical Aspects in Security and Trust, T. Groß and L. Viganò, Eds. Cham, Switzerland: Springer, 2020.

[42] M. Guariglia and C. Quintin, "Thermal Imaging Cameras are Still Dangerous Dragnet Surveillance Cameras," Electronic Frontier Foundation, Apr. 07, 2020. https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dragnet-surveillance-cameras (accessed Jan. 27, 2022).

[43] M. H. Jarrahi, G. Newlands, M. K. Lee, C. T. Wolf, E. Kinder, and W. Sutherland, "Algorithmic Management In a Work Context," Big Data Soc., vol. 8, no. 2, pp. 1-14, 2021, doi: 10.1177/20539517211020332.

[44] A. Mateescu and A. Nguyen, "Explainer: Algorithmic Management in the Workplace," New York, NY, USA, 2019. [Online]. Available: https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf.

[45] European Parliamentary Research Service, "Understanding Algorithmic Decision-Making: Opportunities and Challenges," Brussels, Belgium, Mar. 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.

[46] H. Schaller, G. Zanfir-Fortuna, and R. Hendricks-Sturrup, "Thermal Imaging as Pandemic Exit Strategy: Limitations, Use Cases and Privacy Implications," Future of Privacy Forum, Jun. 03, 2020. https://fpf.org/blog/thermal-imaging-as-pandemic-exit-strategy-limitations-use-cases-and-privacy-implications/.

[47] K. Ball, "Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations," Luxembourg, Luxembourg, 2021. doi: 10.2760/5137.

[48] P. V. Moore, "Data Subjects, Digital Surveillance, AI and the Future of Work," Brussels, Belgium, Dec. 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf.

[49] E. Princi and N. C. Krämer, "Acceptance of Smart Electronic Monitoring at Work as a Result of a Privacy Calculus Decision," Informatics, vol. 6, no. 3, p. 40, 2019, doi: 10.3390/informatics6030040.

[50] C. Catenacci, "Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap," Electronic Thesis and Dissertation Repository, Western University, 2020.

[51] A. E. Waldman, "Privacy as Trust: Sharing Personal Information in a Networked World," SSRN Electron. J., Mar. 2014, doi: 10.2139/SSRN.2309632.

[52] S. Kejriwal and S. Mahajan, "Smart Buildings: How IoT Technology Aims to Add Value for Real Estate Companies," London, United Kingdom, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-fsi-real-estate-smart-buildings-how-iot-technology-aims-to-add-value-for-real-estate-companies.pdf.

[53] D. Brooks, "Security Threats and Risks of Intelligent Building Systems: Protecting Facilities from Current and Emerging Vulnerabilities," Secur. Crit. Infrastructures Crit. Control Syst. Approaches Threat Prot., pp. 1–16, 2012, doi: 10.4018/978-1-4666-2659-1.CH001.

[54] A. Llaria, J. Dos Santos, G. Terrasson, Z. Boussaada, C. Merlo, and O. Curea, "Intelligent Buildings in Smart Grids: A Survey on Security and Privacy Issues Related to Energy Management," Energies, vol. 14, p. 2733, 2021, doi: 10.3390/en14092733.

[55] C. Catenacci, "Plenty of Phishing Going On," First Reference, Sep. 07, 2021.

[56] Canadian Centre for Cyber Security, "Ransomware Playbook (ITSM.00.099)," Nov. 2021. Accessed: Mar. 09, 2022. [Online]. Available: https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099.

[57] Institution of Engineering and Technology, "Intelligent Buildings: Understanding and Managing the Risks," London, United Kingdom, Jan. 2015. [Online]. Available: https://www.fm-house.com/wp-content/uploads/2015/01/Intelligent-Buildings.pdf.

[58] P. Pappachan et al., "Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences," in IEEE 37th International Conference on Distributed Computing Systems Workshops, Jul. 2017, pp. 193-198, doi: 10.1109/ICDCSW.2017.52.

[59] Office of the Privacy Commissioner of Canada, "Guidance on Covert Video Surveillance in the Private Sector," May 2009. Accessed: Mar. 02, 2022. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/surveillance/video-surveillance-by-businesses/gd_cvs_20090527/.

[60] C. Catenacci, "Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap," University of Western Ontario, 2020.

