Workplace Surveillance and Remote Work

Exploring the Impacts and Implications Amidst Covid-19 in Canada

September 2021

M.J. Masoodi | Nour Abdelaal | Stephanie Tran |
Yuan Stevens | Sam Andrey | Karim Bardeesy

Ryerson University

cybersecure policy exchange
Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

This project was co-funded by the Social Sciences and Humanities Research Council and the Government of Canada's Future Skills program.

How to Cite this Report
Masoodi, M.J., Abdelaal, N., Tran, S., Stevens, Y., Andrey, S. and Bardeesy, K. (2021, September). *Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada.* Retrieved from https://www.cybersecurepolicy.ca/workplace-surveillance

Contributors
Nour Abdelaal, Policy Analyst, Cybersecure Policy Exchange
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Mohammed (Joe) Masoodi, Senior Policy Analyst, Cybersecure Policy Exchange
Stephanie Tran, Research and Policy Assistant, Cybersecure Policy Exchange
Yuan Stevens, Policy Lead, Cybersecure Policy Exchange

Our work is guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to be explained and made relevant to Canadians, and cannot be relegated to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

For more information, visit: https://www.cybersecurepolicy.ca/

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

Table of Contents

Executive Summary

Background

As the global Covid-19 pandemic swept across the world, digital technologies played a critical role in connecting employers with employees beyond the physical workplace and into employees' homes. Not only have such advancements in technology allowed employees to work remotely, but they have also enabled employers to track, monitor and analyze workers in new and innovative ways. Emerging technologies provide employers with new forms of data about workers and, as a consequence, new opportunities for worker surveillance, management and even performance evaluation.

Such developments have accelerated pre-existing trends such as the increasing quantification of activities or personal qualities of workers, expanding in breadth and depth.[1] Workplace surveillance, enabled by digital technologies, has been further intensified through the global health crisis, both at home and on-site. Indeed, crises are often used to justify the expansion of surveillance.[2] These latest developments in workplace surveillance are fraught with potential privacy and security concerns and raise questions regarding data protection, rights, power and inequities. With estimates that up to one quarter of work hours could be performed remotely even after the pandemic ends, the tension between the rights of workers and concerns of employers in ensuring a safe and productive workforce are only set to grow.

Objectives

This project extends knowledge on the growing electronic surveillance of workers, mediated through rapid developments in digital technology and further accelerated by the pandemic. This project aims to provide a better understanding of the current state of knowledge regarding workplace surveillance, including remote work surveillance, in Canada. The specific objectives of this research are to:

- Examine the current state of knowledge on electronic workplace surveillance in Canada, building on earlier workplace surveillance literature;
- Investigate the impacts and implications of workplace surveillance technologies, remotely and on-site;
- Identify knowledge gaps and implications for policies and practices that could support workers and employers in responding to the challenges of workplace surveillance; and
- Share and mobilize findings with cross-sectoral stakeholders and the public.

Results

Surveillance is generally observed in the literature as expanding, driven in large part by the growth and commercialization of information and communication technologies, and more recently, due in large part to innovations in artificial intelligence (AI) and data analytics. This project reinforces this general theme as the Covid-19 pandemic and accompanying work-from-home measures are viewed as fueling demand for workplace surveillance technologies.

Employer motivations for surveillance broadly include reducing risk and liability, protecting confidential information and assets, and encouraging productivity. The use of employee surveillance technologies amidst the pandemic has largely focused on three main functions: a) electronically tracking of employee behaviours; b) electronically measuring employee performance, often through AI-enabled technologies; and c) monitoring health data, ostensibly to help employers comply with pandemic-related regulations such as physical distancing and contact tracing.

Greater levels of perceived surveillance are correlated with higher negative attitudes toward this surveillance among employees. Monitoring tools perceived as excessive are also associated with higher employee turnover, absenteeism, weakened morale, reduced trust in management, and poorer relations between employees and employers.

There are relatively few Canadian studies of workplace surveillance overall and even fewer that examine the impact of the pandemic. Nevertheless, the gap in knowledge carries important implications for policy, practice and research. This project makes contributions by building on and extending pre-existing literature on workplace surveillance, especially as it relates to the post-Covid context. In particular, it explores new and emerging workplace surveillance technologies such as automated technologies that monitor and analyze keystrokes, eye movements, facial muscles, tone of voice and geolocation. It identifies the resulting socio-technical, legal and policy challenges and implications. And finally, it offers some promising policies and practices aimed at balancing the rights of workers and concerns of employers.

Key Messages

1. Workplace surveillance is not new, but has accelerated and expanded through new data-gathering practices enabled by digital technologies, due in part to the Covid-19 pandemic.

2. New and emerging workplace surveillance technologies, particularly those using automated decision-making, are challenging what is considered appropriate, as protected by Canada's current privacy legislation.

3. Employers need guidance to develop clear and transparent policies on the deployment and use of new and emerging digital technologies for employee surveillance, both in-person and remotely. These policies should be supported by best practices that enable the protection of employee rights, data security, equitable treatment and trust.

4. Greater enforcement measures may improve employer compliance with legal protections for employees, including the need to obtain meaningful and informed consent, and have reasonable limits on surveillance.

5. There are significant research gaps on the electronic surveillance of workers in Canada. In particular, there is a lack of literature concerning:

   - The impacts of surveillance on vulnerable and marginalized communities in Canada; and

   - The cybersecurity risks posed by digital surveillance and data collection, including risks posed to individual workers' personal and sensitive information.

Methods

This knowledge synthesis project was carried out in phases using a scoping review. This included a review of academic and grey literature, news media reports and a separate examination of legal statutes. It was guided by four research questions:

1. What is the state of knowledge on the use of current digital technologies for the surveillance of workers?;

2. What digital technologies are used to surveil workers, and in which organizations and sectors are they being used?;

3. How do Canada's laws regulate the use of such technologies for worker surveillance?; and

4. What are the impacts and implications of these technologies, particularly for marginalized and underrepresented groups?

Search and screening processes yielded 191 sources. Together, these data formed the basis of the analysis.

Background

01

Background

The monitoring of workers is not a new phenomenon.[3] Surveillance has been at the heart of capitalist work and organization.[4] Employers have consistently used methods to assess employee performance, ensure workers' compliance with employer policies, and limit distractions and inefficiencies. In the past, workplace surveillance involved visually monitoring employees during work hours, and recording work time through stamps and clocking techniques.[5] Surveys from the American Management Association examining workplace surveillance showed that monitoring tools from 1997 to 2007 largely consisted of recordings of telephone calls or voicemail, and the monitoring of email messages, computer files and internet browsing.[6] Less than 21% of the businesses surveyed at the time said they video recorded employees to assess job performance.[7] The more recent proliferation of electronic performance monitoring, conducted through tracking applications downloaded onto mobile and work devices that can be enabled remotely, has created an environment of surveillance that is more timeless, continuous and intrusive.[8]

This use of digital technologies to monitor workers has been further intensified as a result of the Covid-19 pandemic. Various levels of government in Canada enacted emergency measures that restricted gatherings and closed non-essential workplaces — accelerating a transition into remote work that spanned both the public and private sectors.[9, 10] The percentage of employees in Canada who worked any scheduled hours from home was relatively stable between 10% and 13% between 2008 and 2018, with only 4% of employees performing most of their work hours from home in 2016.[11, 12] However, by the last week of March 2020, when most emergency measures had been enacted, this proportion reached 39% — equivalent to the four in ten Canadian jobs that can plausibly be done at home.[13] By June 2021, 30% of employees still worked most of their hours from home.[14]

The swift transition to remote and virtual work will carry lasting effects on the nature of employment in Canada. Survey data from Statistics Canada show that remote work is likely to continue, with one-quarter of Canadian businesses expecting 10% or more of their employees to continue working remotely post-pandemic.[15] Several large employers, including Canadian-based Shopify, have since announced that most of their employees will indefinitely work from home post-pandemic.[16] This transition is supported by an overwhelming majority of Canadians; approximately 80% of Canadians say they prefer to spend at least half their hours working from home after the pandemic is over.[17] Statistics Canada estimates that up to one-quarter of hours worked could be remote after the pandemic ends, up from only 5% pre-pandemic.[18]

Through technological advancements, employers and management have increasingly relied on data collection as the basis for surveillance, performance evaluation and management in a context where employees were no longer subject to the direct monitoring by the employer.[19, 20, 21] Digital technologies have allowed new forms of data to be collected about workers, resulting in the quantification of employees' activities or personal qualities, and expanding the granularity, scale and tempo of data collection.[22]

Moreover, employees' ability to work from home by connecting to personal devices and networks has raised significant cybersecurity concerns. A recent survey of international technology professionals found that pandemic-induced changes in business operations pushed organizations' infrastructure onto cloud servers; yet only 20% of respondents said their security infrastructure was ready for this challenge, and 82% said they were concerned about the security risks that come from managing this remote workforce.[23] Balancing the need to meet employer interests while still protecting employees' privacy, security and safety is one of the most pressing challenges of our post-pandemic workforce.

In light of the global health pandemic, a better understanding of the state of knowledge surrounding workplace surveillance is needed, particularly as it relates to remote work. Employee monitoring and evaluation can serve legitimate interests for both employers and employees, and is a part of good management practice.[24] However, when workplace surveillance goes beyond what is reasonable and appropriate, it can negatively affect levels of trust, employee autonomy, privacy and security.[25, 26]

This study examines sources that discuss digital technologies used by employers to monitor and track workers, collectively referred to as "surveillance". This conceptualization of surveillance derives from surveillance studies, and refers to a "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[27, 28] The terms "worker" and "employee" are used interchangeably throughout, and seek to include a wide range of work arrangements in both the public and private sectors.

Objectives

02

Objectives

The objectives of this study are to provide a current state of knowledge on electronic workplace surveillance in Canada, identify the strengths and gaps in the literature, and recommend best practices and policies that could support workers and employers in responding to the new challenges of workplace and remote work surveillance. The research findings of this project will be shared with relevant stakeholders including through publications, earned and social media and other knowledge mobilization forums.

While there is considerable past research on workplace surveillance, significant gaps in a post-Covid context in Canada remain. This project aims to make contributions by identifying and critically assessing the current state of knowledge on electronic workplace surveillance in Canada, shedding light on recent developments such as remote work surveillance since the pandemic and building on earlier works on workplace surveillance.

Methods

03

Methods

This knowledge synthesis followed Arksey and O'Malley's five-stage framework for scoping reviews: 1) identifying the research questions; 2) identifying the relevant studies; 3) study selection; 4) charting the data; and 5) collating, summarizing and reporting the results.[29]

The synthesis was guided by four research questions:

1. What is the state of knowledge on the use of current digital technologies for the surveillance of workers?
2. What digital technologies are used to surveil workers, and in which organizations and sectors are they being used?
3. How do Canada's laws regulate the use of such technologies for worker surveillance?
4. What are the impacts and implications of these technologies, particularly for marginalized and underrepresented groups?

The PRISMA-ScR (Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews) checklist was used in reporting findings (see Appendix 3 for visualization of PRISMA-ScR process).

The scoping review began by searching 11 platforms and research databases, using relevant search terms related to workplace surveillance. The search strategy included social science, policy, computer and engineering databases to source both academic and grey literature. The search focused on identifying literature sources that specifically discussed the use, effects or implications of digital surveillance technologies to monitor employees or workers in various industries or organizations, including both the private and public sectors. Literature published between 2011 and 2021 was included in order to focus on recent shifts in workplace surveillance trends and themes that followed the Covid-19 pandemic, as well as the expansion of remote work. The list of databases and platforms searched, and the search terms used are identified in Appendix 1.

Scoping reviews describe existing literature and other sources of information from a range of study designs and methods, potentially resulting in a broad scope of collected information. As such, this research primarily focused on the following forms of knowledge: 1) peer-reviewed publications by experts in surveillance, digital technologies and privacy, accessed through electronic databases; 2) grey literature, including scholarly information not formally published, or peer-reviewed, on the deployment and use of digital surveillance technologies in workplaces including government documents, briefs, memoranda, white papers and technical reports; and 3) media reports, newspapers and magazines. In addition, a list of 'known' or familiar literature was compiled; however, these were not subjected to a full scoping review, and instead were used to increase understandings of the research context, speak to any gaps in findings, and help set a benchmark to determine if search strings were effectively identifying target literature.

Sources were deemed relevant and considered to be within the scope of the study if they discussed the ways in which the worker or employee was being monitored, tracked or surveilled electronically by an employer.

This excluded e-recruitment, or the use of surveillance technologies by management to screen and profile potential candidates to assess or determine their suitability before being offered employment. Sources were also required to discuss the monitoring of workers specifically as it is facilitated through the use of digital, rather than manual, approaches. Sources were excluded when employee monitoring was not the author's primary focus (such as, overly technical articles that only explain 'how' surveillance technologies generally worked without discussing workplace, social, legal or policy implications).

Jurisdictions in scope were established as Canada, the United States, New Zealand, Australia, the United Kingdom and the European Union; and only literature discussing these jurisdictions were included. These jurisdictions were selected due to their similarities with Canada, particularly with respect to surveillance trends and practices, as well as policies (for example, all countries included belong to the global surveillance and intelligence gathering alliance known as the Five Eyes). The scoping review also excluded sources that were not written in English or were not available in full text. It is important to note that Arksey and O'Malley point out that date ranges and limits on databases be used for practical reasons, and that there is always the potential to miss relevant sources.[30] All searches were conducted between April and May 2021. Separately, a scan and analysis of Canadian law relevant to workplace surveillance was compiled in Section 4.9.

Following these guidelines, studies were then subjected to a full-text review using a codebook reflective of the research objectives (see Appendix 2). During the charting process, seven primary questions were used to identify and extract key information from each source, which formed the basis of our analysis:

a. What country or jurisdiction is this source coming from or focused on?

b. Does the source mention remote or virtual work?

c. Does the source discuss surveillance technologies in the context of the Covid-19 pandemic?

d. What types of surveillance technologies were discussed?

e. What is the main objective of the source?

f. What policy/legal/social themes and implications were covered by this source?

g. What specific types of industries, organizations, or workers were impacted by the use of the employee monitoring technologies discussed?

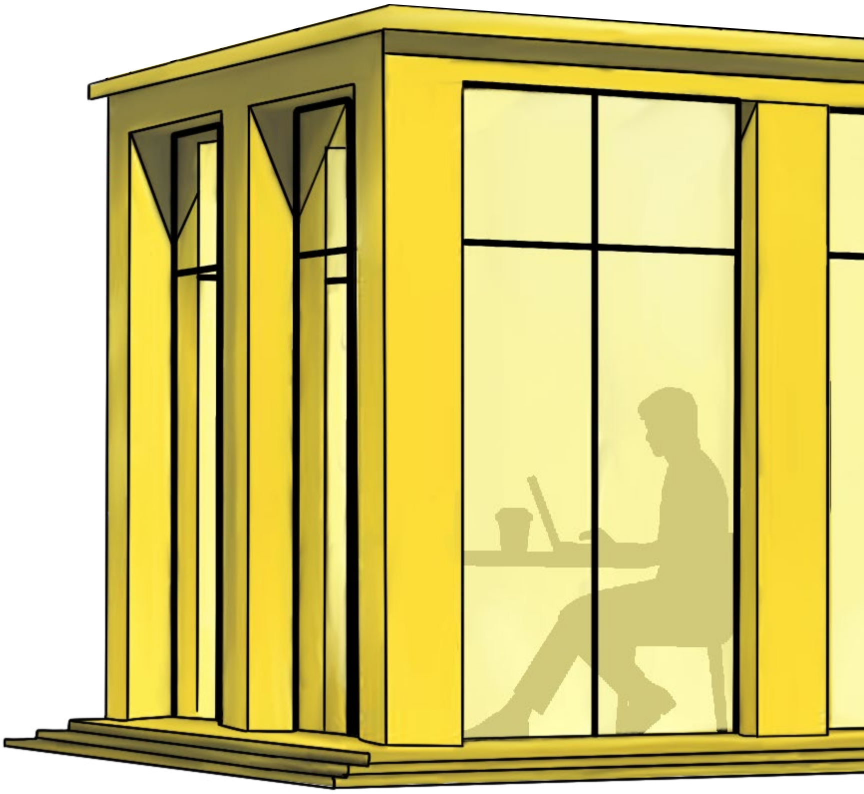
Results

04

4.1 Characteristics of Existing Literature

The literature search produced 3,835 results. An additional 107 sources were identified through other means, such as referrals from colleagues and technology experts, and Google searches. Additional screening of titles and abstracts led to the removal of 33 duplicates, while a majority were excluded (n=3,584) for content out of scope. In total, 325 articles were identified for full review. These articles were independently reviewed by two researchers for the inclusion and exclusion criteria, and were pilot-tested for inter-coder reliability prior to full review to ensure consistency and avoid discrepancy. Articles that were excluded after a full-text review included incorrect concept (n=73) (e.g., examinations of health surveillance and epidemiology, or works that failed to discuss workplace surveillance), incorrect context (n=43) (e.g., sources that fell outside in-scope jurisdictions), and those that were not available as full texts (n=18) (See Appendix 3).

After a full-text review, 191 sources were included in the scoping review and proceeded to the charting stage (see Appendix 5 for full bibliography). During the charting process, a narrative account of the key findings was established in two ways. The first provided a basic numerical analysis of the extent, distribution and nature of the studies included in the review (see Tables 1-3 and Appendix 2). Sources were also reviewed for the extent to which the studies covered the impacts of workplace surveillance on marginalized communities, and the cybersecurity implications of digital surveillance (see Section 4.2), as well as the types of workers and industries the articles discussed (see Section 4.3). This helped to shed light on the characteristics of the literature reviewed and, consequently, identify any research gaps that exist in the literature. Second, the sources were organized thematically using a descriptive-analytical method within the narrative tradition, which is reported below as stage five of the scoping review: collating, summarizing and reporting the results. As set out by Arksey and O'Malley, this method applies a common analytical framework to all the studies, collects standard information on each, provides a broader view of the phenomenon being explored, and ensures that the findings are more contextualized and understandable to readers.[31]



4.2 Strengths and Gaps of Existing Literature

The scoping review revealed several strengths and gaps in the existing literature. Importantly, the gaps point to areas that need to be considered and addressed, as well as where future research on workplace surveillance in Canada is required going forward.

