RISE OF BOSSWARE

PROTECTING THE PRIVACY OF CANADIANS WHO WORK FROM HOME

Michael Coteau
Member of Parliament
Don Valley East
December 2022

This report is also available in French, and it is available electronically at www.michaelcoteau.libparl.ca

Ce rapport est également disponible en français et sous forme électronique à l'adresse www.michaelcoteau.libparl.ca

TABLE OF CONTENTS

INTRODUCTION

In 2020 the COVID-19 pandemic changed the way that Canadians lived and worked. It threatened our economy and our families – and the health of all Canadians. Thousands of lives were lost.

Against this COVID-19 backdrop, as many as 60% of Canadians began working from home – which led to increasing use of surveillance technology by employers. Technologies have included webcam monitoring and keystroke logging, to more sophisticated methods like artificial intelligence and facial recognition to rate employee performance and output.

This increase in remote work was not matched by the necessary safeguards for employees. This has made many Canadians vulnerable to invasive monitoring practices, with only patchwork legislation to offer solutions and protection.

In March 2022, I launched a process to raise awareness about the issue of employers who remotely monitor their employees, and to lead a national discussion about how to best protect workers, their privacy, and to set the rules for employers. The discussion also addressed the need to help employers to better understand their obligations across the country, to foster greater confidence and, as a result, increase business activity in Canada and competitiveness across jurisdictions.

I have heard from hundreds of Canadians, from every province and territory, on this issue. I met with privacy experts, business leaders and leading government officials who recognize that there are significant gaps in protecting the rights of Canadians who work from home.

This report briefly summarizes the issue, what we heard, and lays out a recommended course of action that will benefit people who work from home and their employers. My intention is to introduce legislation in the coming months that will facilitate a pan-Canadian framework, and introduce better protections for employees and employers alike. I am also recommending steps that the federal government and its Crown Corporations and agencies can take right away.

Of course the issue of privacy protections for people who work from home is only a small part of much larger conversations that are taking place around privacy and technology: the role and impact of Big Data, surveillance in the workplace and more broadly in our society, and the power and influence of large corporate interests and government oversight. We haven't tried to tackle all of these important issues in this consultation and report, however we are mindful that any discussion of privacy protections for remote workers must be done in the context of these larger issues.

My work on privacy protections for remote workers, and this report, would not have been possible without the help of many public officials, privacy experts, and members of the public; special thanks are due to researchers at the Parliamentary Library and to my staff, Adam Garisto, Andrew Green and Chris Sardinha who handled my frequent inquiries and kept the team on track. Bruce Davis, the project manager, and Salma El Dessouky played key roles drafting this report. Over the course of several months I also relied on an informal working group of volunteers and I would like to thank those individuals for their insights and their volunteer time.

Joe Masoodi, Joe McDonald, Christine Clayton, and Tina Derak participated in the working group and provided different viewpoints and constructive suggestions. Despite these contributions, the positions and recommendations outlined in the report are ultimately my own and do not necessarily represent the viewpoints or suggestions of the working group, or the organizations with which they may be affiliated.

At the start of my consultation process the issue of employer surveillance of employees who work from home seemed daunting, with multi-layered questions about jurisdictional issues, technologies, employer practices, and employee privacy issues. In a few short months, however, the issue and options have become clearer, leading me to make two simple recommendations outlined in this report.

The release of this report introduces what I hope will be a new phase: the drafting of a Private Member's Bill, the development of a pan-Canadian framework and tangible action by federal institutions.

I encourage my colleagues at the federal and provincial levels of government to assist in moving these privacy protections forward and I look forward to further discussions on this important issue.

Michael Coteau
Member of Parliament, Don Valley East

EXECUTIVE SUMMARY

In March, 2022, Michael Coteau, Member of Parliament for Don Valley East, launched a national public consultation to address the issue of digital surveillance by employers of Canadians who work from home.

Over the course of several months, Coteau met with privacy experts, representatives from industry, labour, government, and non-governmental sectors. Coteau also hosted a series of public town hall consultations to hear from people who work from home. Additionally, a research and literature scan was conducted to identify and extract existing opinions, findings, and recommendations in the field.