[61] Deloitte, "The Use of Smart Building Technology," 2020. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-smart-building-tech-pov.pdf (accessed Feb. 09, 2022).

[62] John Seabrook, "Has the Pandemic Transformed the Office Forever?," The New Yorker, 2021. https://www.newyorker.com/magazine/2021/02/01/has-the-pandemic-transformed-the-office-forever (accessed Feb. 09, 2022).

[63] Alex Cyr, "Case Study: How a Growing Company Overhauled Its Office During the Pandemic," The Globe and Mail, 2021. https://www.theglobeandmail.com/canada/article-case-study-how-a-growing-company-overhauled-its-office-during-the/ (accessed Feb. 09, 2022).

[64] "Privacy and the COVID-19 Outbreak," Office of the Privacy Commissioner of Canada, Mar. 2020. https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/ (accessed Feb.10, 2022).

[65] Claire Brownell, "The Workplace of the Future Will Probably Remain Under Surveillance," 2020. https://www.macleans.ca/work/the-workplace-of-the-future-will-probably-remain-under-surveillance/ (accessed Feb. 09, 2022).

[66] S. Bryant, "Electronic Surveillance in the Workplace," Can. J. Commun., vol. 20, no. 4, 1995, doi: 10.22230/cjc.1995v20n4a893.

[67] M. J. Masoodi, N. Abdelaal, S. Tran, Y. Stevens, S. Andrey, and K. Bardeesy, "Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Admidst COVID-19 in Canada," Toronto, ON, CAN, Sep. 2021. Accessed: Oct. 21, 2021. [Online]. Available: https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/6166d5e131d8606af68eccf9/1634129758502/Workplace+Surveillance+and+Remote+Work.pdf.

[68] Personal Information Protection and Electronic Documents Act. SC 2000, c 5.

[69] Office of the Privacy Commissioner of Canada, "PIPEDA in brief," OPC, May 2019. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (accessed Nov. 25, 2021).

[70] Office of the Privacy Commissioner of Canada, "Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)," OPC, May 2018. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.

[71] Personal Information Protection and Electronic Documents Act. SC 2000, c 5.

[72] "Minister of Innovation, Science and Industry Mandate Letter," Office of the Prime Minister of Canada, Dec. 16, 2021. https://pm.gc.ca/en/mandate-letters/2021/12/16/minister-innovation-science-and-industry-mandate-letter.

[73] M. Hemmadi, "Champagne Promises Updated Privacy Legislation in New Year," The Logic, Dec. 06, 2021. https://thelogic.co/news/champagne-promises-updated-privacy-legislation-in-new-year/.

[74] Office of the Privacy Commissioner of Canada, "Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)," OPC, May 2018.

[75] S. Richardson and D. Mackinnon, "Left to Their Own Devices? Privacy Implications of Wearable Technology in Canadian Workplaces," 2017. Accessed: Jan. 31, 2022. [Online]. Available: https://www.sscqueens.org/sites/sscqueens.org/files/left_to_their_own_devices.pdf.

[76] Privacy Act. RSC, 1985, c. P-21 (Online).

[77] Department of Justice, "Modernizing Canada's Privacy Act – Online Public Consultation," Government of Canada. https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.html (accessed Feb. 04, 2022).

[78] "Minister of Justice and Attorney General of Canada Mandate Letter," Office of the Prime Minister of Canada, Dec. 16, 2021. https://pm.gc.ca/en/mandate-letters/2021/12/16/minister-justice-and-attorney-general-canada-mandate-letter.

[79] An Act to modernize legislative provisions as regards the protection of personal information. National Assembly of Quebec, 2021.

[80] Office of the Privacy Commissioner of Canada, "Summary of privacy laws in Canada," OPC, Jan. 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-1.

[81] E. Denham, "Investigation Report F15-01: Use of Employee Monitoring Software by the District of Saanich," Victoria, BC, Canada, Mar. 2015. [Online]. Available: https://www.oipc.bc.ca/investigation-reports/1775.

[82] Act respecting the protection of personal information in the private sector. CQLR, c P-39.1.

[83] Government of Alberta, "Federally regulated industries – Employment standards exceptions." https://www.alberta.ca/es-exceptions-federally-regulated-industries.aspx (accessed Feb. 08, 2022).