Strengths of Existing Research

The literature reviewed in this project provides foundational knowledge on the psychological and sociological impacts of workplace surveillance,[32, 33, 34] with one prominent source being Ball and Margulis' examination of the established research on the topic.[35] Studies frequently assess such impacts in relation to the concept of privacy. This includes reports published by the research institute Data & Society;[36, 37] Ajunwa, Crawford and Shultz's examination of the effectiveness of U.S. law in protecting workers' privacy rights;[38] and Villeneuve and Elias' discussion on the data privacy implications of workplace surveillance technologies in Canada.[39] These studies enable a deeper understanding of workplace surveillance, taking the analysis beyond privacy — which is often conceptualized as an individual right that is weighed against the legitimate concerns of employers — and clarify the broader impacts of workplace surveillance, for example on employee-employer trust, and worker autonomy and well-being. Other studies are useful for their exploration of the effects of workplace surveillance on the individual and collective well-being of workers. Many sources included examine how employees perceive their level of privacy while under surveillance, linking overly intrusive forms of workplace surveillance to reduced productivity and increased stress.[40, 41, 42]

In addition, there is a growing body of work that utilizes empirical research methods to reveal employees' attitudes and views on workplace privacy and surveillance through surveys and interviews with workers in various positions and sectors. This includes Charbonneau and Doberstein's[43] survey of Canadian public servants; Bernd, Abu-Salma and Frik's[44] study on nannies working in the U.S., the UK, and Germany; Bakewell et al.'s[45] study on a group of field engineers in the UK; Winston, Paul and Lyer's[46] survey of American doctors and nurses; and Anteby and Chan's[47] study on workers at an American airport. Due to the highly surveilled nature of call centre work, several studies examined the impacts of surveillance in such settings.[48, 49] These studies shed further light on the tension and balancing act between worker privacy, on the one hand, and on the other hand, employer concerns used to justify monitoring practices.

In contrast to such sector-specific analysis, many sources examine workers' privacy attitudes regarding workplace surveillance more generally.[50, 51, 52, 53, 54] These studies provide a broader understanding of workplace surveillance, through analysis of overarching themes, including the importance of privacy for employees. One study reveals the risks related to overly intrusive forms of surveillance that go beyond individual privacy, such as high turn-over rates, absenteeism, low morale, and low levels of productivity — resulting in counter-productive impacts on the organization performing the excessive monitoring.[55]

Gaps within Existing Research

Lack of Studies Examining Impacts on Vulnerable and Marginalized Communities

This review demonstrates that vulnerable and marginalized communities are uniquely and significantly impacted by the prospect of workplace surveillance, yet only a small proportion of the literature analyzes the impacts of such surveillance on these populations (n=9). Two studies indicate that female study respondents tend to be more concerned about being monitored at work. Ball, Daniel and Stride's study on call centre workers found that female employees demonstrated greater concern for their privacy than their male co-workers.[56] Stark, Stanhaus and Anthony arrived at a similar finding in their study on the gendered aspects of facial recognition technology in the workplace, wherein women were significantly more likely to view workplace camera surveillance as unacceptable.[57] Other articles highlight the discriminatory implications of surveillance technologies, specifically through electronic wearables and productivity apps, introduced as part of workplace wellness programs. Richardson and Mackinnon define wearables as "a class of devices that incorporate electronics, software, and sensors on to, on top of, and around the body."[58] Examples of these devices include smart watches, fitness trackers and smart glasses which may be used to monitor and measure human activities and behaviours.[59] Work by Oravec has highlighted the biased and unequal treatment of employees through self-tracking medical devices.[60] Not only does such monitoring place undue stress on those with addictions and chronic health conditions, but they also have the "potential for 'function creep' as data collected about workers for one objective (e.g., encouraging workplace wellness) can be repurposed for other uses (e.g., employee discrimination)."[61] Anjuwa et al. also explain how wearables and productivity apps can facilitate employment discrimination, particularly against smokers, pregnant people, and those who have disabilities or who are obese.[62] Further, other studies examine the challenges for marginalized and vulnerable groups to resist surveillance. For instance, Nguyen describes how low-wage workers typically cannot afford to opt-out of invasive surveillance measures due to the high costs of withholding consent, including the potential loss of income or livelihood for not participating.[63] Under such circumstances, low-wage workers face higher pressures to consent to employers' surveillance measures.

Although these studies highlight the consequences of extensive workplace surveillance on vulnerable and marginalized groups, including their potential to perpetuate discriminatory and unequal treatment on the grounds of gender, health, age, ability and class, we found few studies within a Canadian context. Particularly missing from the results were Canadian studies that investigate new and emerging forms of workplace surveillance driven by AI and other analytics software, as well as their impacts on marginalized groups, such as foreign workers, temporary workers, youth, low-income and precarious workers, Indigenous peoples, and racialized Canadians more broadly.

Lack of Studies on Cybersecurity Implications

Few of the studies we examined discuss the cybersecurity risks and challenges introduced through workplace surveillance technologies, particularly in the context of the Covid-19 pandemic, where employers often hastily deployed remote surveillance technologies to monitor employees due to a significant shift toward working from home.

According to one study, 63% of Canadian companies reported an increase in targeted attacks since transitioning to remote work in 2020.[64] Cyberattacks directly aimed at remote-access systems, which allow outsiders to gain access to a worker's computer and virtually monitor their activities, have skyrocketed in frequency up to an estimated 768% through the course of 2020.[65] IBM Security's report revealed that the average cost of a data breach in Canada was $6.75 million per incident from May 2020 to March 2021, up from $6.35 million the year before.[66] This surge can be explained in part by the transition to remote work, with employees increasingly relying on personal unsecured networks and devices to conduct work activities.[67, 68, 69]

Cybersecurity advisories from the U.S., the UK and Australia revealed that the four most targeted security vulnerabilities in 2020 were attributed to remote work, VPNs or cloud-based technologies.[70] Moreover, data breaches cost $1 million more on average when remote work is indicated as a factor in the event.[71]

Despite the increase and severity of such attacks and their connections to remote work, there is a significant absence in the literature on the connections or impacts to workplace surveillance tools, as well as the risks, challenges and mitigations for attacks on detailed personal data. This was found to be true across all jurisdictions covered in this project, and not just in Canada.

Few Canadian Studies Overall

Most of the literature reviewed took place within a U.S. context (n=108), followed by the UK (n=50) and then Canada (n=13) (see Table 1 and Appendix 4 for full list of Canadian sources). A majority of Canadian studies were sourced from news articles and magazines. Some discussed workplace surveillance in relation to remote work and the Covid-19 pandemic, while others discussed workplace surveillance and its impacts on workers more generally. Regardless, in both cases, the increasing adoption of digital surveillance technologies was a common theme, with the pandemic serving as a catalyst for this increase in use. Further, only two results were empirical studies that assessed Canadian attitudes toward workplace surveillance technologies. Charbonneau and Doberstein conducted three surveys examining the attitudes of Canadian public servants and the Canadian public regarding the intrusiveness and reasonableness of various workplace surveillance technologies for public sector employees.[72] The second study, by Richardson and MacKinnon, involved two case studies of health and wellness self-tracking challenges for staff and faculty at McMaster University and the University of British Columbia.[73]

These studies begin to improve understanding of how some Canadian workers experience, view and deal with workplace surveillance. They nonetheless reveal a relative dearth in knowledge on the topic in the Canadian context, not least due to the limited number of empirical studies available, but also due to the types of workers and workplaces that those studies consider. Indeed, surveillance is experienced by numerous workers beyond public servants, and staff and faculty at universities — with impacts that may be felt with far greater intensity due to the precarious nature of their work. Although Charbonneau and Doberstein's study included a survey of the general Canadian public, their survey questions examined the public's views on workplace surveillance technologies for public sector employees.[74] Thus, the lack of empirical studies examining workplace surveillance in the Canadian context demonstrates a gap in the literature and an opportunity for further study, including better understanding the prevalence of different surveillance technologies and the types of workplaces using them in Canada.

Table 1: Jurisdiction Source of Literature Reviewed

Jurisdiction	% of Literature	# of Sources
U.S.	56.5%	108
UK	26.2%	50
Canada	7.3%	13
E.U.	5.2%	10
Australia	4.2%	8
New Zealand	1.1%	2

4.3 The Rise of Remote Work Surveillance

Nearly two-thirds of the literature reviewed (63.4%, n=122) specifically mentioned remote work in their discussion of workplace surveillance. Among this 63.4%, a majority of sources were news and magazine pieces (80.3%, n=98); while just 7.4% (n=9) were journal articles. Most of these articles discussing remote work took place within an American context (33.5%, n=64), followed by the UK (20.9%, n=40). A relatively smaller number of articles mentioning remote work were from Canada (5.3%, n=10).

Although remote work is not a new phenomenon — and has in fact been a common practice for workers in various industries for years prior to the pandemic — much of the literature that discusses remote work in connection to workplace surveillance was published after 2019, or the onset of the pandemic (n=120). Only two articles published between 2011 and 2019 mention remote work with reference to workplace surveillance. This suggests that the Covid-19 pandemic has prompted particular interest in examining remote work surveillance — an intersection that lacked significant attention prior to 2020 (see Table 2).

Table 2: Workplace Surveillance Literature that Mentions "Remote Work" by Year (n=122)

Year	% of Literature	# of Sources
2021	18.3%	35
2020	44.5%	85
2019	0.0%	0
2018	0.5%	1
2017	0.5%	1
2016	0.0%	0
2015	0.0%	0
2014	0.0%	0
2013	0.0%	0
2012	0.0%	0
2011	0.0%	0

A majority of the literature made reference to “remote workers” or to workers in a more general sense, without identifying any specific industry or occupation type (44.5% and 37.7%, respectively) (see Table 3). Thirteen sources mentioned Amazon workers (6.8%), and particularly Amazon warehouse and delivery staff. These articles mainly focused on the use of new and emerging surveillance technologies driven by artificial intelligence to monitor employees,[75, 76, 77] including plans to install AI surveillance cameras to watch its delivery drivers;[78] and the company’s patents for devices meant to further monitor employees, including an ultrasonic bracelet for tracking the location of warehouse workers.[79, 80]

Five articles in the review were on call-centre workers (2.6%). The highly monitored nature of this type of work makes call centres a frequently discussed area in surveillance studies literature, as employees experience frequent forms of surveillance including having their phone calls and computer activities recorded and monitored on a continuing basis by their supervisors.[81, 82, 83] An examination of healthcare workers such as nurses and other hospital staff also produced five results (2.6%). These particular workers were frequently discussed in the context of the geo-location badges that they are often mandated to wear.[84, 85, 86] These badges track the location of employees, monitoring how much time they spend with patients, which is used as a variable to measure worker efficiency. Other sources examined hospital workers’ perceptions and use of RFID devices;[87] and a case study of a California medical corporation that installed hidden cameras in break rooms.[88]

Table 3: Type of Workers in Literature (n=191)

Types of Workers	% of Literature	# of Sources
Remote workers (general)	44.5%	85
General (no specific type/industry)	37.7%	72
Amazon workers	6.8%	13
Call centre workers	2.6%	5
Healthcare workers	2.6%	5
Drivers	2.1%	4
Public servants	1.6%	3
Bank workers	1.1%	2
Walmart workers	1.1%	2

4.4 Employer Motivations for Surveillance

The following themes were identified as driving factors for employers to introduce surveillance measures aimed at monitoring workers. Employer motivations include reducing risk and liability, protecting confidential information and assets, and maintaining productivity.

Reducing Risk and Liability

Employers may surveil workers to try and minimize the risks of legal liability to third parties, or the occurrence of any harm to the organization resulting from employee misconduct.[89] As companies can be liable for abusive, offensive and otherwise harmful material that originates from the organization, employers try to protect themselves to avoid negative publicity or costly litigation claims.[90] Work monitoring can also help to reduce risk through detecting "negligent hiring and retention, security breaches, viruses and worms, hostile work environment, dangerous work conditions, and fraud and embezzlement."[91] Employers may also seek to monitor employees' electronic communications, such as emails, at times for the purposes of gathering evidence related to potential liability.[92]

Workplace surveillance technologies are also implemented as safety measures and for training purposes. Electronic monitoring through wearables, smartphones, intelligent protective clothing and other devices have been adopted by organizations to track the health and safety of employees.[93] For instance, installed in UPS delivery vans is a device that records seat belt usage and driving patterns.[94] As described in depth later on, the Covid-19 pandemic has further introduced a large number of workplace surveillance technologies, such as biosensors and wearable devices, to track compliance with regulations such as physical distancing and temperature monitoring.

Protecting Confidentiality

Another common motivation for workplace surveillance is to prevent confidential information and assets from being exposed or misused. It is in the organization's interest to prevent the disclosure of sensitive information, including trade secrets, intellectual property and the personal information of employees and clients, to competitors or third parties.[95] Confidential information can be leaked intentionally or accidentally by employees, such as through phishing attacks, weak passwords and insecure devices.[96] As sensitive company information can be transmitted or exposed through such channels as email and phone calls, organizations can feel motivated to monitor these communications to ensure that confidential information does not leak to competitors or the public.

Improving Productivity

Ensuring that employees are working effectively and productively is another reason for adopting worker surveillance technologies. McParland and Connolly's literature review on workplace surveillance found that improving "work rate and productivity" was a common motivator for workplace monitoring.[97] In a 2020 survey by monitoring software provider, ActivTrak, small and medium-sized businesses ranked productivity as their top concern with remote work.[98] This concern helps explain the large-scale adoption of productivity monitoring software by organizations that have shifted toward remote work.

Work monitoring software is argued to promote productivity by preventing distractions, and producing business intelligence that employers can use to improve work processes. Surveillance software can "track deviant behaviour," monitoring employees to check for non-productive uses of computer systems during work hours (also referred to as "cyberloafing").[99] In addition to acting as an incentive for employees to avoid distractions, monitoring software is also marketed to employers as a productivity-improving measure, claiming to allow them to learn "how employees work best" through compiled data that depict employees' most productive periods, or which combination of people may produce the most work together, and "what tools employees need."[100]

In addition, with the rapid growth of gig and digital labour platforms, such as delivery services, surveillance technologies and associated performance scores have become a central part of both their business models and workers' evaluations. Accessing such performance metrics and ensuring their accuracy requires that the service application monitor the worker's location, punctuality, and number of tasks completed or clients served. The data being collected has expanded not just the breadth of performance information available to employers, but is used to affect the economic returns of the workers by managing workers on the margins, so that only those most responsive to the surveillance are rewarded.[101]

4.5 Growing Trend of Digital Performance Analysis

A major trend in the literature was a growing use of digital technologies to assess employee performance. In one pre-pandemic study conducted in 2019, 66% of U.S. companies said they monitor their employee's internet use, 45% track keystrokes and time spent at the keyboard, and 43% store and review computer files.[102] Moreover, more than six in ten senior executives said they are using new technologies to collect data on their employees to gain more insights about the quality of their work, the way people collaborate, and their well-being.[103] The so-called 'productivity software industry' has been steadily growing since 2015 and is expected to hit an estimated US$38 billion in value by 2027.[104] Through their use of AI and other analytics software, these technologies not only monitor but also increasingly have the capability and capacity to analyze and assess the work performance of employees. Assessments or decisions made by software based on collected employee data, many of which can be intertwined with employee personal information, is a growing industry. The market for such technology was estimated to be worth $1.1 billion in 2018 and is expected to grow to $3.3 billion by 2023.[105]

Some of the largest global companies have reportedly used employee surveillance software prior to the pandemic. A survey of 239 large companies conducted by Garner in 2018 revealed that more than half were using "some type of non-traditional monitoring techniques."[106] Among these techniques is the use of InterGuard which enables employers to record employees' "email, social media, instant-message, keystroke, internet, geolocation, file and printing activity" through intelligent search and comparative analytics that can rank employee performance and send alerts regarding unusual behaviour patterns.[107] In recent years, surveillance technologies have also extended to the monitoring of social media networking sites, where monitoring tools are able to detect the social media sites that employees use and uncover their user profiles.[108]

The use of employee surveillance technology is widespread and spans across a variety of industries. Customers of the employee monitoring company Hubstaff — a software that enables employers to track workers' hours, mouse movement, keystrokes and websites visited — reportedly include Instacart, Groupon, and Ring.[109] Reporting from the Electronic Frontier Foundation (EFF) also revealed that the employee monitoring tool Time Doctor claims it has over 83,000 users, including high-profile customers such as Allstate, Ericsson, Verizon and Re/Max.[110] Moreover, the EFF states that StaffCop and Teramind claim that their employee monitoring software is used among clients in industries including "healthcare, banking, fashion, manufacturing and call centres."[111] Other surveillance software companies that have offered similar computer surveillance technologies in recent years include Avaza, VeriClock, Boomr, DeskTime Pro, TrackView, Toggl, Activity Monitor, WorkTime Corporate, Bergun and Wiretap.[112, 113] Indeed, the reviewed literature demonstrates that the employee surveillance monitoring industry is active and growing.