PRIVACY SURVEY

A 'Working from Home Privacy' survey received 337 responses. The survey responses indicated that most respondents would accept a degree of remote monitoring contingent on certain conditions or limitations, although a significant minority did not accept any employer monitoring of employees working from home. Overall, very few respondents thought that employers should have complete freedom to conduct surveillance as they see fit.

ROUND TABLE DISCUSSION

A roundtable discussion with experts highlighted potential concerns or risks that come with approaching the issue of digital surveillance of remote-work employees. They provided insight into the direction and structure of an effective framework. Key points to take away from our discussions were: the issue of digital surveillance of remote workers requires a high-level approach to be comprehensive; regulation and policy-making on this issue should include employee participation; regulation should promote 'privacy as default' not 'surveillance as default'; and finally, given the nature and scope of the issue, the federal government has a large role to play in creating a framework that better protects employees' privacy rights in their homes.

LITERATURE REVIEW

Many of the findings from the consultation were supported by the research and literature scan conducted for this report. Namely, that existing legislative frameworks are not comprehensive nor contemporary enough to address and regulate the proliferated use of surveillance on remote workers, whether that's at a regional or national level.

Moreover, the absence of regulation is having a palpable impact (psychological, social, and professional) on employees working from home who feel their privacy rights and job security are both threatened by the increased use of digital monitoring.

RECOMMENDATIONS

Findings from the consultation have informed the following recommendations. First, the federal government and its Crown Corporations and agencies have leadership roles to play, as employers, regulators, and purchasers of goods and services, to protect employees from unwarranted intrusion into their homes. Second, the Government of Canada and provincial and territorial governments need to negotiate a framework agreement that protects individuals in their homes where they live, regardless of their employer.

The proposed framework should establish stringent guidelines and regulations with regard to consent and transparency, reasonable/permissible uses and mechanisms of digital monitoring, the storage and activities relating to employee data and personal information, and company policies enacted to protect the rights of remote workers should employers choose to use digital monitoring. Most importantly, employees must have a participatory role in shaping the surveillance policies of their workplace when monitoring takes place in their homes as it is their rights that lie at the heart of this issue.

METHODOLOGY

In March 2022 I launched a consultation process and review of the issue of employee surveillance with six key elements:

- Online and in-person focus groups;
- Round table consultation with key privacy experts;
- Interviews with provincial privacy commissioners, government officials and legislators and experts;
- An online survey soliciting opinions on in-home monitoring;
- A review of existing research and literature in the field; and
- A review of relevant legislation or proposed legislation across Canada.

A roundtable discussion with experts highlighted potential concerns or risks that come with approaching the issue of digital surveillance of remote-work employees. They provided insight into the direction and structure of an effective framework.

The 'Working from Home Privacy Survey' provided key insights on priority issues and popular opinions among Canadians on remote work surveillance. Through a series of multiple-choice and open-ended questions, respondents were able to provide their thoughts on digital monitoring and gave us a more nuanced understanding of Canadians' opinions on the issue. The detailed survey results are outlined on my webpage at www.michaelcoteau.libparl.ca.

The consultations did present certain limitations. First, the available literature and research in the Canadian context is limited in variety and scope. This is understandable given the novelty of government-mandated lockdowns and accompanying work-from-home measures. One notable knowledge gap is the insufficiency of studies on the impacts of employee surveillance on marginalized communities and low-wage workers. Characteristics including age, gender, sexual orientation, race, (dis)ability, and income may factor into an individual's vulnerability to employee surveillance further exacerbating the power imbalance between the employer and employee.

Second, data collected from our online survey may present a risk of bias. Distribution of the survey took place at the various town halls, on social media platforms and through personal connections and networks. This would assume that predominantly like-minded individuals with concerns about digital monitoring responded to the survey. Moreover, it is more likely that those who felt strongly about in-home employee monitoring responded to the survey.

As a result, the online survey is not considered statistically significant, but it provides valuable directional feedback and qualitative insights on the nuances of the issue.

OVERVIEW

Employee surveillance is not new. With time, however, workplace surveillance practices have evolved, increasingly facilitated by digital technologies and accelerated as the world saw a great shift to remote work.