[84] Canada Labour Code. RSC 1985, c L-2.

[85] "Electronic Employee Monitoring: Potential Reform Options."

[86] R. Kattapuram, "An Employer's Guide to Privacy in the Workplace," Canadian Employment & Labour Law, Aug. 08, 2018. https://www.employmentandlabour.com/an-employers-guide-to-privacy-in-the-workplace/ (accessed Nov. 25, 2021).

[87] V. Hooper, G. Anderson, and S. Blumenfeld, "A question of trust: should bosses be able to spy on workers, even when they work from home?," The Conversation, Jun. 16, 2020. https://theconversation.com/a-question-of-trust-should-bosses-be-able-to-spy-on-workers-even-when-they-work-from-home-140623 (accessed Nov. 25, 2021).

[88] S. J. Kiss and V. Mosco, "Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada," Can. J. Commun., vol. 30, no. 4, pp. 549-564, 2005, doi: 10.22230/cjc.2005v30n4a1671.

[89] D. Doorey, The Law of Work, 2nd ed. Emond Publishing, 2020.

[90] H. M. McNaughton, Bill 88, Working for Workers Act, 2022. Legislative Assembly of Ontario, 2022.

[91] V. Bednar, "Debating the Right Balance(s) for Privacy Law in Canada: Summary and Discussion of Two Roundtables," Jan. 2022. Accessed: Feb. 09, 2022. [Online]. Available: https://ppforum.ca/wp-content/uploads/2022/01/DebatingTheRightBalancesForPrivacyLawInCanada-PPF-Jan2022-EN.pdf.

[92] United Nations General Assembly, Universal Declaration of Human Rights. 1948.

[93] UN General Assembly, International Covenant on Civil and Political Rights. 1966.

[94] Human Rights Council, The right to privacy in the digital age: resolution. 2019.

[95] UN Office of the High Commissioner on Human Rights, "Special Rapporteur on the right to privacy." https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (accessed Mar. 09, 2022).

[96] International Labour Organization, "Protection of workers' personal data," Geneva, Switzerland, 1997. [Online]. Available: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

[97] International Organization for Standardization, "ISO - ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection." https://www.iso.org/committee/45306.html (accessed Mar. 09, 2022).

[98] Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. ISO/IEC 27701:2019.

[99] Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines (Adopted ISO/IEC 27701:2019, first edition, 2019-08) CSA ISO/IEC 27701:20

[100] Cybersecurity – IoT security and privacy – Guidelines. ISO/IEC DIS 27400.

[101] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regu. OJ L 119, 4.5.2016, p 1.

[102] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," Wilmslow, Chesire, England, Aug. 2018. [Online]. Available: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

[103] Trades Union Congress, "Your right to privacy at work," London, United Kingdom. [Online]. Available: https://www.tuc.org.uk/sites/default/files/tuc/privacyatwork.pdf.

[104] Information Commissioner's Office, "Guide to the UK General Data Protection Regulation (UK GDPR)," ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed Feb. 04, 2022).

[105] T. K. Lively, "US State Privacy Legislation Tracker," International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (accessed Mar. 09, 2022).

[106] I. Ajunwa, K. Crawford, and J. Schultz, "Limitless Worker Surveillance," Calif. Law Rev., vol. 105, no. 3, pp. 735–776, 2017, doi: 10.15779/Z38BR8MF94.

[107] California Consumer Privacy Act of 2018. Cal. Stats. 2018, c 55, s 3.

[108] W. Ellis, "Workplace Surveillance Act NSW," Privacy Australia, Apr. 06, 2021. https://privacyaustralia.net/workplace-surveillance-act-nsw/.

[109] "5 Things You Need to Know About The Workplace Surveillance Act – Lawpath," https://lawpath.com.au/blog/5-things-you-need-to-know-about-the-workplace-surveillance-act (accessed Nov. 28, 2021).

[110] N. Zon and A. Lipsey, "Children's Safety and Privacy in the Digital Age," May 2020. Accessed: Jun. 15, 2020. [Online]. Available: https://www.csagroup.org/article/research/childrens-safety-and-privacy-in-the-digital-age/.