However, the increasing use of such employee monitoring technologies has not been without controversy. The UK-based bank Barclays is being investigated by the UK Information Commissioner's Office for allegedly installing a heat and motion tracking device beneath employees' desks called OccupEye in 2017, to track if traders and bankers were sitting and working or away from their desk.[114] Amazon's use of similar employee monitoring technologies has notably been introduced as a means to manage and control perhaps their most vulnerable workers in warehouses and factories, even prior to the pandemic.[115] In addition to the security cameras that track every detail of Amazon workers' behaviour, item scanners are used to record how many seconds it takes an employee to complete a task (such as retrieve a package), issuing warnings and terminations if an employee takes too long or falls short of a specific productivity rate.[116, 117] Amazon also uses a navigation software called the Rabbit or Dora to track delivery driver routes and location.[118] Call centres reportedly record a large amount of information on workers, including the number of phone calls taken, the length of phone calls, recordings of the calls, and even length of washroom breaks.[119, 120]

Some companies have even experimented with such technologies to track the social interactions between employees, such as how employees talk with one another, and for how long, by using microphones, location sensors, and accelerometers.[121] The Bank of America reportedly used employee ID badges in 2015 to record how employees interact at the cafeteria and during work hours.[122] In 2018, Walmart was reportedly interested in acquiring a new software system called "Listening to the Frontend", which would enable the company to use sound sensors to record the conversations of store staff and customers, as well as other noises such as scanner beeps and bag movements.[123]

4.6 Covid-19 and Accelerated Remote Work Surveillance

The pandemic has accelerated remote work, and in tandem, remote work surveillance. This acceleration has been fueled by employer demands relying on new and pre-existing technologies to ensure that workers are not circumventing responsibilities or failing to meet productivity targets. During the onset of the pandemic, many employers and organizations hastily procured remote surveillance technologies, with news reports describing the moves as "panic-buying."[124] For example, Hubstaff said the number of its UK customers increased four times since 2020.[125] In addition, Sneek, which provides group video conference software that is always on by default, also reported a five-fold increase in the number of users during the first lockdown, reaching almost 20,000 users in total.[126] According to the EFF, surveillance companies are using the pandemic, and the management difficulties associated with remote work, to pitch their monitoring tools, applications, and services to employers.[127]

A survey of over 2,000 companies in the UK indicates that by December 2020, one in five businesses had begun using technology that tracks worker's online activity.[128, 129] Prodoscore, an employee monitoring software company that uses analytics to produce productivity scores for workers saw a 600% increase in interest from prospective clients from March to June 2020.[130, 131] Employee monitoring software TransparentBusiness also saw a 500% spike in users month-to-month during the same period.[132] In Canada, Hubstaff claims to have signed up to 550 Canadian firms for a free trial of its employee monitoring software during the same period, while 79 had already made purchases.[133]

Research suggests that many believe remote work during the pandemic is more than a temporary shift, while analysts predict that the related increase in remote work surveillance technologies is here to stay. Eight out of ten of the most in-demand employee surveillance software companies incentivize and promote "long-term use" of their technologies to their clients.[134] Further, according to analysis by the internet security and digital rights firm Top10VPN, "global demand for employee monitoring software increased by 87% in April 2020" compared to the monthly pre-pandemic average.[135] This surge in demand was sustained throughout the year as demand for monitoring technology remained 51% higher than pre-pandemic levels from June to September 2020.[136] Moreover, the surveillance company Gartner found that "16% of employers were using technologies more frequently to monitor [remote] employees through methods such as virtual clocking in and out, tracking work computer usage, and monitoring employee emails or internal communications."[137] The top three most popular tools are Time Doctor, Hubstaff, and FlexiSPY, which account for almost 60% of global demand in surveillance software, according to Top10VPN.[138]

4.7 New Surveillance Technologies to Oversee the 'Overseen'

In the context of work during the pandemic, the use of new and emerging employee surveillance technologies largely focused on three main: 1) electronically tracking employee behaviours; 2) electronically measuring employee performance by quantifying work in terms of 'productivity scores'; and 3) monitoring health data, purportedly to help companies comply with Covid-related regulations such as social distancing and effective contact tracing.

Electronic Tracking of Behaviours

The majority of workplace surveillance technologies are intended to track employees' behaviours as a means to ensure that employer policies and goals are met and to avoid work distractions. Performance monitoring software collects data on the activities performed by the worker, as well as the environment in which they operate. Recording information on workers' activities can require software or hardware that directly monitors communications (such as email, text, calls, work messaging software, etc.), keystrokes, search engine browsing, and 'idle' time. Collecting data on the environment of the worker can require employers to rely on webcam surveillance software, CCTV or sound recording devices, and location tracking through GPS or AI-enabled cameras.

Webcam Surveillance

Following the onset of the Covid-19 pandemic, a video conference call software called Sneek gained traction as companies pivoted to remote work settings.[139] As briefly described earlier, Sneek takes a picture of employees every one to five minutes through a front-facing laptop webcam.[140] The pictures are combined to create a "wall of faces" featuring employees as they work that is available for everyone to view throughout the workday.[141] The talent management company Crossover also installed a productivity tool called WorkSmart that takes photos of remote employees and their workstations every 10 minutes through their webcam.[142]

Teleperformance, one of the world's largest call centre companies with more than 380,000 employees globally, rescinded their decision to require its UK-based employees to keep their webcams turned on if they are working remotely as a result of the pandemic.[143] The company said the "installation of video surveillance tools would be voluntary" after it had informed employees that they would be required to use AI-enabled webcams to track real-time work for "data security reasons."[144] The webcams would have also reportedly been used to scan for potential work violations, and take screenshots of potential infractions to send directly to the employee's manager.[145] However, Teleperformance is still expected to use this tracking software in more than 30 other countries where labour laws allow this kind of surveillance.[146]

San Francisco technology start-up Pragli also developed remote work software that allows employees to create a "digital avatar" and work in a "virtual 'office' setup with chat room cubicles" that require workers to keep their webcams and microphones on at all times to enable spontaneous chats.[147] Numerous other pieces of software, such as Time Doctor, Hubstaff, and RemoteDesk, also use webcams to continuously take pictures of employees.

Desktop and Keyboard Activity Monitoring

Most surveillance software employs a range of desktop and keyboard activity monitoring. According to one study, 81% of the most popular employee monitoring tools offer keystroke logging so that employers can see employees' every click on the keyboard; 61%

provide instant messaging monitoring; 65% can send 'user action alerts' to the employer (such as when a user's keyboard has been idle for a long time); and 38% are able to remotely control the worker's screen to block access to websites or install software.[148] Keystroke logging can be particularly problematic if surveillance tools can capture passwords typed by the employee — an ability that the monitoring program Work Examiner boasts its software is able to do.[149] Other monitoring tools can measure distraction by tracking the extent to which an employee is "switching between applications."[150]

Moreover, Teramind's surveillance technology can monitor private conversations and detect if a "pre-selected keyword" that is deemed "inappropriate" by the software is used, triggering an alert to the employer and disabling the conversation.[151] Hubstaff, one of the most popular employee surveillance tools, also monitors screen time, mouse activity, tasks completed, and hours working in real time.[152] Veriato also captures videos of screen activities conducted by the employee to send to the employer; and Work Examiner allows the employer to fully view the employee's "internet usage and block distracting content."[153] Reporting from The Guardian also notes that Wiretap can monitor "workplace chat forums such as Slack and Yammer to identify intentional and unintentional harassment, threats, and intimidation", and alert employers of concerns.[154]

Facial Recognition and AI-Enabled Technologies

The technology company Fujitsu developed a facial recognition software program that purports to detect the focus of employees and remote workers.[155] The AI-powered tool analyzes changes in facial muscle movements every few seconds to assess the employee's level of focus, and cross-references this data with the user's past muscle behaviour and the attention requirements of the specific task conducted.[156] Moreover, one of the most controversial developments in employee surveillance following the pandemic was accounting firm PwC's deployment of a facial recognition tool that records and analyzes how long employees remain in front of their computer screens.[157] The tool requires PwC employees to provide "a written reason for any absences, including toilet breaks."[158]

A still unnamed "meeting insight computing system" technology developed by Microsoft is also planned, to allow employers to "read a room" during remote meetings and video calls, including analyzing facial movements and body language like eye rolls, to score the quality of a meeting.[159] In addition, a new device from Amazon called Halo is a wristband software that can keep track of a user's mood and tone of voice by using machine-learning algorithms to analyze the user's voice through its embedded microphone.[160] The band can provide the user with in-depth feedback such as "'you're sounding too tense' or 'you're being too assertive'."[161] The Amazon band has not been used in workplaces in a systematic manner; however, concerns have arisen over its potential implications on the workplace.[162] Aware's Spotlight software conducts "AI-driven behavioural analysis" to track changes in employees' "mood, tone, and attitude" during conversations taking place on the user's devices.[163] Not only does AI-enabled software analyze employee behaviour, but industries requiring relatively greater security have also used AI and biometric authentication to ensure only cleared employees can access work-related sensitive information from home.[164]

GPS and Location Monitoring

A number of employee monitoring tools can track the location of employees in real time, particularly in industries that require the physical movement of workers, such as delivery services or warehouse operations. For example, legislation in the United States requires that all U.S. truck drivers attach an electronic logging device to their vehicle — software that monitors "speed, location, and driving schedules" to report that data "back to an employer or third-party monitoring service."[165] Long-haul truckers have protested the implementation of these devices because they can restructure the times and routes they drive in ways they say may not be safe or efficient.[166] Moreover, many delivery and truck workers also use their vehicles to conduct personal affairs, and monitoring technology may not be able to accurately distinguish on-the-job movements from personal use.[167]

Location tracking is significantly used in essential work industries. The Massachusetts State Police is also planning to introduce geolocalization technology in its 2,900 vehicles to track how and where officers move during shifts.[168] Nurses are also increasingly instructed to wear geo-location badges and other hardware to help track where they are located in the hospital.[169] Other monitoring software can also track the movement of office staff via GPS on their phones or work-provided devices.[170]

Electronic Measurements of Performance

A number of surveillance tools provide employers with real-time analytics, delivering an amalgamated 'productivity score' that evaluates the employee's quality of work, comparing the results across workers using many of the same behaviour monitoring techniques. For example, WorkSmart uses a combination of screenshots of workstations, application use and keystrokes to provide a "focus" and "intensity" score to measure the degree and extent of each employee's work habits.[171] According to Crossover, the company developing WorkSmart, 'intensity' scores assess the employee's "ability to focus on one activity at a time" rather than constantly changing between activities; while 'focus' scores analyze the employee's keystrokes and mouse clicks to determine how intensely and efficiently the employee is working.[172]

ActivTrak also collects and reports on a variety of data through automated screenshots of workers' screens to provide employers with a "data-backed overview of employee performance", allowing managers to identify inefficiencies in the work process.[173] The employee's productivity scores can be viewed by both managers and other team members, and the tool's "team pulse" feature "provides a daily summary of which team members are most productive" to increase motivation among workers.[174] In addition, Prodoscore monitors a wide range of tasks undertaken by an employee, including checking emails, work documents and, calendar appointments, and transcribes phone calls on internet-based phone services.[175] The software then uses these data points to provide managers with "a score on a productivity scale."[176] Similarly, Isaak software tracks employee interactions to analyze each person's collaboration level, and incorporates this information with individual user data to identify "change-makers" in the company.[177]

In the last two years, there have been a number of instances of major technology platforms backtracking on productivity measures following public or employee concerns and advocacy for technology in the public interest. For example, Microsoft's Productivity Score provides employers with "insights" into employees' productivity behaviours, including categorizing information on workers' use of Microsoft software. The software tracks data on the number of days spent reading emails, chatting, collaborating on shared documents, or using mentions in communications.[178] Individuals' scores are "allocated based on categories such as 'Communication', 'Meetings', 'Content', and 'Teamwork'," and points are amalgamated into an overall score for the employee.[179] Comparing scores between employees would have allowed employers to identify gaps in specific employees's performance, and motivate underperformers to better meet productivity targets. But after facing controversy,[180] Microsoft removed the program's ability to display specific usernames associated with the scores.[181] The company said the program will transition to providing IT specialists with information on user uptake and use of Microsoft's suite of products.[182] However, administrators of the program may have special privileges to view individual user behavior if the employee has not opted-out from having their data reviewed by the software.[183]

An attention tracking feature on Zoom, first introduced in early 2020, alerted meeting hosts when participants did not have the Zoom meeting screen active and open for more than 30 seconds while someone was sharing their screen.[184] While users could disable this feature from their account settings, the meeting organizer could also make this feature mandatory for all participants if they wish.[185] Zoom removed this feature in April 2020 following backlash and concerns over privacy and misuse.[186] Additionally, essential workers facing workplace surveillance have fought against the "electronic whip" software, which presents employees' productivity scores onto a "leader board" to encourage underperforming employees to increase their speed.[187]

Health Monitoring

Following the pandemic, a growing number of employee surveillance technologies have been adopted to track workers' health to ensure compliance with Covid-19 regulations including physical distancing and temperature monitoring. Employers have become more interested in using telehealth technologies to continuously monitor employee symptoms and prevent Covid-19 outbreaks. One such technology that has received increased interest from corporations is LifeSignal, a "thin, disposable skin patch that uses an integrated biosensor" to monitor a range of vital signs, including users' "respiration rate, skin temperature, blood pressure, posture and even electrocardiography (ECG)."[188] The health monitoring company is now working with eight organizations to launch corporate health tracking programs where data from the patch will be transmitted to an app on employees' phones and the company's occupational-health department.[189] Employers are also increasingly asking employees to disclose their personal medical and health information, including experienced symptoms, pre-existing conditions, and risk of exposure to the virus through self-assessment applications.[190]

Many workplaces, particularly those of essential businesses and vulnerable groups such as nursing homes and grocery stores, began tracking workers' body temperatures at the start of their shifts using basic thermometers or more sophisticated heat sensors.[191] Feevr is a "thermal imaging device" that allows employers to check workers' temperatures quickly before they enter the workplace, preventing long lines of employees waiting to enter buildings.[192] Employees can also log into the Feevr application at home through a "facial scan," take their temperature using a "digital thermometer," and send the data to their employer to receive permission to enter the workplace.[193]

New health tracking tools to track employees' location and social distancing behaviour also emerged following the pandemic. Amazon developed a Distance Assistant software that uses "machine learning in warehouse cameras" to "identify high traffic areas and encourage better distancing."[194] As workers move around the warehouse, the camera positively detects employees maintaining six-feet distance with a green circle and negatively detects employees standing too close with a red circle.[195] In the same vein, Ford Motor Company developed a wrist watch that can tell employees if they are complying with the six-feet distance measure;[196] and consulting firm PwC also created a phone application that traces employees' contacts by analyzing their interactions in the office.[197] In one application, employers would track workers' location and movement through their smartphone, earning higher scores the more times a user maintains six-feet distancing and aggregating total scores for employers to review.[198]

Efficient contact tracing has also been a significant impetus for adopting greater monitoring tools in the workplace. Contact tracing tools also come in the form of wearable devices. Some health tracking software is marketed as workplace safety wearables that can track users' health status and provide insights on the effectiveness of social distancing measures.[199] Similarly, PwC offers an application called Check-In that uses GPS location tracking, Wi-Fi and Bluetooth capabilities to keep track of workers who have been in close contact with positive cases, and determine where and when "workers are on the company's premises."[200]

4.8 Employee Perceptions and Reactions to Surveillance

Various factors have been identified in the literature as shaping how employees react to surveillance; namely, workers' perceived degree of surveillance, a sense of control over information shared with employers, and clarity of the purposes surrounding such monitoring. Worker reactions to surveillance can involve acts of individual resistance, which must be considered in light of the power imbalances between employers and employees, and in the context of labour relations.

Perceived Degree of Surveillance

Multiple empirical studies have found that workers with greater levels of perceived surveillance at work tend to harbour more negative attitudes toward the surveillance systems.[201, 202, 203] Workplace surveillance measures that are perceived to be excessive have been shown to lead to higher employee turnover and absenteeism, weakened morale, reduced trust in management, and poorer relations between employees and employers.[204] In one study, Martin, Wellen and Grimmer surveyed employed Australians to test the relationship between the perceived level of surveillance at work and counterproductive work behaviours (CWB), wherein employees work at less than full effort and/or subvert their managers.[205] The researchers found that "higher levels of perceived surveillance were associated with more CWB," and that "this relationship was mediated by attitudes towards surveillance."[206] In other words, this study suggests that when workers believe that they are under a high degree of electronic surveillance, and when these workers view workplace surveillance as invasive and as an indication of the employer's lack of employee trust, they are more likely to engage in deviant work behaviours.

The extent to which workplace surveillance impedes on the privacy of workers has also been found to play a role in workers' perceptions and reactive behaviours to monitoring measures. Chory, Vela and Avtgis studied American employees from across occupations and organizations to examine employee concerns regarding the monitoring of electronic communications at work.[207] Their study found that full-time working adults who perceive less computer privacy in their workplace view the organization's policies as less fair, hold less trust in upper management, and demonstrate less commitment to their organizations. Moreover, the study found that employees' perceived degree of procedural justice (in terms of the organization's ability to fairly respond to concerns and complaints) mediated the relationship between employees' feelings of trust and commitment toward the organization and their perception of privacy.[208]

Employee Control

How employees interpret their level of control over surveillance has been identified as a key contributor to their reactions to surveillance measures.[209] The study by Chory, Vela and Avtgis also indicates that when workers feel that they lack control over the information that is accessible to their employers through monitoring, they are also more likely to view work procedures as unfair, with subsequent decreased feelings of trust and security in their relationship with their employer.[210] In their review of psychological and sociological research on employee surveillance, Ball and Margulis discuss the body of work that demonstrates the relationship between employee control and stress, with the common finding that workers' lack of control over the monitoring process is associated with higher levels of stress.[211] The authors concluded that "worker control over monitoring, whether officially or unofficially sanctioned, can mitigate stress levels."[212]

Clarity of Purpose

Research has shown that employee perceptions about the rationale for work surveillance systems play a major role in how they react to such measures. When workers do not see a clear work purpose for monitoring technologies, they are likely to view the surveillance measures negatively.[213] In their study on Canadian public servant attitudes on workplace surveillance technologies, Charbonneau and Doberstein found a "very strong correlation between one's sense of the intrusiveness of a technology and their views of its reasonableness for use in a public sector work environment."[214] The surveillance technologies that were commonly identified as "very unreasonable" lacked a clear association between the technology and its purpose for measuring workplace performance or productivity. Technologies that were viewed as "very unreasonable" tended to capture physical activity, such as non-visible cameras, personal devices that record audio, video and location of the wearer (e.g., tracking badges by the company Humanyze), and body heat measurement devices (e.g., those provided by OccupEye). Computer software surveillance methods such as keylogging, internet usage recording and AI email analysis were viewed as less intrusive, which the authors argued is due to the clearer relationship that these technologies have with performance monitoring.