As many as 60% of Canadians started to work from home since the onset of the pandemic.[1] It is expected that as many as 40% of employment positions will remain permanently at home even after the pandemic ends.[2] As a result, the surveillance practices ordinarily relegated to the workplace have increasingly moved into workers' homes. Such practices raise many questions, including on employee rights and the extent to which they are protected amidst this sharp emergence of in-home digital monitoring.

While the shift in working from home was happening, COVID-19 also changed family and personal life: parents working while they also managed their children's remote learning, while they struggled to manage family responsibilities, individuals coping with the stress of isolation and with sickness. These family and personal responsibilities were potentially done all while under the scrutiny of the employer. This is germane to our discussions because employer monitoring of home workspaces had the potential to also capture unwitting family members, it had the potential to catch people under considerable stress and poor health. It had the potential to exacerbate the stress of lockdown measures by allowing employers and work colleagues to intrude into the private life and space of Canadians.

> *As many as 60% of Canadians started to work from home since the onset of the pandemic.*

Recent innovations in technology have also introduced new, more intrusive forms of surveillance systems. Such technologies are increasingly relying on various types of data to monitor workers, and are increasingly being equipped with Artificial Intelligence (AI) to automate monitoring, and in some cases, even evaluate the performance of individual

1 PricewaterhouseCoopers. (2021). *Canadian Office Worker Survey 2021*. PwC. Retrieved from https://www.pwc.com/ca/en/today-s-issues/upskilling/surveys/office-workers-survey-2021-canadian-outlook.html

2 Mehdi, T., & Morissette, R. (2021, October 27). *Working from home in Canada: What have we learned so far?* Retrieved from https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021010/article/00001-eng.htm

workers. They record and track keystrokes, facial features and eye movements (e.g., biometric data), and a person's location. Such software can monitor personal information like emails, texts, and passwords and even detect an employee's mood, tone, or attitude.[1] [2] The software, Hubstaff, for instance, can capture screen activity that can be customized for each person, reporting once, twice or three times per 10 minute increments at the employer's discretion.[3]

As technology advances, there are a lot of grey areas where privacy, data protection, and transparency are concerned. In most cases, jurisdictions provide that such monitoring is legally permissible, and often leave the limits of monitoring to the discretion of employers.[4] Thus, the limits of in-home employee monitoring are not well or consistently defined. With the wide range of surveillance tools at an employer's disposal, a great deal of authority is placed in their hands. The nature of this type of monitoring raises concerns including whether such surveillance should take place in the first place, but also on transparency. In some cases of digital monitoring, individuals may not be aware of the extent of monitoring or whether it is happening at all.

1 West, D. M. (2022, March 9). *How Employers Use Technology to Surveil Employees.* Brookings. Retrieved from https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/

2 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

3 Blackman, R. (2021, Aug 30). *How to Monitor Your Employees - While Respecting Their Privacy.* Harvard Business Review. Retrieved from https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy

4 Hunter, T. (2021, October 4). *Here Are All the Ways Your Boss Can Legally Monitor You.* The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2021/08/20/work-from-home-computer-monitoring/

JURISDICTIONAL SCAN

At the moment, there is no provincial, territorial or federal legislation in Canada dealing specifically with work-from-home surveillance. Rather, there is a patchwork of legislation that inadequately protects the privacy of individuals in today's data-driven society, including those working from home. Thus, employers across Canada are left trying to navigate this patchwork.

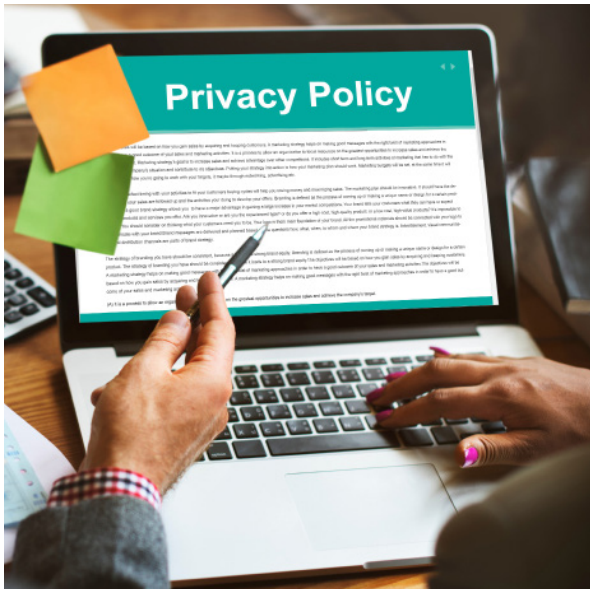
The following is a scan of the various legislation in place protecting privacy rights in the face of surveillance.