[111] K. Alwani and M. C. Urban, "The Digital Age: Exploring the Role of Standards for Data Governance, Artificial Intelligence and Emerging Platforms," May 2019. Accessed: Aug. 31, 2020. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-research-Digital-Economy.pdf.

[112] S. Johal et al., "Report of the Expert Panel on Modern Federal Labour Standards," 2019. Accessed: Feb. 03, 2022. [Online]. Available: https://www.canada.ca/en/employment-social-development/corporate/portfolio/labour/programs/labour-standards/reports/what-we-heard-expert-panel-modern-federal.html.

[113] Office of the Privacy Commissioner of Canada, "The future of privacy law reform in Canada," May 2021. Accessed: Feb. 03, 2022. [Online]. Available: https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210526/.

[114] Ministry of Government and Consumer Services, "Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy," Toronto, ON, CAN, Jun. 2021.

[115] Government of Ontario, "Ontario Releases Report to Lead the Future of Work," Dec. 2021. Accessed: Feb. 03, 2022. [Online]. Available: https://news.ontario.ca/en/release/1001304/ontario-releases-report-to-lead-the-future-of-work.

[116] I. Ajunwa, "Protecting Workers' Civil Rights in the Digital Age," Accessed: Nov. 11, 2021. [Online]. Available: https://scholarship.law.unc.edu/ncjolt/vol21/iss4/2.

[117] P. and E. House of Commons Standing Committee on Access to Information, "Statutory Review of the Personal Information Protection and Electronic Documents Act," May 2007. Accessed: Feb. 09, 2022. [Online]. Available: https://www.ourcommons.ca/Content/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-e.pdf.

[118] H. Kronk, "Facial Recognition Technology in the Workplace: Employers Use It, Workers Hate It, Regulation Is Coming for It," Corporate Compliance Insights, Mar. 03, 2021.

[119] D. West, "How employers use technology to surveil employees," Brookings Institutionng, 2021. https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/ (accessed Jan. 24, 2022).

[120] American Civil Liberties Union, "Privacy in America: Electronic Monitoring," 2003. Accessed: Nov. 18, 2021. [Online]. Available: https://www.aclu.org/other/privacy-america-electronic-monitoring.

[121] S. Adler-Bell and M. Miller, "The Datafication of Employment: How Surveillance and Capitalism Are Shaping Workers' Futures without Their Knowledge," New York, NY, USA, Dec. 2018. [Online]. Available: https://production-tcf.imgix.net/app/uploads/2018/12/03160631/the-datafication-of-employment.pdf.

[122] M. R. Bueckert, "Electronic Employee Monitoring: Potential Reform Options," Manit. Law J., pp. 99-116, 2009, [Online]. Available: http://themanitobalawjournal.com/wp-content/uploads/articles/UTGB_6/Electronic-Employee-Monitoring:-Potential-Reform-Options.pdf.

[123] M. Lane, "Regulating platform work in the digital age," Paris, France, 2020. [Online]. Available: https://goingdigital.oecd.org/toolkitnotes/regulating-platform-work-in-the-digital-age.pdf.

[124] N. Abdelaal and S. Tran, "Abdelaal and Tran: Proposed right-to-disconnect plan falls short," Ottawa Citizen, Nov. 04, 2021. https://ottawacitizen.com/opinion/abdelaal-and-tran-ontarios-proposed-right-to-disconnect-policies-fall-short-on-protecting-privacy?utm_source=pocket_mylist.

[125] BLG, "Québec adopts Bill 64 – Key requirements for businesses," Sep. 2021. Accessed: Nov. 25, 2021. [Online]. Available: https://www.blg.com/en/insights/2021/09/quebec-adopts-bill-64-key-requirements-for-businesses.

[126] Federal Register of the United States Government, "Science and Technology Policy Office," https://www.federalregister.gov/agencies/science-and-technology-policy-office (accessed Feb. 09, 2022).

[127] U.S. Equal Employment Opportunity Commission, "EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness," Oct. 28, 2021. https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness (accessed Feb. 09, 2022).

[128] A. Nguyen, "Work Under Digital Surveillance," May 2011. Accessed: Dec. 01, 2021. [Online]. Available: https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf.