Individual Resistance

Research from the field of psychology suggests that employees with more negative attitudes toward workplace surveillance are more likely to resist complying with it.[215] According to one survey done by a UK human resources firm, 70% of respondents believed that the level of trust between themselves and their bosses would likely diminish from the adoption of monitoring software.[216] Studies have also continually emphasized the significance of trust between employers and employees, as "employees' actions, behaviours and willingness to disclose certain information can be significantly impacted if there is no trust in the relationship," with potential employee retaliation such as engaging in deviant behaviours."[217] As such, workers with eroded levels of trust in their employers may engage in resistance against surveillance through evasion or deception. Acts of evasion, or "invisibility practices,"[218] allow workers to hide from their employer's gaze. This could be done physically through, for example, going to areas exempt from CCTV-patrol or changing out of uniform during breaks to prevent scrutiny from supervisors and customers.[219] One digital invisibility practice would be avoiding online spaces where one's employer can view worker activity and data, for example, the use of an app other than the Uber app as a driver for navigation. Deceiving work surveillance systems can also be accomplished using software to mimic computer activity in order to appear more productive. One such program called Move Mouse, which automates the movement of a computer's mouse, saw a large rise in downloads during the shift toward remote work.[220]

Power Imbalances and Labour Relations

The power imbalance between employers and their employees complicates the concept of worker consent, in turn facilitating the introduction of workplace surveillance technologies. Workers may agree to surveillance measures in order to avoid potential consequences that a refusal may bring, such as retaliation or joblessness.[221] This is evident in Bernd, Abu-Salma and Frik's study on how nannies in the UK, Germany and the U.S. interpret their experiences working under camera surveillance installed and monitored by the families that employ them.[222] Participants commonly shared that they felt they were not in a position to express privacy concerns due to the power dynamics with the parents who employed them.[223] With regards to the pressures placed upon workers to accept surveillance, digital rights groups Data & Society and the Electronic Frontier Foundation have expressed that "a choice between invasive and excessive monitoring and joblessness is not really a choice at all,"[224] in turn "making consent seem almost meaningless."[225]

Employers' power over their workers can also be compounded by workplace surveillance technologies. Nguyen describes how the extensive and continuous collection of data creates "massive challenges for any employee to fully comprehend the scale of the data collected about them."[226] This asymmetry of information between managers and workers may put employers "in a privileged negotiating position, facing workers with reduced bargaining power."[227]

There is also the concern that workplace surveillance may impede on workers' union organizing efforts. Surveillance technologies constrict workers' ability to organize collective action as their communications are at risk of being monitored by their employers. Although organizations may adopt surveillance measures for reasons unrelated to deterring union organizing, the presence of these systems can nonetheless have a chilling effect on union activity.[228] On top of inadvertently impending collective action, organizations may also purposely engage in surveillance to stifle labour organizing. Amazon's monitoring of its employees' union-organizing efforts drew criticism from two U.S. senators in September 2020,[229] when it came to light that Amazon corporate employees were regularly monitoring the social media activity of its drivers to identify and track labour organizing.[230]

Contractually obligated to comply with employer policies, workers typically lack the power to reject installing and using monitoring software.[231] One method for protecting workers in this domain is to include clauses in collective agreements concerning electronic monitoring, as discussed by Hooper, Anderson and Blumenfeld from New Zealand.[232] Despite this option, the authors found that only 5% of collective agreements in the country mentioned electronic monitoring in June 2019.

4.9 Canadian Legal Framework Addressing Workplace Surveillance

When it comes to employees' privacy rights with respect to workplace surveillance, there is a patchwork set of laws that apply in Canada. These regulations are addressed in Canada's international law, the *Charter of Rights and Freedoms* and, the *Criminal Code of Canada*, as well as various federal and provincial privacy and labour laws.

International Law

Canada is a signatory to a number of international agreements that include provisions regarding the protection of privacy rights. Article 17 of the *International Covenant on Civil and Political Rights* protects individuals from "arbitrary or unlawful interference with [their] privacy, family, home or correspondence."[233] *The American Declaration of the Rights and Duties of Man* also protects individuals from abusive attacks on one's private and family life, as well as one's right to the inviolability of his home and transmission of his correspondence.[234]

Canadian Charter of Rights and Freedoms

The *Canadian Charter of Rights and Freedoms* contains provisions applicable to employee privacy in the context of workplace surveillance. Privacy is a constitutional right by virtue of sections 7 and 8 of the *Charter*,[235] which respectively protect the right to "life, liberty and security of the person",[236] as well as the right "to be secure against unreasonable search or seizure."[237] The Supreme Court has also recognized that privacy is an essential component of individual freedom, with the

Charter serving as a restraint "imposed on government to pry into the lives of the citizen go to the essence of a democratic state."[238]

While the *Charter* does not bind private actors,[239] court decisions have been considerably impacted by *Charter* values in cases involving disputes over electronic surveillance in private workplaces.[240] The Supreme Court has recognized three spheres of privacy: spatial, physical and informational.[241] Spatial privacy relates to an individual's home, which is an area of case law particularly relevant to the surge in surveillance over work-from-home employees.[242] The physical sphere refers to an individual's body; and the informational relates to the ability of a person to control what information about oneself is revealed to whom and when.[243]

Other case law involving the *Charter* also reaffirms a general expectation of privacy for the worker. In 2010, the Supreme Court ruled that individuals have a reasonable expectation of privacy in the informational content of their personal computers.[244] Then in 2012, the Supreme Court held that the right to privacy extends to information related to work-issued computers, which may be diminished dependent on the totality of the circumstances in question, including workplace policies such as whether employees were previously aware of potential monitoring on work devices.[245] However, the police must still obtain a warrant for the search and seizure of information with respect to work-issued devices, even if the information in question was lawfully obtained by the employer.[246]

Criminal Code

The *Criminal Code of Canada* also outlines relevant provisions related to employees' right to privacy in the workplace. Section 184 of the *Criminal Code* holds that the willful interception of private communication by any device is an offence, where "intercept" refers to "the listen[ing], record[ing], or acquir[ing] [of] a communication", and "private communication" refers to any oral or telecommunication in which it is "reasonable for the originator to expect that it will not be intercepted by any person" other than its intended recipient.[247] Section 342 of the *Criminal Code* also prohibits the direct or indirect interception of any computer service done fraudulently or without right, which can include the monitoring of electronic information such as email.[248]

However, the prohibition on communication interception does not apply when consent (express or implied) is obtained,[249] provided that the consent is freely given by the originator of the communication without coercion.[250] The prohibition also does not apply to a person providing a communication service to the public if the interception is, in part, conducted as part of random monitoring for quality control checks[251] — an area of business operation where employers could potentially collect employee information for quality monitoring purposes without consent. For example, in one case in Quebec, the court found that the employer's decision to record telephone conversations of the employee was not a breach of Section 184(1) of the *Code* because the employer intended to check the quality of the employee's work as allowed under the *Code*'s exceptions.[252]

Federal Privacy and Data Protection Laws

Privacy Act

The federal *Privacy Act* regulates the collection of personal information by federal government institutions.[253] Section 4 of the *Privacy Act* limits the collection of information to that which "relates directly to an operating program or activity of the institution."[254] The legislation also requires that federal government institutions inform individuals of the purpose for which the information is being collected.[255] However, these requirements are exempted if obtaining consent results in the collection of inaccurate information or defeats the purpose for which the information is being collected.[256] Individuals also do not have the right to know or provide consent over the collection, use or disclosure of their information.[257] Section 8(2)(a) of the *Privacy Act* allows federal government institutions to disclose personal information when doing so would be for a use "consistent" with the original purpose for which it was collected.[258]

Directive on Automated Decision-Making

The federal government's *Directive on Automated Decision-Making* was enacted in 2019 to establish administrative law principles that regulate the government's use of artificial intelligence in administrative decisions.[259] The *Directive* requires federal programs using an Automated Decision System developed or procured after April 2020 to complete and publicly release an Algorithmic Impact Assessment (AIA) prior to the deployment of the system, to identify risks, mitigate harms and ensure procedural fairness.[260] The AIA evaluates the program's impact level by analyzing the system's design, algorithm process, decision type, the sensitivity of the data to be collected, and measures to safeguard personal information.[261]

Pursuant to the *Directive*, federal departments are also required to provide notice to impacted individuals of the automated system, and provide meaningful explanations of how and why automated decisions were made, as well as publicly release information on the system's effectiveness and efficiency in meeting program objectives.[262] Final decisions also must be made by a human if the decision is likely to have high impacts on the rights, well-being or economic interests of individuals. However, the *Directive* only applies to services where the intended client is external to the federal government and therefore is unlikely to be required in most instances of automated workplace surveillance tools used by federal employers. Likewise, a similar framework to guide private sector organizations' use of automated decision-making software — such as AI-enabled employee surveillance technologies — is not present in Canada.

Directive on Privacy Impact Assessments

The *Directive on Privacy Impact Assessment* (PIA) also provides guidance to federal institutions on how to assess the privacy impacts of programs involving the collection and use of personal information.[263] According to the *Directive*, a PIA is required for any new or substantially modified activity or program where personal information is used for decision-making processes or an administrative purpose.[264] PIAs are also required if transferring program activities to another level of government or the private sector will substantially modify the program, including its use of personal information.[265]

The *Directive* provides that PIAs should include a description of the planned program, its objectives, assessment of privacy compliance, evaluation of potential impacts on individuals' privacy, and the mitigating measures implemented to ensure compliance with privacy provisions.[266] Organizations are encouraged to conduct PIAs during early stages of program development, consult with stakeholders within and outside the organization, and make results publicly available.[267] In its landmark June 2021 investigation, the OPC found that the Royal Canadian Mounted Police's use of facial recognition technology contravened *Privacy Act* provisions.[268] The OPC's investigation highlighted that the RCMP failed to properly assess privacy risks, and recommended the integration of PIAs prior to deploying facial recognition technology.[269]

Personal Information Protection and Electronic Documents Act

The privacy right of many employees is protected privacy under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal law that governs the collection, use or disclosure of personal information related to the private sector's commercial activities or a "federal work, undertaking or business" within the legislative authority of Parliament (e.g., telecommunications, banking, transportation).[270] PIPEDA does not apply to non-profits, charities, associations or political parties unless they are engaging in commercial activities.[271] PIPEDA applies when personal information is transferred across borders within or outside Canada. It also applies to the private sector in all provinces except Alberta, British Columbia and Quebec, which have their own private sector privacy laws that are deemed sufficiently similar to PIPEDA.[272]

Three main components of PIPEDA can relate to the collection of personal information as a result of employee surveillance:

1. **Appropriate purposes:** Employers subject to the law may "collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[273] This standard seeks to ensure that the surveillance taking place must clearly meet appropriate purposes that are identified by the employer before or at the time of collection.[274] The Office of the Privacy Commissioner (OPC) of Canada states on its website that it does not generally consider surveillance of an individual using their own device's audio or video functions to be appropriate by a reasonable person.[275]

2. **Individual access and challenge:** Employees generally have the right to be informed of the existence, use and disclosure of their personal information upon request; to be given access to that information; to be able to challenge the accuracy and completeness of the information; and to have it amended as appropriate.[276]

3. **Knowledge and consent requirements:** Knowledge and consent of the individual are also generally required for the collection, use or disclosure of personal information.[277] Employers are encouraged to be honest about the reasons they are collecting personal information without

being misleading or deceptive.[278] Employers are also encouraged to seek express consent when:

a. The collection involves sensitive information; or
b. The personal information obtained is "outside the reasonable expectations of the individual"; or
c. The collection of personal information creates "a meaningful residual risk of significant harm."[279]

However, there are numerous exceptions to PIPEDA's consent requirements. Consent for the collection of personal information is not required when it cannot be obtained in a timely manner and the collection "is clearly in the interests of the individual."[280] Moreover, consent is not needed when it is reasonable to expect that its attainment would compromise the availability or accuracy of the information or if the collection is reasonable for investigating "a breach of an agreement or a contravention of the laws."[281] Directly related to the workplace, an amendment to PIPEDA in June 2015 has since enabled organizations to collect personal information without knowledge or consent if the information "was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced."[282]

Among other responsibilities, the OPC oversees the implementation of the *Privacy Act* and PIPEDA by investigating complaints, issuing findings of compliance breach, and presenting non-enforceable recommendations.[283] In a previous investigation, the OPC found that an internet service provider using video cameras to monitor staff for the purpose of ensuring security and managing employee productivity was unreasonable on the basis that there existed less intrusive methods to address the employer's concerns.[284] In another case, the OPC recommended the removal of cameras where it found the use of camera surveillance was not demonstrably necessary for the purpose of maintaining security, hygiene or worker and product safety, and because less invasive safety methods could be used.[285]

OPC investigations have come to involve a four-part test to evaluate whether an employer's purposes for collecting personal information would be considered appropriate by a reasonable person. The test includes whether: a) the surveillance activity is necessary to meet a specific employer need; b) the surveillance is likely to be effective in meeting that need; c) the loss of privacy is proportional to the benefit gained; and d) there is a less privacy-invasive way of achieving the same end.[286] The OPC has also previously found it unacceptable for organizations to monitor employee emails without justifiable purposes under PIPEDA.[287] However, broad exceptions may allow organizations to access employee emails without consent, particularly for investigating a possible breach of an agreement or contravention of Canadian laws.[288]

Significant overhauls to PIPEDA have been proposed by the federal government through Bill C-11. The Bill has yet to advance in the legislative process beyond the first reading since being proposed in November 2020.[289] Yet, it nonetheless indicates the potential future of privacy and data protection rights in Canada, including in the context of the workplace. The Bill would enact the *Consumer Privacy Protection Act* (CPPA), repealing the parts of PIPEDA that concern the protection of personal information. It would create the Personal Information and Data Protection Tribunal, which would both hear appeals of certain decisions from the Office of the Privacy Commissioner and impose penalties for the violation of certain provisions of the CPPA. The prospect of organizations facing administrative penalties that are enforceable for CPPA-related violations is a significant step forward for privacy and data protection rights in Canada; however, the Office of the Privacy Commissioner has stated that these penalties would not apply to the most common and frequent violations of the proposed CPPA related to consent.[290]

In the workplace context, the CPPA would bring at least a few notable changes to the current privacy regime.[291] The law would continue to allow the *collection* of personal information without an employee's knowledge or consent if the information was "produced in the course of employment, business or profession" and if doing so is consistent with the purposes for which the information was produced. However, unlike PIPEDA, the CPPA would also allow for the *use* and *disclosure* of such personal employee information.[292] This change is important because it could enable employers to analyze information gathered in a way that augments surveillance capabilities. For example, this provision could allow employers to deploy software that recognizes and categorizes biometric data, including faces, potentially to the detriment of marginalized groups who face greater inaccuracy rates such as women, seniors or racialized people.[293]

It is also significant that the CPPA gives individuals the right to an explanation of any predictions, recommendations or decisions that are made using their information through an automated decision system.[294] However, it is plausible that broad exceptions to providing this explanation could be relied on by employers[295] in ways that deny employees the right to access and amend their information in situations where the use of technology could automate human prejudices and biases in ways that could violate equality rights.

One last proposed set of changes in the CPPA worth mentioning concerns de-identified information. Unlike PIPEDA, the CPPA provides special treatment for this type of information, defined in the CPPA as the modification or creation of personal information through "technical processes" to ensure that information does not identify an individual whether used alone or with information.[296] The CPPA allows organizations to use and disclose de-identified personal information for prospective business transactions without knowledge or consent, such as an employer disclosing de-identified employee information for the purposes of analysis or examination by a third party.[297] It also allows organizations to disclose de-identified personal information without knowledge or consent for "socially beneficial purposes" to Canadian government institutions, health care and post-secondary institutions, public libraries, or any organization mandated by law or contract to "carry out socially beneficial purpose."[298] On top of the risk of data re-identification,[299] these proposed changes in the CPPA could expand the surveillance of employees to third parties, including private organizations and government institutions without adequate regulatory oversight, which is rooted in the protection of the rights to knowledge and consent over how personal information is used and disclosed.

Canada Labour Code

The *Canada Labour Code* regulates the working conditions of employees at federally-regulated employers, such as transportation, telecommunications or banking corporations.[300] It establishes a framework for negotiating collective agreements in the unionized context and sets out certain norms for all workers, including those who are not unionized. Use of certain surveillance technology or tactics in the workplace may constitute harassment or may violate a given applicable collective agreement. In one case involving a claim of unjust dismissal, the Federal Court held that disclosure of the employee's personal information to a medical professional without consent was not unlawful pursuant to PIPEDA because "an individual who accepts employment is deemed to have consented to the collection, use and disclosure of personal information for management purposes."[301]

Private Sector Provincial Privacy Law

The provinces and territories across Canada also have laws for the private sector and many for the public sector, which could apply in the context of workplace surveillance.[302] The following analysis is limited to provincial private sector privacy laws.

British Columbia and Alberta

British Columbia and Alberta's provincial private sector privacy laws directly regulate employment-related collection, use and disclosure of personal information.[303] British Columbia and Alberta's *Personal Information Protection Acts (PIPA)* both stipulate that an organization can collect, use and disclose an employee's personal information without their consent if the collection is reasonable for the purposes of "establishing, managing or terminating an employment relationship between the organization and the individual."[304, 305] However, the organization is still required to give notice to the employee and outline the purposes of collecting personal information before it takes place.[306, 307] Under British Columbia's PIPA, this notice is exempted for a variety of reasons, including if the information is publicly available; consent cannot be achieved in a timely manner; consent would compromise the availability or accuracy of the information; or the collection is necessary to determine the individual's suitability to receive an honour, award or similar benefit.[308]

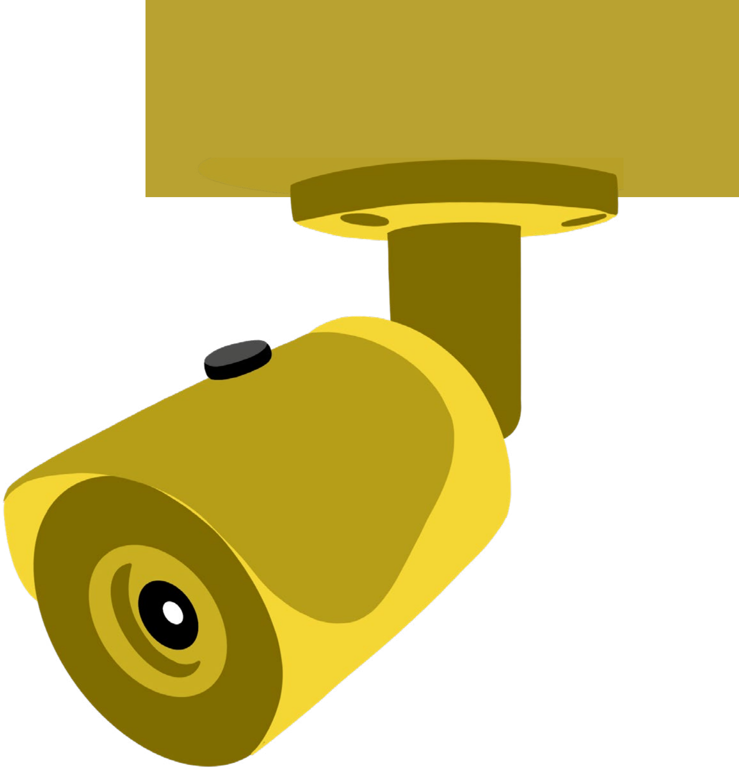
Quebec

The right to privacy in Quebec is enshrined in the *Quebec Charter of Human Rights and Freedoms* and the *Civil Code of Quebec*. Unlike the *Canadian Charter*, the *Quebec Charter* is not limited to "government action" only, and instead applies generally to all legal disputes in the province.[309] Section 4 of the *Quebec Charter* protects individuals' rights to safeguard one's dignity, honour and reputation; and Section 5 protects the right to respect for one's private life.[310]

The *Civil Code of Quebec* also contains provisions that are possibly applicable to employees' rights under surveillance. Section 3 of the *Code* protects the right to the inviolability and integrity of the person, and the right to the respect of one's reputation and privacy.[311] Moreover, section 36 outlines a set of actions that may be considered an invasion of privacy: the intentional interception of private communications; appropriating or using a person's image or voice while he is in private premises; keeping a person's life under observation by any means; using a person's name, image, likeness or voice for a purpose other than the legitimate information of the public; and finally, using a person's correspondence, manuscripts or other personal documents.[312]

Quebec's private sector privacy law allows employers to "establish a file" on another person only for a "serious and legitimate reason."[313] Among other rights, individuals must be informed of the "object" of the file, how collected information will be used, the categories of person who will have access to it, and where it is stored, as well as the rights to access and rectification of the information.[314] In June 2020, Quebec began the process of overhauling its private sector privacy law through Bill 64, heralding a potential new era of new changes, including tougher penalties for privacy violations and the right to object to automated decision-making.[315]

The Quebec Court of Appeal has held that invasions of privacy by employers may be justified on rational grounds when there is a reasonable connection between the surveillance measure deployed and the proper functioning of the organization, as well as when the surveillance is carried out by reasonable means. For example, when the employer has serious reasons for questioning the honesty of an employee's behaviour, the surveillance must occur only for the purpose of verifying the employee's behaviour and must use the least intrusive possible method of monitoring.[316]



Common Law Torts

There are also numerous torts that do not exist in statute, but have emerged in common law by virtue of precedent decisions in specific case disputes. Since 2012, the Ontario Court of Appeal has recognized the common law tort of "intrusion upon seclusion", involving the intentional (including reckless) invasion of a person's private affairs or concerns without lawful justification that a reasonable person would regard as highly offensive, causing distress, humiliation or anguish.[317] The publicity or publishing of private facts has also been applied or recognized in many cases by various courts and may be available to employees wishing to initiate civil proceedings on these bases against their employers.[318]

Implications

The review's findings have several critical implications for research, policy and practice, focused on the socio-technical, legal and policy challenges, in light of the global health pandemic.

05

5.1 Workplace Surveillance Accelerating and Expanding

Workplace surveillance, including through digital means, is not new. Prior to the pandemic, workplaces in various sectors and industries were steadily adopting surveillance technologies to monitor workers and conduct employee performance assessments. The rapid shift to remote work facilitated by the Covid-19 pandemic has increased employer demand for such surveillance technologies as a means to bridge the gap for employers unable to conventionally supervise workers onsite.[319] The pandemic has not only accelerated demands for remote work surveillance technologies, but has also shifted the ways in which such technologies are being used on-site.

Studies reveal that surveillance tends to accelerate and intensify during national crises and emergencies in a process known as 'surveillance creep,' where surveillance technologies used in one context are repurposed and deployed in others.[320, 321, 322] Literature discussing the pandemic's role in further expanding and accelerating surveillance practices, including in the workplace, are therefore not surprising. The sources reviewed reveal that workplace surveillance can raise concerns over employee privacy, the ethics of monitoring and human rights. The negative impacts of excessive workplace surveillance, that is when it goes beyond what is reasonable or necessary, include psychological effects such as low self-esteem, anxiety and depression.[323] When employees experience stress due to excessive monitoring, physical symptoms can also appear, including repetitive stress injuries or musculoskeletal discomfort.[324] Surveillance technologies that are increasingly able to assess worker performance through AI and other analytics software may lead to prejudicial treatment on the basis of age, race or gender, thereby exacerbating existing inequities.[325] Excessive surveillance practices, either on-site or at home, can come at a direct cost to human dignity, autonomy, and well-being.[326] It is therefore critical for policymakers and stakeholders to avoid focusing on privacy implications alone to account for the negative impacts of excessive workplace surveillance, and to expand their analyses to worker human rights.

5.2 Challenges with Current Employee Privacy Protections

New and emerging workplace surveillance technologies are used not only for monitoring workers, but are also increasingly relying on granular forms of data collection linked to AI and other analytics tools to measure employee performance or productivity, such as technologies that monitor keystrokes, eye movements, facial muscles, tone of voice and geolocation. While such technologies have often been discussed in relation to their growing use on-site, especially in manual labour and low-wage work settings,[327, 328] their expansion to monitor workers at home, in light of the pandemic, is further raising concerns over their implications — where the distinction between work and private activities is often blurred, particularly through use of personal devices and networks for work-related activity. Canada's current legal framework with respect to workplace surveillance provides employers with considerable leeway to surveil employees, so long as the surveillance is linked appropriately to employers' interests and goals.[329] There is a significant legal gap in that Canada's federal privacy law for the private sector does not currently presumptively extend protection to those working in the non-profit and charity sector, nor for political parties. New and emerging technologies are also shifting the legal analysis of workplace surveillance moving from earlier ones that focused on whether a worker had a reasonable expectation of privacy to one today where the analysis focuses on whether the surveillance itself is reasonable.[330]

The breadth of tools available for the collection, use and distribution of employee personal information, including without the knowledge of employees, may render the protections that privacy laws offer illusory.[331] This is particularly the case for surveillance technologies driven by AI and other analytics software, which are further complicating how to determine whether a reasonable person would consider the certain surveillance activity "appropriate in the circumstances" as required in Canada's federal private sector privacy law. Such automated technologies, capable of performance analysis using granular and expansive data collection, and ostensibly offering organizational enhancements to productivity (often with little or no evidence), are perhaps where the most challenges arise —¬ and where regulatory protection of employee's privacy is needed the most. Other jurisdictions, such as the EU, are advancing protections with respect to automated decision-making, providing the rights to be informed, receive meaningful explanations, and to not have decisions that produce legal or significant effects be based solely on automated processing without explicit consent.[332]

Many experts have also advocated that future amendments to Canada's federal privacy laws explicitly prioritize the right to privacy and data protection for individuals and workers, as has been enacted in the EU and California.[333, 334, 335] The ultimate impact of grounding Canada's privacy and data protection laws in a human rights approach would also ensure that the principles of necessity, proportionality and minimal intrusiveness — which are fundamental to rights-based balancing tests — are core features to any future modifications of the *Privacy Act* and PIPEDA.

5.3 Need for Workplace Guidance

Current Canadian privacy laws can provide employers with considerable latitude to use workplace surveillance technologies. On top of this, employers that utilize AI and other analytics tools for performance assessments pose some of the largest challenges in terms of balancing privacy and equality rights with their use. As a result, employers require guidance to ensure appropriate use of surveillance technologies that is informed by evidence-based best practices, which could include the following principles:

Transparency:

Employers should ensure that all information regarding the use of monitoring or surveillance tools is fully available to employees at all times and upon request. Employees must also be able to request that employers share any personal data they have collected, challenge its accuracy and completeness, and have it amended as appropriate. Employees should also have the ability to ask any questions related to their organization's surveillance policies without fear of repercussions; and the employer should answer truthfully and completely.

Clarity:

Employers should take active measures to ensure that employees are informed about how surveillance technology works, including the role of any automated decision-making, and the potential risks associated with such workplace monitoring and assessment. Training sessions should inform employees about the potential cybersecurity and privacy risks, harms, and benefits of using surveillance technology. Considering the novelty and technical complexity of new forms of employee monitoring, employers should ensure that complex, inaccessible jargon is not used to intimidate employees from fully understanding the nuances and drawbacks of employee surveillance technologies, particularly when working from home.

Inclusion:

Employers should include the opinion and voices of all relevant stakeholders, including vulnerable and minority employees, prior to adopting any form of surveillance technology. Employees should be consulted about the most accurate and fair metrics by which employers can assess productivity. Demanding that employees provide information about all aspects of their work behaviour, such as monitoring screen time and keystrokes, may be an inaccurate reflection of the employee's quality of work and, therefore, an ineffective measure by which to rank employees.

Equity:

Employers should regularly review its surveillance practices, including any associated automated decision-making procedures, to ensure they do not result in differential treatment of any group based on a prohibited ground of discrimination within human rights laws, such as race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics and disability. This should include empowering the voices of underrepresented groups and incorporating their specific recommendations in updating workplace surveillance policies.

Reasonable expectations of employees:

Employers should assure workers that they are entitled to reasonable breaks, free from any electronic monitoring, and are limited to specific work hours. Employees should not be pressured to work significantly long hours at a time or neglect important personal matters. Employers should also consider flexibility and acceptance of different working styles if deliverables are met and completed on time and with good quality.

Security:

Employers must develop, implement and maintain a security policy that protects employee personal information collected through monitoring tools using appropriate and necessary security safeguards. These include strong user authentication, data access limits, secure device configuration, encryption, perimeter defenses, software security updates and ongoing staff training.

Least intrusive approach:

Employers should operate based on a principle of minimalism; the least intrusive methods that fulfill the employer's needs should be used. If less granular and invasive monitoring tools can replace existing techniques while still fulfilling the employer's purpose, then employers have a responsibility to update their policies and practices accordingly, and transition to more secure, less pervasive and intrusive monitoring tools. Employers should justify their use of certain technologies by clearly demonstrating a lack of a sufficient alternative. They should also ensure that employee personal data are only stored for as long as required to serve the intended purpose.

One way to effectively advance these standards is through the implementation of data protection and privacy impact assessments prior to the deployment of any surveillance practices in the workplace. The findings of these assessments should ideally be made public and/or available to employees, to enable better informed consent decisions and trust.

5.4 Need for Greater Regulatory Enforcement

Although Canada's current private sector privacy law outlines principles on the regulation of personal information, it lacks substantial enforcement powers to implement these principles into day-to-day business operations.[336] The Office of the Privacy Commissioner does not currently have the ability to issue final binding orders of compliance or levy fines, even if it finds that the entity in question has violated the provisions or principles set out in the *Privacy Act* or PIPEDA.[337] The OPC also does not currently have the authority to proactively inspect the practices of private sector organizations, in the absence of a complaint or open investigation, unlike the powers given to data protection authorities in the UK and Australia.[338]

Greater enforcement mechanisms would set clearer limits for non-compliant behaviours and unreasonable surveillance practices or tools, deter employers from violating privacy protections, and make it in the best interest of organizations to comply with OPC investigations.[339] Weak enforcement mechanisms hinder the ability to place reasonable limits on employee surveillance, and make it far more challenging to ensure that employers are sufficiently protecting the personal and sensitive data collected from workers. On this latter point, ineffective data management practices in fact make organizations more vulnerable to cybersecurity attacks, which have significantly increased since the onset of the pandemic. Reports have linked the rise in cyberattacks to organizations' hasty deployment of remote surveillance technologies to monitor employees at home, many of which were found to contain weaknesses and other vulnerabilities for attackers to exploit.[340]

Greater enforcement measures could also improve the effectiveness of organizations in obtaining informed and meaningful consent prior to the collection of personal and sensitive employee information through surveillance tools. Currently, the OPC does not have the power to compel organizations to enforce consent requirements with respect to employee monitoring. Even if it did, workers typically lack the power to meaningfully withhold consent from employer monitoring activity.[341] Truly meaningful consent includes employees being well-informed of the surveillance technology used for monitoring, including how the technology works; the information that will be collected; where this information will be stored; any privacy risks; how the information will be used; how the data collected may impact employment conditions; to whom this data will be disclosed; how to access and seek corrections to the information; and, ideally, what alternatives may exist without consequences for employment. As a result, workers in Canada may find their personal information in the hands of their employers without sufficient knowledge of how date are collected and used. Stronger mechanisms to ensure that organizations attain informed, meaningful consent from employees under surveillance, especially when performance analysis tools are deployed, would promote greater trust in workplace environments.

5.5 Need to Fill Research Gaps on Marginalized Communities and Cybersecurity

This scoping review demonstrates that there is a dearth of knowledge about the impacts of workplace surveillance on vulnerable and marginalized communities in Canada. It is well-known that surveillance and automated technologies may exacerbate inequities through their design and deployment. For instance, there is a growing body of research that outlines the presence of bias in facial recognition technologies,[342] whose algorithms have been found less accurate when performed on darker skin tones, women, trans and non-binary people, and seniors.[343] Workplace surveillance technologies, particularly those that are driven by AI, may lead to biased treatment on the basis of age, gender and race. This review provides a window into the biased treatment of employees based on such traditional markers of difference, for instance including the gender-based aspects of experiencing greater concern for one's privacy when monitored at work,[344] and being more likely to view workplace camera surveillance as unacceptable.[345] More broadly, surveillance studies literature has frequently shown how racialized communities are disproportionately targeted and subject to greater surveillance and biased treatment, facilitated through digital technologies.[346, 347, 348] However, studies in the scoping review revealed a significant absence in research on the impacts of workplace surveillance on marginalized and vulnerable communities, particularly in the Canadian context, for example based on age, gender, sexual orientation, race, (dis)ability and other bases of protection provided by equality laws.

More research on the impacts of workplace surveillance technologies, particularly in a post-Covid and remote-working era, is critical to shaping policy and protecting employee rights and privacy, particularly those who are most vulnerable in Canadian society. To some extent, the lack of research on workplace surveillance, particularly on remote work, is understandable given the novelty of the pandemic. However, it is not only remote work surveillance but also research on workplace surveillance on-site that is also absent. Key areas of future Canadian research include surveillance in low-wage work settings, particularly as the costs of resisting surveillance may be too high for such groups, including the potential loss of income, creating

an unfair distribution of power between employer and employee.[349] It is also known that workers in manual labour and low-wage work settings are subject to more overt and continuous surveillance, such as overt cameras and electronic tracking.[350] Such workplaces often consist of highly racialized work forces. Such intrusive surveillance technologies could harm vulnerable employees' health and well-being by promoting unreasonable work demands and developing an organizational culture that promotes an excessively fast-paced, minimal downtime approach to work.[351] Work strain and stress have long been linked to a variety of mental health issues, including anxiety, depression and loss of concentration.[352] Unreasonable work expectations and the discouragement of breaks could be particularly harmful for people with disabilities or older adults, who face a significant risk of harm from working at a faster pace with no rest. Thus, the need for Canadian-specific research on workplace surveillance is crucial to producing further knowledge and creating policies aimed at dismantling structural inequities.

In addition, this review indicates a significant absence of studies on the cybersecurity implications of workplace surveillance in the Canadian context. There is also little in-depth research on the cybersecurity risks posed by surveillance technologies, despite the steep increase in cyberattacks on workplaces since the beginning of the Covid-19 pandemic. The rise in cyberattacks is costly for businesses, and places employees' personal information at greater risk of misuse. The increasing demands for remote surveillance technologies by employers are linked globally to an increase in cybersecurity attacks and data breaches. More research is needed in Canada on how the Covid-19 pandemic and the rapid expansion and acceleration of remote surveillance technologies correlates, and in what ways, with cyber attacks. More research outlining the extent and types of cybersecurity risks related to workplace surveillance technologies — particularly as work-from-home measures continue to be more than temporary arrangements — is also critical to the development and effective implementation of strong data protection and security measures in a post-Covid context.

Project Limitations

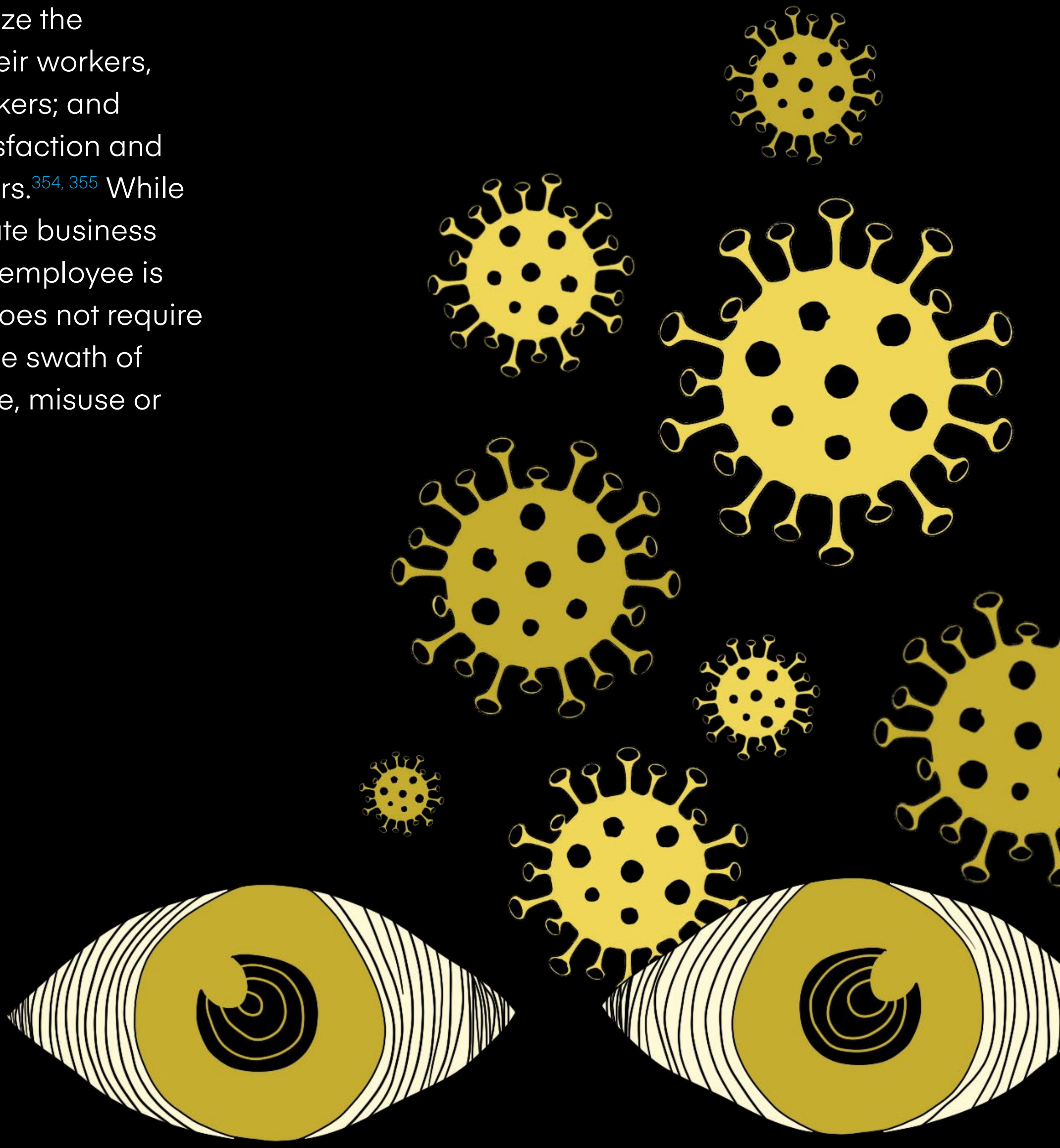
Like all scoping reviews, this project has some limitations. Scoping reviews gather information from various sources with a range of designs and methods. As a result, the sources included can produce a sizeable result, focusing on breadth and not necessarily depth, with the aim of providing an overview of the available literature. To this end, scoping reviews do not aim to produce a "critically appraised and synthesized result/answer to a particular question."[353] Although the project has aimed to be as comprehensive as possible, this review may have not identified all literature published on this topic in the last 10 years. Various search strings were developed to describe the electronic surveillance of workers; however, other terms and variations, may also exist. Like other studies, there is also a risk of bias, including selection bias. Our review included sources published only in English and was conducted using only English terms. Further, the lack of critical appraisal may also impact the implications for practice, particularly by being limited in terms of providing granular guidance. As Munn et al. have suggested, scoping reviews are often seen as a precursor to systematic reviews and indeed this study may act as such, and indeed, as a springboard for other studies.