[129] OECD, "Innovative Citizen Participation and New Democratic Institutions," OECD, Jun. 2020. doi: 10.1787/339306DA-EN.

[130] Canada Revenue Agency, "Disability Advisory Committee (DAC)," https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/disability-advisory-committee.html (accessed Feb. 09, 2022).

[131] Canadian Centre for Occupational Health and Safety, "Joint Health and Safety Committee – What is a Joint Health and Safety Committee?," https://www.ccohs.ca/oshanswers/hsprograms/hscommittees/whatisa.html (accessed Feb. 09, 2022).

[132] C. Bernier, "Governance for Innovation and Privacy: The Promise of Data Trusts and Regulatory Sandboxes," Feb. 2021. Accessed: Feb. 09, 2022. [Online]. Available: https://www.cigionline.org/articles/governance-innovation-and-privacy-promise-data-trusts-and-regulatory-sandboxes/.

[133] K. Gregory, "'Worker Data Science' Can Teach Us How to Fix the Gig Economy," Wired, Dec. 07, 2021.

[134] Standard for Ethernet, IEEE 802.3-2018, IEEE SA, Piscataway, NJ, 2018

[135] Lighting systems. CSA C22.2 No. 250.2:20, Canadian Standards Association, Toronto, 2020

[136] Model Commercial Lease UK, "Model Commercial Lease." https://modelcommerciallease.co.uk/frequently-asked-questions/ (accessed Mar. 09, 2022).

[137] Government of Ontario, "Guide to Ontario's standard lease," https://www.ontario.ca/page/guide-ontarios-standard-lease (accessed Mar. 09, 2022).

[138] Government of New Brunswick, "The standard lease," https://www2.gnb.ca/content/gnb/en/corporate/promo/renting-in-new-brunswick/lease-information/standard-lease.html (accessed Mar. 09, 2022).

[139] "Canadian Centre for Cyber Security," https://cyber.gc.ca/en/ (accessed Feb. 10, 2022).

[140] Government of Canada, "Budget 2021: Part 2 – Creating Jobs and Growth," 2021. Accessed: Feb. 10, 2022. [Online]. Available: https://www.budget.gc.ca/2021/report-rapport/p2-en.html.

Appendix A – Stakeholder Interviews

Interview Questions

Some or all of the general questions below were asked to all participants, as time allowed. Additional questions were asked based on the interviewee's background and area of expertise and the discussion in the interview.

1. Based on your experience, knowledge, and background to date, how is climate change impacting dam safety and operations? How would you expect this to change with further changes in our climate? In your perspective, what are the greatest climate change risks for dams in Canada?
2. How do you believe climate change should be considered in relation to the safety, operation, design, and maintenance of dams? (e.g. best practices, guidance, literature, standards, requirements, maintenance and operation procedures, operation management plans, asset management plans, future planned expenditure, risk assessments, financial planning, policy.)
   - 2.1 What do you believe could be the most effective method to encourage implementation of climate adaptation considerations for dams? (i.e. encourage academic and private research, support public literature, data platforms, funding programs, conferences and knowledge exchange, committees or taskforces, rules and regulations, codes, standards, guidance, by-law and laws, nothing, etc.)
3. Can you share any notable examples of climate adaptation and resilience of dams in Canada or internationally that have, in your opinion, been successful? (e.g. site-specific adaptations, organizational changes, wide-scale initiatives)
4. Have you noticed any trends or changes in the regulations, policy, operations management, design, best practices, discussions, general interest, etc. regarding dams' adaptation to climate change?
5. What are the barriers to considering climate change in relation to the safety, operation, design, and maintenance of dams? (e.g. lack of available literature, guidance, time, funding, motivation, expertise or knowledge.)
6. What are some resources that you have either come across or used to address climate risk or adaptation? (e.g. partners, tools, etc.)
7. Do you believe standards are needed to address climate adaptation for dams? If so, what would be an ideal format (standards, guidelines, regulations), and how, if at all, do you think these should be enforced?
   - 7.1. What is your perspective regarding the variation between provincial and territorial regulations across Canada and how this relates to climate change adaptation? What changes, if any, do you think would support safe implementation of climate change adaptation practices for dams in Canada?
   - 7.2. If you believe a standard is necessary, what scope (federal, provincial, organization-level) should it have?

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™