Conclusion

06

The increased monitoring and surveillance of workers spurred on by Covid-19 has provoked significant concern from a wide range of stakeholders including activists, legal experts, workers and regulators. 'Work' environments have increasingly come to encompass employees' personal homes amid the normalization of remote work. This has blurred the lines of what constitutes work and personal life, with workers now facing an increased risk of exposing personal and sensitive information while using personal devices and network connections. It is in workers' and organizational interests for employers to prioritize the privacy and equality rights of their workers, in order to build trust; retain workers; and improve worker motivation, satisfaction and positive perceptions of employers.[354, 355] While employers have certain legitimate business interests, assessing whether an employee is engaged, attentive or efficient does not require invasive software, placing a wide swath of personal data at risk of exposure, misuse or biased assessment.

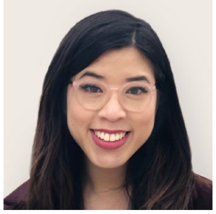
The Covid-19 pandemic has not brought to light anything new regarding the monitoring of workers; instead it has reinforced and accelerated surveillance trends, exacerbating what many workers in Canada have long experienced through both overt and covert surveillance practices. Canada's employers need better guidance and enforcement to ensure that the treatment of workers and their information is reasonable, appropriate and best engenders privacy, security and trust.



About the Authors

Mohammed (Joe) Masoodi is a Senior Policy Analyst in the Ryerson Leadership and Cybersecure Policy Exchange. Joe has been conducting research and policy analysis at the intersections of surveillance, digital technologies, security and human rights for over six years. He has conducted research at the Surveillance Studies Centre at Queen's University and the Canadian Forces College. He holds an MA in war studies from the Royal Military College of Canada, an MA in sociology from Queen's University, and has studied sociology as a PhD candidate from Queen's University, specializing in digital media, information and surveillance.

Nour Abdelaal is a Policy Analyst in the Ryerson Leadership and Cybersecure Policy Exchange. Nour has been working at the intersection of research, public service, academia, and social advocacy for four years. She is passionate about advancing innovative policy solutions in the realms of technology, cybersecurity, and digital inclusion. Prior to joining the Leadership Lab, she was a Political Assistant at the U.S. Consulate General in Toronto, working to advance U.S.-Canada relations and provide research insights for the U.S. State Department's technology and economic portfolio. Nour was also a Compliance Analyst at the G20 Research Group at the Munk School of Global Affairs and the Finance Director of the University of Toronto's Amnesty International Chapter. She holds an MA in political theory and a BA in political science and economics from the University of Toronto.



Stephanie Tran is an experienced researcher with over five years of experience analyzing public policy and human rights issues related to digital technologies, with past experience working for the Citizen Lab, Amnesty International Canada, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) and more. She is a trained computer programmer, having earned a Diploma in Computer Programming from Seneca College. She also holds a dual degree Master of Public Policy (Digital, New Technology and Public Affairs Policy stream) from Sciences Po in Paris, and a Master of Global Affairs from the University of Toronto. She earned her BA degree from the University of Toronto specializing in Peace, Conflict and Justice.

Yuan Stevens is the Policy Lead at the Cybersecure Policy Exchange and the Ryerson Leadership Lab. Yuan is an action-oriented researcher working at the intersections of law, policy and computer security. Her work equips society with the ability to understand and patch up harmful vulnerabilities in sociotechnical and legal systems. Passionate about building community, she is also a research affiliate at the Data & Society Research Institute and a research fellow at the Centre for Media, Technology & Democracy at McGill's School of Public Policy. She received her B.C.L./J.D. from McGill University in 2017, working as a research assistant for hacker expert Gabriella Coleman. She serves on the board of directors for Open Privacy Research Institute and previously worked at the Berkman Klein Center for Internet & Society at Harvard University.

Sam Andrey is the Director of Policy & Research at the Ryerson Leadership Lab. Sam has led applied research and public policy development for the past decade, including the design, execution and knowledge mobilization of surveys, focus groups, interviews, randomized controlled trials and cross-sectional observational studies. He also teaches about public leadership and advocacy at Ryerson University and George Brown College. He previously served as Chief of Staff and Director of Policy to Ontario's Minister of Education, in the Ontario Public Service and in not-for-profit organizations advancing equity in education and student financial assistance reform. Sam has an Executive Certificate in Public Leadership from Harvard's John F. Kennedy School of Government and a BSc from the University of Waterloo.

Karim Bardeesy is the Co-Founder and Executive Director of the Ryerson Leadership Lab. Karim is a public service leader who has worked in progressively senior roles in public policy, politics, journalism and academia in Toronto and the United States since 2001. He is also a board member of The Atmospheric Fund and Corporate Knights, Inc., a member of the Banff Forum, and a founding faculty member of Maytree Policy School. Karim was previously Deputy Principal Secretary for the Premier of Ontario, the Honourable Kathleen Wynne, and served as Executive Director of Policy for Premiers Wynne and Dalton McGuinty. He has worked as a journalist, an editorial writer at *The Globe and Mail*, and as an editorial assistant at Slate magazine. Karim holds a Master in Public Policy from Harvard's John F. Kennedy School of Government.

References

[1] Mateescu, A. & Nguyen, A. (2019, February 6). Explainer: Workplace Monitoring & Surveillance. *Data & Society*. https://datasociety.net/library/explainer-workplace-monitoring-surveillance/

[2] Ball, K., & Webster, F. (2003). *The Intensification of surveillance: Crime, terrorism and warfare in the information age*. London: Pluto Press.

[3] See for instance the work of Braverman, H. (1974). Labor and monopoly capital: The degradation of work in the twentieth century.

[4] Ball, K. (2002). Elements of surveillance: a new framework and future research directions. Information Communication and Society, 5(4), 573-590.

[5] Manokha, I. (2020). The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace. Surveillance & Society, 18(4), 540–554. https://doi.org/10.24908/ss.v18i4.13776

[6] Ford, J. C., Willey, L., & White, B. J. (2014). New Concerns in Electronic Employee Monitoring: Have You Checked Your Policies Lately? Allied Academies International Conference. Academy of Legal, Ethical and Regulatory Issues. Proceedings, 18(1), 7.

[7] Ibid.

[8] Charbonneau, É., & Doberstein, C. (2020). An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector. Public Administration Review, 80(5), 780–791. Scopus. https://doi.org/10.1111/puar.13278

[9] Martin, T. (2020, March 11). More companies asking employees to work from home to slow spread of coronavirus. The Globe and Mail. https://www.theglobeandmail.com/business/article-more-companies-asking-employees-to-work-from-home-to-slow-spread-of/.

[10] Nardi, C. (2020, March 13). Ottawa to allow federal bureaucrats to work from home if possible to prevent coronavirus spread. The National Post. https://nationalpost.com/news/canada/ottawa-orders-federal-bureaucrats-to-work-from-home.

[11] Deng, Z., Morissette, R. & Messacar, D. (2020, May 28). Running the economy remotely: Potential for working from home during and after COVID-19. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2020001/article/00026-eng.htm.

[12] Statistics Canada. (2021, August 4). The Daily—Working from home during the COVID-19 pandemic, April 2020 to June 2021. Statistics Canada. https://www150.statcan.gc.ca/n1/daily-quotidien/210804/dq210804b-eng.htm

[13] Deng, Z., Morissette, R. & Messacar, D. (2020, May 28). Running the economy remotely: Potential for working from home during and after COVID-19. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2020001/article/00026-eng.htm.

[14] Statistics Canada. (2021, August 4). The Daily—Working from home during the COVID-19 pandemic, April 2020 to June 2021. Statistics Canada. https://www150.statcan.gc.ca/n1/daily-quotidien/210804/dq210804b-eng.htm

[15] Neustaeter, B. (2020, July 14). More Canadians will be working from home post-pandemic, StatsCan data suggests. CTV News. https://www.ctvnews.ca/health/coronavirus/more-canadians-will-be-working-from-home-post-pandemic-statcan-data-suggests-1.5023822

[16] Cheng, C. (2020, May 21). Shopify Is Joining twitter in Permanent Work-From-Home Shift. Bloomberg. https://www.bloomberg.com/news/articles/2020-05-21/shopify-is-joining-twitter-in-permanent-work-from-home-shift.

[17] Statistics Canada. (2021, April 1). Percentage of new teleworkers who reported that they would prefer to work at least half of their hours at home once the COVID-19 pandemic is over, by sex and selected characteristics. Statistics Canada. https://www150.statcan.gc.ca/n1/daily-quotidien/210401/t003b-eng.htm

[18] Hertzberg, E. (2021, May 26). Remote Work Habits Are Likely to Outlast the Pandemic in Canada. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-26/remote-work-habits-are-likely-to-outlast-the-pandemic-in-canada

[19] Bennett, C. (2005) "Surveillance, Employment and Location: Regulating the Privacy of Mobile Workers in the Mobile Workplace," in S. O. Hansson and E. Palm, The Ethics of Workplace Privacy (Brussels: Peter Lang).

[20] Garson, B. (1988). The Electronic Sweatshop, New York: Simon and Shuster.

[21] Zuboff, S. (1998). In the Age of the Smart Machine: The Future of Work and Power, New York: Basic Books.

[22] Mateescu, A. & Nguyen, A. (2019, February 6). Explainer: Workplace Monitoring & Surveillance. Data & Society. https://datasociety.net/library/explainer-workplace-monitoring-surveillance/

[23] Vigliarolo, B. (2021, June 3). COVID-19 has transformed work, but cybersecurity isn't keeping pace, report finds. TechRepublic. https://www.techrepublic.com/article/covid-19-has-transformed-work-but-cybersecurity-isnt-keeping-pace-report-finds/

[24] Holland, P., Cooper, B. & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace. Personnel Review. 44. 161-175. https://doi.org/10.1108/PR-11-2013-0211.

[25] Ball, K. (2010). Workplace surveillance: an overview. Labor History, 51, 106 - 87. https://www.doi.org/10.1080/00236561003654776

[26] Ball, K. S., & Margulis, S. T. (2011). Electronic Monitoring and Surveillance in Call Centres: A Framework for Investigation. New Technology, Work & Employment, 26(2), 113–126. https://doi.org/10.1111/j.1468-005X.2011.00263.x

[27] Lyon, D. (2007). Surveillance Studies: An Overview. Cambridge: Polity Press, 14

[28] Lyon, D. (2009). "Surveillance, Power, and Everyday Life." pp. 449-470 in The Oxford Handbook of Information and Communication Technologies, edited by C. Avgerou, R. Mansell, D.Quah, and R. Silverstone. New York: Oxford University Press.

[29] Arksey, H. & O'Malley, L. (2005). Scoping Studies: Towards a Methodological Framework. International Journal of Social Research Methodology 8 (1): 19–32.

[30] Ibid, 24

[31] Ibid, 26.

[32] McParland, C., & Connolly, R. (2020). Dataveillance in the Workplace: Managing the Impact of Innovation. Business Systems Research, 11(1), 106–124. http://dx.doi.org.ezproxy.lib.ryerson.ca/10.2478/bsrj-2020-0008

[33] Backhaus, N. (2019). Context Sensitive Technologies and Electronic Employee Monitoring: A Meta-Analytic Review. 2019 IEEE/SICE International Symposium on System Integration (SII), 548–553. https://doi.org/10.1109/SII.2019.8700354

[34] Khakurel, J., Melkas, H., & Porras, J. (2018). Tapping into the wearable device revolution in the work environment: A systematic review. Information Technology & People, 31(3), 791–818. https://doi.org/10.1108/ITP-03-2017-0076

[35] Ball, K. S., & Margulis, S. T. (2011). Electronic Monitoring and Surveillance in Call Centres: A Framework For Investigation. New Technology, Work & Employment, 26(2), 113–126. https://doi.org/10.1111/j.1468-005X.2011.00263.x

[36] Nguyen, A. (2021). The Constant Boss. Data & Society. https://datasociety.net/library/the-constant-boss/

[37] Mateescu, A., & Nguyen, A. (2019). Explainer: Workplace monitoring and surveillance. https://apo.org.au/node/218571

[38] Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. California Law Review, 105(3), 735–776. Scopus. https://doi.org/10.15779/Z38BR8MF94

[39] Villeneuve, S., & Elias, D. (2020, September 2). Surveillance Creep: Data collection and privacy in Canada during COVID-19. Brookfield Institute for Innovation + Entrepreneurship. https://brookfieldinstitute.ca/surveillance-creep-data-collection-and-privacy-in-canada-during-covid-19

[40] Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance. Journal of the Association for Information Science & Technology, 71(9), 1074–1088. https://doi.org/10.1002/asi.24342

[41] Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. International Journal of Human Resource Management, 27(21), 2635–2651. https://doi.org/10.1080/09585192.2016.1225313

[42] Chory, R. M., Vela, L. E., & Avtgis, T. A. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. Employee Responsibilities and Rights Journal, 28(1), 23–43. Scopus. https://doi.org/10.1007/s10672-015-9267-4

[43] Charbonneau, É., & Doberstein, C. (2020). An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector. Public Administration Review, 80(5), 780–791. Scopus. https://doi.org/10.1111/puar.13278

[44] Bernd, J., Abu-Salma, R., & Frik, A. (2020). Bystanders' privacy: The perspectives of nannies on smart home surveillance. FOCI 2020 - 10th USENIX Workshop on Free and Open Communications on the Internet, co-located with USENIX Security 2020. Scopus. https://www.usenix.org/system/files/foci20-paper-bernd.pdf

[45] Bakewell, L. L., Vasileiou, K., Long, K. S., Atkinson, M., Rice, H., Barreto, M., Barnett, J., Wilson, M., Lawson, S., & Vines, J. (2018). Everything We Do, Everything We Press: Data-Driven Remote Performance Management in a Mobile Workplace. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–14. https://doi.org/10.1145/3173574.3173945

[46] Winston, T. G., Paul, S., & Iyer, L. (2016). A Study of Privacy and Security Concerns on Doctors' and Nurses' Behavioral Intentions to Use RFID in Hospitals. 2016 49th Hawaii International Conference on System Sciences (HICSS), 3115–3123. https://doi.org/10.1109/HICSS.2016.392

[47] Anteby, M., & Chan, C. K. (2018). A Self-Fulfilling Cycle of Coercive Surveillance: Workers' Invisibility Practices and Managerial Justification. Organization Science, 29(2), 247–263. https://doi.org/10.1287/orsc.2017.1175

[48] Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: An empirical study. Information Technology & People, 25(4), 376–394. https://doi.org/10.1108/09593841211278785

[49] Sewell, G., Barker, J. R., & Nyberg, D. (2012). Working under intensive surveillance: When does "measuring everything that moves" become intolerable? Human Relations, 65(2), 189–215. Scopus. https://doi.org/10.1177/0018726711428958

[50] Stark, L., Stanhaus, A. and Anthony, D.L. (2020). "I don't want someone to watch me while I'm working": Gendered views of facial recognition technology in workplace surveillance. JASIST, 71(9), 1074-1088

[51] Henderson, T., Swann, T., & Stanford, J. (2018). Under the employer's eye: Electronic monitoring and surveillance in Australian workplaces (Australia) [Report]. Centre for Future Work. https://apo.org.au/node/204726

[52] Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. International Journal of Human Resource Management, 27(21), 2635–2651. https://doi.org/10.1080/09585192.2016.1225313

[53] Chory, R. M., Vela, L. E., & Avtgis, T. A. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. Employee Responsibilities and Rights Journal, 28(1), 23–43. Scopus. https://doi.org/10.1007/s10672-015-9267-4

[54] Jeske, D., & Santuzzi, A. M. (2015). Monitoring what and how: Psychological implications of electronic performance monitoring. New Technology, Work & Employment, 30(1), 62–78. https://doi.org/10.1111/ntwe.12039

[55] Ball & Margulis, Electronic Monitoring and Surveillance in Call Centres.

[56] Ball, Daniel & Stride, Dimensions of employee privacy.

[57] Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance. Journal of the Association for Information Science & Technology, 71(9), 1074–1088. https://doi.org/10.1002/asi.24342

[58] Richardson, S., & Mackinnon, D. (2018). Becoming Your Own Device: Self-Tracking Challenges In The Workplace. Canadian Journal of Sociology, 43(3), 225–250. https://doi.org/10.29173/cjs28974

[59] Ibid.

[60] Oravec, J. A. (2020). Digital iatrogenesis and workplace marginalization: Some ethical issues involving self-tracking medical technologies. Information, Communication & Society, 23(14), 2030–2046.

[61] Mateescu, A., & Nguyen, A. (2019). Explainer: Workplace monitoring and surveillance. 16. https://apo.org.au/node/218571

[62] Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. California Law Review, 105(3), 735–776. Scopus. https://doi.org/10.15779/Z38BR8MF94

[63] Nguyen, A. (2021). The Constant Boss. Data & Society. https://datasociety.net/library/the-constant-boss/

[64] Proofpoint. (2021). 2021 Voice of the CISO Report. Proofpoint. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf

[65] Kovac, R. (2021). ESET Threat Report Q4 2020. ESET. https://www.welivesecurity.com/2021/02/08/eset-threat-report-q42020/

[66] Stephenson, A. (2021, July 28). Cost of data breaches in Canada hit new record in 2021: IBM. Calgary. https://calgary.ctvnews.ca/cost-of-data-breaches-in-canada-hit-new-record-in-2021-ibm-1.5526127

[67] Irwin, L. (2021, May 5). The cyber security risks of working from home—IT Governance blog. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home

[68] Brute-force RDP attacks are when attackers repeatedly attempt to login using different passwords, hoping to guess login credentials correctly.

[69] Cimpanu, C. (2020, April 29). Kaspersky: RDP brute-force attacks have gone up since start of COVID-19. ZDNet. https://www.zdnet.com/article/kaspersky-rdp-brute-force-attacks-have-gone-up-since-start-of-covid-19/

[70] FBI National Press Office. (2021, July 28). U.S., U.K., and Australia Issue Joint Cybersecurity Advisory [Press Release]. Federal Bureau of Investigation. https://www.fbi.gov/news/pressrel/press-releases/us-uk-and-australia-issue-joint-cybersecurity-advisory

[71] IBM. (2021). Cost of a Data Breach Report 2021. IBM. https://www.ibm.com/security/data-breach

[72] Charbonneau & Doberstein, An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector.

[73] Richardson and MacKinnon, Becoming Your Own Device.

[74] Ibid.

[75] Fierro, D. (2020, September 21). How Amazon (and Others) Spy on Workers. Lifewire. https://www.lifewire.com/how-amazon-and-others-spy-on-employees-5078745

[76] Gurley, L. K., & Cox, J. (2020, January 9). Inside Amazon's Secret Program to Spy On Workers' Private Facebook Groups. Vice. https://www.vice.com/en/article/3azegw/amazon-is-spying-on-its-workers-in-closed-facebook-groups-internal-reports-show

[77] Hanley, D. A., & Hubbard, S. (2020). Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power. Open Markets. https://www.openmarketsinstitute.org/publications/eyes-everywhere-amazons-surveillance-infrastructure-and-revitalizing-worker-power

[78] Asher-Schapiro, A. (2021, February 5). Amazon AI van cameras spark surveillance concerns. News.Trust.Org. https://news.trust.org/item/20210205132207-c0mz7/

[79] Delfanti, A., & Frey, B. (2020). Humanly Extended Automation or the Future of Work Seen through Amazon Patents. Science Technology and Human Values. Scopus. https://doi.org/10.1177/0162243920943665

[80] Sheng, E. (2019, April 15). Employee privacy in the US is at stake as corporate surveillance technology monitors workers' every move. CNBC. https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html

[81] Ball & Margulis, Electronic Monitoring and Surveillance in Call Centres.

[82] Ball, Daniel & Stride, Dimensions of Employee Privacy.

[83] Sewell, G., Barker, J. R., & Nyberg, D. (2012). Working under intensive surveillance: When does "measuring everything that moves" become intolerable? Human Relations, 65(2), 189–215. Scopus. https://doi.org/10.1177/0018726711428958

[84] McCallum, J. K. (2021, February 24). Remote Controlled Workers. The American Prospect. https://prospect.org/api/content/3bcf0f42-7618-11eb-9deb-1244d5f7c7c6/

[85] Katz, L. M. (2015). Big Employer Is Watching. HR Magazine. 60(5) http://search.proquest.com/pqrl/docview/1684996595/abstract/501050B521949FBPQ/115

[86] Gamble, J. (2019, June 3). The Inequalities of Workplace Surveillance. The Nation. https://www.thenation.com/article/archive/worker-surveillance-big-data/

[87] Winston, T. G., Paul, S., & Iyer, L. (2016). A Study of Privacy and Security Concerns on Doctors' and Nurses' Behavioral Intentions to Use RFID in Hospitals. 2016 49th Hawaii International Conference on System Sciences (HICSS), 3115–3123. https://doi.org/10.1109/HICSS.2016.392

[88] Schnake, M., & Copeland, R. (2015). Harris medical center and Harris memorial hospital: Unfair labor practices or management's rights? Journal of the International Academy for Case Studies, 21(1), 81–86. Scopus.

[89] Ford, J., Willey, L., White, B. J., & Domagalski, T. (2015). New Concerns in Electronic Employee Monitoring: Have You Checked Your Policies Lately? Journal of Legal, Ethical and Regulatory Issues, 18(1), 51–70.

[90] McParland, C., & Connolly, R. (2020). Dataveillance in the Workplace: Managing the Impact of Innovation. Business Systems Research Journal, 11(1), 106–124. https://doi.org/10.2478/bsrj-2020-0008

[91] West, J. P., & Bowman, J. S. (2016). Electronic Surveillance at Work: An Ethical Analysis. Administration and Society, 48(5), 628–651. Scopus. https://doi.org/10.1177/0095399714556502

[92] Chory, R. M., Vela, L. E., & Avtgis, T. A. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. Employee Responsibilities and Rights Journal, 28(1), 23–43. Scopus. https://doi.org/10.1007/s10672-015-9267-4

[93] Backhaus, N. (2019). Context Sensitive Technologies and Electronic Employee Monitoring: A Meta-Analytic Review. 2019 IEEE/SICE International Symposium on System Integration (SII), 548–553. https://doi.org/10.1109/SII.2019.8700354.

[94] Katz, L. M. (2015). Big Employer Is Watching. HRMagazine, 60(5). https://www.proquest.com/trade-journals/big-employer-is-watching/docview/1684996595/se-2

[95] Chory, Vela & Avtgis. Organizational Surveillance of Computer-Mediated Workplace Communication.

[96] McParland & Connolly, Dataveillance in the Workplace.

[97] Ibid.

[98] Business Wire. (2020, May 7). ActivTrak Survey: SMBs Cite Productivity as a Top Concern as 43% More Companies Transition to a Remote Workforce. Business Wire. https://www.businesswire.com/news/home/20200507005856/en/ActivTrak-Survey-SMBs-Cite-Productivity-as-a-Top-Concern-as-43-More-Companies-Transition-to-a-Remote-Workforce

[99] Backhaus, Context Sensitive Technologies and Electronic Employee Monitoring.

[100] Katz, Big Employer Is Watching.

[101] Manokha, I. (2020). The implications of digital employee monitoring and people analytics for power relations in the workplace. Surveillance and Society, 18(4), 540–554. Scopus. https://doi.org/10.24908/ss.v18i4.13776

[102] American Management Association. (2019, April 8). The Latest on Workplace Monitoring and Surveillance. American Management Association. https://www.amanet.org//articles/the-latest-on-workplace-monitoring-and-surveillance/

[103] Shook, E., Knickrehm, M., & Sage-Gavin, E. (n.d.). Decoding Organizational DNA. Accenture. Retrieved August 9, 2021, from https://www.accenture.com/us-en/insights/future-workforce/workforce-data-organizational-dna

[104] Intrado Global Newswire. (2021, January 22). Cloud-based Office Productivity Software Industry 2020-2027—Worldwide Market Shares for Adobe, Amazon, Apple, Google, HP, IBM, Microsoft and Other Competitors. https://www.globenewswire.com/fr/news-release/2021/01/22/2162754/0/en/Cloud-based-Office-Productivity-Software-Industry-2020-2027-Worldwide-Market-Shares-for-Adobe-Amazon-Apple-Google-HP-IBM-Microsoft-and-Other-Competitors.html

[105] Global User Activity Monitoring Market 2018-2023—A $3.33 Billion Market Opportunity—ResearchAndMarkets.com. (2018, April 11). Business Wire. https://www.businesswire.com/news/home/20180411005833/en/Global-User-Activity-Monitoring-Market-2018-2023---A-3.33-Billion-Market-Opportunity---ResearchAndMarkets.com

[106] Jagannathan, M. (2020, August 4). Like 'punching a time clock through your webcam': How employers are keeping tabs on remote workers during the pandemic. MarketWatch. https://www.marketwatch.com/story/like-punching-a-time-clock-through-your-webcam-how-employers-are-keeping-tabs-on-remote-workers-during-the-pandemic-11596484344

[107] Katz, Big Employer Is Watching.

[108] Anderson, G., Blumenfeld, S., & Hooper, V. (2020, June 16). A question of trust: Should bosses be able to spy on workers, even when they work from home? The Conversation. http://theconversation.com/a-question-of-trust-should-bosses-be-able-to-spy-on-workers-even-when-they-work-from-home-140623

[109] Cyphers, B., & Gullo, K. (2020). Inside the Invasive, Secretive "Bossware" Tracking Workers. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

[110] Ibid.

[111] Ibid.

[112] Ibid.

[113] McCallum, J. K. (2021, February 24). Remote Controlled Workers. The American Prospect. https://prospect.org/api/content/3bcf0f42-7618-11eb-9deb-1244d5f7c7c6/

[114] Kelly, J. (2020, August 13). Big British Bank Barclays Accused Of Spying On Employees—This May Be The New Trend. Forbes. https://www.forbes.com/sites/jackkelly/2020/08/13/big-british-bank-barclays-accused-of-spying-on-employees-this-may-be-the-new-trend/

[115] Hanley, D. A., & Hubbard, S. (2020). Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power. Open Markets. https://www.openmarketsinstitute.org/publications/eyes-everywhere-amazons-surveillance-infrastructure-and-revitalizing-worker-power

[116] Ibid.

[117] Lecher, C. (2019, April 25). How Amazon automatically tracks and fires warehouse workers for 'productivity.' The Verge. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

[118] Hanley & Hubbard, Eyes Everywhere.

[119] Pringle, M., & O'Leary, A. (2019, January 15). Call centre staff given just two minutes per day for toilet breaks. Mirror. https://www.mirror.co.uk/news/uk-news/virgin-media-call-centre-staff-13853032

[120] Connolly, R. (2020, December 14). The pandemic has taken surveillance of workers to the next level. The Guardian. http://www.theguardian.com/commentisfree/2020/dec/14/pandemic-workers-surveillance-monitor-jobs

[121] Manokha, The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace.

[122] The Week Staff. (2015, July 5). The Rise of Workplace Spying. The Week. https://theweek.com/articles/564263/rise-workplace-spying

[123] McGregor, J. (2018, July 12). Analysis | What Walmart's patent for audio surveillance could mean for its workers. Washington Post. https://www.washingtonpost.com/business/2018/07/12/what-walmarts-patent-audio-surveillance-could-mean-its-workers/

[124] Mosendz, P., & Melin, A. (2020, March 27). Bosses are panic-buying spy software to keep tabs on remote workers. Los Angeles Times. https://www.latimes.com/business/technology/story/2020-03-27/coronavirus-work-from-home-privacy

[125] Jones, L. (2020, September 29). "I monitor my staff with software that takes screenshots." BBC News. https://www.bbc.com/news/business-54289152

[126] Ibid.

[127] Cyphers & Gullo, Inside the Invasive, Secretive "Bossware" Tracking Workers.

[128] Hughes, O. (2021, February 17). More bosses are using software to monitor remote workers. Not everyone is happy about it. ZDNet. https://www.zdnet.com/article/more-bosses-are-using-software-to-monitor-remote-workers-not-everyone-is-happy-about-it/

[129] Ballard, B. (2021, January 19). One in five firms admit to illegally spying on employees working from home. TechRadar. https://www.techradar.com/uk/news/one-in-five-firms-admit-to-illegally-spying-on-employees-working-from-home

[130] Isaak, A. (2020, June 17). Employee tracking is increasingly widespread, and it could be doing more harm than good. CNBC. https://www.cnbc.com/2020/06/17/employee-surveillance-software-is-seeing-a-spike-as-workers-stay-home.html

[131] Hanley & Hubbard, Eyes Everywhere.

[132] Ibid.

[133] Ibid.

[134] Migliano, S. (2020). Employee Surveillance Software Demand up 58% Since Pandemic Started. Top10VPN. https://www.top10vpn.com/research/covid-employee-surveillance/

[135] Ibid.

[136] Ibid.

[137] Baker, M. (2020, June 8). 9 Future of Work Trends Post-COVID-19. Gartner. https://www.gartner.com/smarterwithgartner/9-future-of-work-trends-post-covid-19/

[138] Brown, E. (2020, November 16). Employee surveillance software demand increased as workers transitioned to home working. ZDNet. https://www.zdnet.com/article/employee-surveillance-software-demand-increased-as-workers-transitioned-to-home-working/

[139] Holmes, A. (2020, March 23). Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working—And the service is seeing a rapid expansion since the coronavirus outbreak. Business Insider. https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3

[140] Ibid.

[141] Ibid.

[142] Solon, O. (2017, November 6). Big Brother isn't just watching: Workplace surveillance can track your every move. The Guardian. https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology

[143] Walker, P. (2021, April 21). Call centre firm tells UK homeworkers they will not be watched with webcam. The Guardian. http://www.theguardian.com/business/2021/apr/21/call-centre-teleperformance-tells-homeworkers-they-will-not-be-watched-webcam

[144] Ibid.

[145] Ibid.

[146] Walker, P. (2021, March 26). "Missing from desk": AI webcam raises remote surveillance concerns. The Guardian. http://www.theguardian.com/business/2021/mar/26/missing-from-desk-ai-webcam-raises-remote-surveillance-concerns

[147] Working from home surveillance software for your boss. (2020, April 30). Washington Post. https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

[148] Migliano, Employee Surveillance Software Demand up 58% Since Pandemic Started.

[149] Ibid.

[150] Solon, Big Brother isn't just watching.

[151] Migliano, Employee Surveillance Software Demand up 58% Since Pandemic Started.

[152] Bednar, V. (2020, August 18). Vass Bednar: Your boss is watching you while you work. The National Post. https://nationalpost.com/opinion/vass-bednar-your-boss-is-watching-you-while-you-work

[153] Ibid.

[154] Solon, Big Brother isn't just watching.

[155] Keane, J. (2021, March 10). Fujitsu designs facial recognition to track workers' concentration. Silicon Republic. https://www.siliconrepublic.com/machines/fujitsu-facial-recognition-workers-concentration

[156] Ibid.

[157] Webber, A. (2020, June 16). PwC facial recognition tool criticised for home working privacy invasion. Personnel Today. https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion/

[158] Ibid.

[159] Is your boss watching you? Widespread computer surveillance of remote workers 'worrisome on a bunch of levels.' (2021, February 27). Mimicnews. https://mimicnews.com/is-your-boss-watching-you-widespread-computer-surveillance-of-remote-workers-worrisome-on-a-bunch-of-levels

[160] Ibid.

[161] Ibid.

[162] Ibid.

[163] Migliano, Employee Surveillance Software Demand up 58% Since Pandemic Started.

[164] Burt, C. (2020, August 13). Concentrix launches remote work platform with facial biometric authentication for CX industry. Biometricupdate.Com. https://www.biometricupdate.com/202008/concentrix-launches-remote-work-platform-with-facial-biometric-authentication-for-cx-industry

[165] Haubursin, C. (2017, November 20). Automation is coming for truckers. But first, they're being watched. Vox. https://www.vox.com/videos/2017/11/20/16670266/trucking-eld-surveillance

[166] Catarevas, M. (2019, February 25). Reefer Sadness: a long-haul driver's ELD lament. American Trucker. https://www.trucker.com/regulations/article/21747683/reefer-sadness-a-longhaul-drivers-eld-lament

[167] Haubursin, C. (2017, November 20). Automation is coming for truckers. But first, they're being watched. Vox. https://www.vox.com/videos/2017/11/20/16670266/trucking-eld-surveillance

[168] Charbonneau & Doberstein, An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector.

[169] McCallum, Remote Controlled Workers.

[170] QuickBooks Canada Team. (2021, February 19). How Canadian Employees Feel about GPS Tracking in the Workplace. QuickBooks Canada. https://quickbooks.intuit.com/ca/resources/time-tracking/how-canadian-employees-feel-about-gps-tracking-in-the-workplace/

[171] Charbonneau & Doberstein, An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector.

[172] Crossover. (2019, May 23). What is Deep Work and how can it push capabilities to the limit? Medium. https://medium.com/@crossoverforwork/what-is-deep-work-and-how-can-it-push-capabilities-to-the-limit-998c14d65dc7

[173] Finnegan, M. (2020, October 29). The New Normal: When work-from-home means the boss is watching. Computerworld. https://www.computerworld.com/article/3586616/the-new-normal-when-work-from-home-means-the-boss-is-watching.html

[174] Ibid.

[175] Fortson, D. (2021, January 3). Is your employer spying on you as you work from home? The Times. https://www.thetimes.co.uk/article/is-your-employer-spying-on-you-as-you-work-from-home-5pdglfpp0

[176] Manokha, I. (2020). Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic. Political Anthropological Research on International Social Sciences (PARISS), 1(2), 273–287. https://doi.org/10.1163/25903276-BJA10009

[177] Heaven, W. D. (2020, June 4). This startup is using AI to give workers a "productivity score." MIT Technology Review. https://www.technologyreview.com/2020/06/04/1002671/startup-ai-workers-productivity-score-bias-machine-learning-business-covid/

[178] Mackie, K. (2020, December 1). Microsoft Pulls Productivity Score Feature After Privacy Concerns. Redmond Channel Partner. https://rcpmag.com/articles/2020/12/01/microsoft-productivity-score-privacy.aspx

[179] Ibid.

[180] Hern, A. (2020, November 26). Microsoft productivity score feature criticised as workplace surveillance. The Guardian. http://www.theguardian.com/technology/2020/nov/26/microsoft-productivity-score-feature-criticised-workplace-surveillance

[181] Mackie, Microsoft Pulls Productivity Score Feature After Privacy Concerns.

[182] Microsoft 365 admin. (2021, July 12). Microsoft Productivity Score. Microsoft Documentation. https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/productivity-score

[183] Ibid.

[184] Amatulli, J. (2020, March 25). Zoom Can Track Who's Not Paying Attention In Your Video Call. Here's How. HuffPost. https://www.huffpost.com/entry/zoom-tracks-not-paying-attention-video-call_l_5e7b96b5c5b6b7d80959ea96

[185] Ibid.

[186] Attendee attention tracking. (2021, January 11). Zoom Help Center. https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking

[187] McCallum, Remote Controlled Workers.

[188] Cox, D. (2020, November 10). The rise of employee health tracking. BBC. https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking

[189] Ibid.

[190] Lynn, S. (2020, May 23). As employee monitoring extends to workers' homes and health, some see civil rights threat. ABC News. https://abcnews.go.com/US/employee-monitoring-extends-workers-homes-health-civil-rights/story?id=70665085

[191] Nguyen, A. (2020). New Digital Infrastructures of Workplace Health and Safety (Watching the Watchers: The New Frontier of Privacy and Surveillance under COVID-19). Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/new-digital-infrastructures-of-workplace-health-and-safety

[192] Putzier, K., & Cutter, C. (2020, May 5). Welcome Back to the Office. Your Every Move Will Be Watched. The Wall Street Journal. https://www.wsj.com/articles/lockdown-reopen-office-coronavirus-privacy-11588689725

[193] Ibid.

[194] Nguyen, New Digital Infrastructures of Workplace Health and Safety.

[195] Porter, B. (2020, June 16). Amazon introduces "Distance Assistant." About Amazon. https://www.aboutamazon.com/news/operations/amazon-introduces-distance-assistant

[196] Naughton, K. (2020, April 15). "Ford Tests Buzzing Wristbands to Keep Workers at Safe Distances." Bloomberg. https://www.bloomberg.com/news/articles/2020-04-15/ford-tests-buzzing-distancing-wristbands-to-keep-workers-apart

[197] Putzier & Cutter, Welcome Back to the Office.

[198] Ibid.

[199] Nguyen, New Digital Infrastructures of Workplace Health and Safety.

[200] Windwehr, K. R. and S. (2020, September 10). Workplace Surveillance in Times of Corona. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/09/workplace-surveillance-times-corona

[201] Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extra role performance. Journal of Applied Psychology, 91, 221–232

[202] Varca, P. E. (2006). Telephone surveillance in call centers: Prescriptions for reducing strain. Managing Service Quality: An International Journal, 16, 290–305. https://www.doi.org/10.1108/09604520610663507

[203] Lockwood, G. (2018), 'Workplace monitoring and surveillance: The British context', Athens Journal of Law, Vol.4, No. 3, pp. 205–228, cited by Riso, S. (2020). Employee monitoring and surveillance: The challenges of digitalisation. Publications Office of the European Union. https://www.eurofound.europa.eu/publications/report/2020/employee-monitoring-and-surveillance-the-challenges-of-digitalisation

[204] Douthitt, E. A., & Aiello, J. R. (2001). The role of participation and control in the effects of computer monitoring on fairness perceptions, task satisfaction, and performance. Journal of Applied Psychology, 86, 867–874.10.1037/0021-9010.86.5.867

[205] Martin, A. J., Wellen, J. M., & Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. International Journal of Human Resource Management, 27(21), 2635–2651. https://doi.org/10.1080/09585192.2016.1225313

[206] Ibid.

[207] Chory, Vela & Avtgis. Organizational Surveillance of Computer-Mediated Workplace Communication.

[208] Ibid.

[209] Martin, Wellen & Grimmer, An eye on your work.

[210] Chory, Vela & Avtgis, Organizational Surveillance of Computer-Mediated Workplace Communication

[211] Ball & Margulis, Electronic monitoring and surveillance in call centres,

[212] Ibid, 120.

[213] Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. Journal of Management, 46(1), 100–126. https://doi.org/10.1177/0149206319869435

[214] Charbonneau & Doberstein, An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector.

[215] Ball & Margulis, Electronic monitoring and surveillance in call centres.

[216] Boland, H. (2020, August 11). Meet the workers fighting back against bosses who spy on them while working from home. Telegraph.Co.Uk. https://www.telegraph.co.uk/technology/2020/08/11/meet-workers-fighting-back-against-bosses-spy-working-home/

[217] McParland & Connolly, Dataveillance in the Workplace.

[218] Anteby, M., & Chan, C. K. (2018). A Self-Fulfilling Cycle of Coercive Surveillance: Workers' Invisibility Practices and Managerial Justification. Organization Science, 29(2), 247–263. https://doi.org/10.1287/orsc.2017.1175

[219] Ibid.

[220] Boland, Meet the workers fighting back against bosses who spy on them while working from home.

[221] Riso, Employee monitoring and surveillance.

[222] Bernd, Abu-Salma & Frik, Bystanders' privacy.

[223] Ibid.

[224] Cyphers & Gullo, Inside the Invasive, Secretive "Bossware" Tracking Workers.

[225] Nguyen, The Constant Boss.

[226] Ibid, 13.

[227] Mateescu & Nguyen, Explainer: Workplace monitoring and surveillance.

[228] Garden, C. (2018). Labor Organizing in the Age of Surveillance, St. Louis U. L.J. 55. https://digitalcommons.law.seattleu.edu/faculty/814

[229] Fierro, D. (2020, September 21). How Amazon (and Others) Spy on Workers. Lifewire. https://www.lifewire.com/how-amazon-and-others-spy-on-employees-5078745

[230] Gurley, L. K., & Cox, J. (2020, September 1). Inside Amazon's Secret Program to Spy On Workers' Private Facebook Groups. Vice. https://www.vice.com/en/article/3azegw/amazon-is-spying-on-its-workers-in-closed-facebook-groups-internal-reports-show

[231] Anderson, Blumenfeld & Hooper, A question of trust.

[232] Ibid.

[233] UN General Assembly (1966, December 19), International Covenant on Civil and Political Rights, United Nations, Treaty Series, vol. 999, 171, https://www.refworld.org/docid/3ae6b3aa0.html

[234] American Declaration of the Rights and Duties of Man, (1948). https://www.oas.org/dil/access_to_information_human_right_American_Declaration_of_the_Rights_and_Duties_of_Man.pdf

[235] Forest, G. V. L. (2005). The Offices of The Information And Privacy Commissioners: The Merger and Related Issues. Department of Justice. https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p2.html

[236] Canadian Charter of Rights and Freedoms, s 7, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html

[237] Canadian Charter of Rights and Freedoms, s 8, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html

[238] R. v. Dyment, (1988) 2 S.C.R. 417 at 427-28.

[239] Canadian Charter of Rights and Freedoms, s 32(1), Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art321.html

[240] Morgan, C. (1999). Employer Monitoring of Employee Electronic Mail and Internet Use, 44-2 McGill Law Journal 849, 1999 CanLIIDocs 51, https://canlii.ca/t/2bdd

[241] R. v. Dyment, 1988 CanLII 10 (SCC), 2 SCR 417, (1988), https://canlii.ca/t/1ftc6

[242] Ibid.

[243] Ibid.

[244] R. v. Morelli, (2010), SCC 8 (CanLII), 1 SCR 253, https://canlii.ca/t/28mrg

[245] R. v. Cole, (2012) SCC 53 (CanLII), 3 SCR 34, https://canlii.ca/t/ft969

[246] Canadian Charter of Rights and Freedoms, s 8.

[247] Geist, M. A. (2003), "Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance," 82:2 Can B Rev 151

[248] Canadian Charter of Rights and Freedoms, s 8.

[249] Ibid.

[250] R. v. Duarte, 1990 CanLII 150 (SCC), (1990) 1 SCR 30, https://canlii.ca/t/1fszz

[251] Geist, "Computer and E-Mail Workplace Surveillance in Canada."

[252] Syndicat des employées et employés du C.L.S.C. Les Forges et Centre local de services communautaires Les Forges (M. Gérard Forget), 1997 CanLII 22524 (QC SAT), (1997), https://canlii.ca/t/hnk53

[253] Privacy Act, RSC 1985, c P-21, (1985), https://canlii.ca/t/543hl

[254] Ibid.

[255] Ibid. Section 5(1-2)

[256] Ibid. Section 5(3)

[257] Ibid.

[258] Ibid.

[259] Directive on Automated Decision-Making, (2019). https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

[260] Ibid.

[261] Treasury Board of Canada Secretariat. (2021, March 22). Algorithmic Impact Assessment Tool [Guidance]. Government of Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

[262] Directive on Automated Decision-Making.

[263] Ibid.

[264] Ibid.

[265] Ibid.

[266] Office of the Privacy Commissioner of Canada. (2020, March). Expectations: OPC's Guide to the Privacy Impact Assessment Process. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

[267] Office of the Privacy Commissioner of Canada. (2016, March 7). Top Ten Dos and Don'ts for Privacy Impact Assessments. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_59_pia/

[268] Office of the Privacy Commissioner of Canada. (2021). Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology). Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1

[269] Ibid.

[270] Office of the Privacy Commissioner of Canada. (2004, November 5). Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/ .

[271] Office of the Privacy Commissioner of Canada. (2014, May 15). Summary of privacy laws in Canada. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2-2

[272] Ibid.

[273] PIPEDA s. 5(3)

[274] Office of the Privacy Commissioner of Canada. (2019, May). PIPEDA fair information principles. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[275] Ibid.

[276] PIPEDA, Schedule 1 Principle 9

[277] PIPEDA, s. 4.3 of Schedule 1

[278] Office of the Privacy Commissioner of Canada. (2020, August). PIPEDA Fair Information Principle 4 – Limiting Collection. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_collection/

[279] Office of the Privacy Commissioner of Canada. (2020, August). PIPEDA Fair Information Principle 3 – Consent. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/

[280] PIPEDA, s. 7(1)(a)

[281] PIPEDA, s. 7(1)(a-b)

[282] PIPEDA, s. 7(1)(b.2); see e.g. https://www.fasken.com/en/knowledge/2015/07/privacyampinformationprotectionbulletin-20150706

[283] Office of the Privacy Commissioner of Canada. (2020, April 22). Types of dispositions. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/def-cf/

[284] Surveillance of employees at work, 2004 CanLII 52849 (PCC), (2004), https://canlii.ca/t/1jvxj

[285] Video surveillance cameras at food processing plant questioned, 2005 CanLII 15490 (PCC), (2005), https://canlii.ca/t/1kfv1

[286] Eastmond v. Canadian Pacific Railway, 2004 FC 852 (CanLII), (2004), https://canlii.ca/t/1hclc

[287] Office of the Privacy Commissioner of Canada. (2010, July 21). Collection and use of employee's email deemed acceptable for purposes of investigating breach of agreement. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-019/

[288] Ibid.

[289] Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2nd Session, 43rd Parliament, 2020. https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

[290] Therrien, D. (2021). Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/

[291] For example, see s. 6(4)(d) which states that the CPPA does not apply to "any organization in respect of an individual's personal information that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession", which warrants clarity in terms of when this provision applies.

[292] CPPA s. 23

[293] Stevens, Y., & Solomun, S. (2021). Facing the Realities of Facial Recognition Technology: Recommendations for Canada's Privacy Act. Cybersecure Policy Exchange. https://www.cybersecurepolicy.ca/frt-privacy-act

[294] CPPA s. 63(3)

[295] See for example sections 70(1), which concerns revealing information about other individuals, and 70(7)(b), which concerns revealing confidential commercial information.

[296] CPPA, s. 2.

[297] CPPA, s. 22

[298] CPPA, s. 39

[299] Rocher, L., Hendrickx, J.M. & de Montjoye, YA. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069. https://doi.org/10.1038/s41467-019-10933-3

[300] Canada Labour Code, RSC 1985, c L-2, https://canlii.ca/t/54wgb

[301] Kniss v. Canada (Privacy Commissioner), 2013 FC 31 (CanLII), https://canlii.ca/t/fvt9j

[302] Office of the Privacy Commissioner of Canada. (2020, June 11). Provincial and territorial privacy laws and oversight. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

[303] Office of the Privacy Commissioner of Canada. (2020, June 11). Provincial and territorial privacy laws and oversight. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

[304] Personal Information Protection Act, s 13, SBC 2003, c 63, (2003), https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01#section13

[305] Personal employee information. (n.d.). Government of Alberta. Retrieved August 9, 2021, from https://www.alberta.ca/personal-employee-information.aspx

[306] Personal Information Protection Act, s 13, SBC 2003, c 63.

[307] Personal employee information. (n.d.). Government of Alberta

[308] Personal Information Protection Act, s 13, SBC 2003, c 63.

[309] Morgan, C. (1999). Employer Monitoring of Employee Electronic Mail and Internet Use, 44-2 McGill Law Journal 849, 1999 CanLIIDocs 51, https://canlii.ca/t/2bdd

[310] Charter of Human Rights and Freedoms, CQLR c C-12

[311] Civil Code of Québec, CQLR c CCQ-1991

[312] Civil Code of Québec, CQLR c CCQ-1991, s 36.

[313] Act respecting the protection of personal information in the private sector, CQLR c P-39.1, https://canlii.ca/t/5534s at s. 5.

[314] Act respecting the protection of personal information in the private sector, CQLR c P-39.1, https://canlii.ca/t/5534s at s. 8.

[315] Morgan, C., Joizil,, K., Trottier, M., Bherer, K., & Chen. E.Y. (2020, June 19). Bill 64: An Overhaul of Quebec's Privacy Law Regime – Implications for Business. McCarthy Tetrault TechLex. https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business..

[316] Pamphile et Sobeys Québec inc., 2016 QCTAT 1670 (CanLII), (2016), https://canlii.ca/t/gnxjc as cited in Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (csn) c. Trudeau, 1999 CanLII 13295 (QC CA), (1999), https://canlii.ca/t/1mvsx

[317] Jones v. Tsige, 2012 ONCA 32 (CanLII), (2012), https://canlii.ca/t/fpnld

[318] Barbara von Tigerstrom, Direct and Vicarious Liability for Tort Claims Involving Violation of Privacy, 2018 96-3 The Canadian Bar Review 539, 2018 CanLIIDocs 295, (2018), https://canlii.ca/t/2d96

[319] Scassa, T. (2021, Jun 8). Privacy in the precision economy: the rise of AI-enabled workplace surveillance during the pandemic. CIGI. https://www.cigionline.org/articles/privacy-in-the-precision-economy-the-rise-of-ai-enabled-workplace-surveillance-during-the-pandemic/?s=09

[320] Villeneuve, S., & Elias, D. (2020, September 2). Surveillance Creep: Data collection and privacy in Canada during COVID-19. Brookfield Institute for Innovation + Entrepreneurship. https://brookfieldinstitute.ca/surveillance-creep-data-collection-and-privacy-in-canada-during-Covid-19

[321] Lyon, D. (2001). Surveillance after September 11. Sociological Research Online, 6(3), 116–121.

[322] Masoodi, J. (2020, March 23). Police and governments may increasingly adopt surveillance technologies in response to coronavirus fears. The Conversation. https://theconversation.com/police-and-governments-may-increasingly-adopt-surveillance-technologies-in-response-to-coronavirus-fears-133737

[323] Ball & Margulis, Electronic monitoring and surveillance in call centres.

[324] Ibid.

[325] Scassa, Privacy in the precision economy.

[326] Ball, Workplace surveillance.

[327] Fierro, How Amazon (and Others) Spy on Workers.

[328] Asher-Schapiro, Amazon AI van cameras spark surveillance concerns.

[329] Scassa, Privacy in the precision economy.

[330] Geist, "Computer and E-Mail Workplace Surveillance in Canada."

[331] Forcese, C. (2011, July). The limits of reasonableness: the failures of the conventional search and seizure paradigm in information-rich environments. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/forcese_201107/

[332] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, (2017). https://ec.europa.eu/newsroom/article29/items/612053/en

[333] Therrien, Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act.

[334] Scassa, T. (2020, November 18). It's not you, it's me? Why does the federal government have a hard time committing to the human right to privacy? Teresascassa.ca. https://teresascassa.ca/index.php?Itemid=80&id=333%3Ait%E2%80%99s-not-you-it%E2%80%99s-me%3F-why-does-the-federal-government-have-a-hard-time-committing-to-the-human-right-to-privacy%3F&option=com_k2&view=item

[335] Cofone, I. (2020, November). Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/

[336] Morgan, C. S., Gillis, M., & Thompson, K. (2018, March 31). Parliamentary Committee Recommends Substantial Revisions to PIPEDA – Part 4 – Enforcement Powers. McCarthy Tétrault. https://www.mccarthy.ca/en/insights/blogs/snipits/parliamentary-committee-recommends-substantial-revisions-pipeda-part-4-enforcement-powers

[337] Ibid.

[338] Office of the Privacy Commissioner of Canada. (2020, November 12). A Regulatory Framework for AI: Recommendations for PIPEDA Reform. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

[339] Ibid.

[340] Knorr, E. (2021). CSO Global Intelligence Report: The State of Cybersecurity in 2021. IDG Communications, In. https://www.csoonline.com/article/3627274/cso-global-intelligence-report-the-state-of-cybersecurity-in-2021.html

[341] Anderson, Blumenfeld & Hooper, A question of trust.

[342] Schiebinger, L., Klinge, I., Sánchez de Madariaga, I., Paik, H. Y., Schraudner, M., and Stefanick, M. (Eds.) (2011-2021). Facial Recognition: Analyzing Gender and Intersectionality in Machine Learning. Gendered Innovations in Science, Health & Medicine, Engineering and Environment. https://genderedinnovations.stanford.edu/case-studies/facial.html#tabs-2

[343] Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81:1-15. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[344] Ball, Daniel & Stride, Dimensions of employee privacy.

[345] Stark, Stanhaus & Anthony, "I Don't Want Someone to Watch Me While I'm Working."

[346] Gellman, B., & Adler-Bell, S. (2017). The Disparate Impact of Surveillance. The Century Foundation. https://tcf.org/content/report/disparate-impact-surveillance/

[347] The Color of Surveillance: Government Monitoring of American Immigrants. (2017, June 22). Georgetown Law. https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/

[348] Dodd, V. (2019, January 26). Met police "disproportionately" use stop and search powers on black people. The Guardian. http://www.theguardian.com/law/2019/jan/26/met-police-disproportionately-use-stop-and-search-powers-on-black-people

[349] Nguyen, The Constant Boss.

[350] Holland, Cooper & Hecker, Electronic Monitoring and Surveillance.

[351] Scherer, M., & Brown, L. X. Z. (2021). Warning: Bossware May Be Hazardous to Your Health. Center for Democracy & Technology. https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/

[352] Rajgopal, T. (2010). Mental well-being at the workplace. Indian Journal of Occupational and Environmental Medicine, 14(3), 63–357.

[353] Rajgopal T. Mental well-being at the workplace. Indian J Occup Environ Med 2010;14:63-5

[354] Munn, Z., Peters, M.D.J., Stern, C. et al. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodology, 18(143).

[355] Chory, Vela & Avtgis. Organizational Surveillance of Computer-Mediated Workplace Communication.