FEDERAL LEGISLATION

At the federal level, Canada's framework governing privacy, data handling (e.g., data collection, use, disclosure) and surveillance consist of the following most notable documents:

- Personal Information Protection and Electronic Documents Act (PIPEDA),
- Privacy Act (PA),
- Canadian Charter of Rights and Freedoms, and
- Criminal Code of Canada (CCC).

Collectively, these statutes deal with the protection of privacy, define harmful data collection and acknowledge a person's right to an inherent value of freedom from surveillance. However, these statutes and the Charter come with limitations, whether with respect to jurisdiction, the availability of loopholes, or in some cases, leaving generous room for interpretation. For instance, the protection of privacy rights under PIPEDA only covers federally regulated organizations that conduct business in Canada – a mere 10% of all employees across Canada and even fewer who work from home.



Moreover, while the Charter protects a person's right "to be secure against unreasonable search and seizure", it too does not bind private actors.[1]

Looking to recent bills, like Bill C-11 the **Digital Charter Implementation Act, 2020**, and Bill C-27 **An Act to enact the CPPA, the PIDPTA, and the AIDA and to make consequential and related amendments to other Acts**, we see the potential to overcome these limitations. These Bills aimed to introduce a modernized legislative regime and to provide greater protection of privacy rights in the private sector.[2]

While Bill C-11 did not pass prior to the last election, a significant portion of it was transferred over to the current Bill C-27, which if passed, would introduce more stringent regulations that would subsequently/indirectly better protect the privacy rights of employees who work from home. Some of the more pertinent changes called for by the Bill include greater transparency when using automated decision systems; enhancing information made available to individuals as a condition for informed consent; and preventing the collection or use of data or personal information from an individual's electronic device.[3] However, as much as Bill C-27 pushes to modernize privacy laws, it ultimately accepts the use of surveillance by employers with the mere condition of enhancing transparency.

PROVINCIAL AND TERRITORIAL LEGISLATION

The **Personal Information Protection Act** (PIPA) is provincial legislation that protects an individual's privacy rights in provincially regulated private sector organizations and goes further than PIPEDA in many respects regarding the collection, use and disclosure of personal information. PIPA and similar private-sector privacy laws have been adopted by British Columbia, Alberta, and Québec, with Québec being the most comprehensive and rigorous insofar as protecting privacy rights.

Québec's National Assembly introduced Bill 64, making significant amendments

1 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

2 Department of Justice, Government of Canada. (2021, September 1). Charter statement Bill C-11: An act to enact the consumer privacy protection act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other acts. Government of Canada, Department of Justice, Electronic Communications. Retrieved from https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html

3 McCorkindale, V., & Williams, S. T. (2022, June 21). *Modernizing Canada's privacy laws: What employers need to know about Bill C-27.* Hicks Morley. Retrieved from https://hicksmorley.com/2022/06/21/modernizing-canadas-privacy-laws-what-employers-need-to-know-about-bill-c-27/

to the province's private sector privacy act, **An Act Respecting the Protection of Personal Information in the Private Sector**. This is Québec's primary legislative instrument governing the collection, use, and disclosure of personal information and protects the privacy rights conferred by articles 35 to 40 of the **Civil Code of Québec**. Bill 64, which passed on September 21st, 2021, introduces new privacy obligations for business organizations in Québec, addresses many of the weaknesses and gaps of the previous version of the Act and it presents new enforcement measures, unlike many privacy laws, including PIPEDA, that do not enforce compliance.[1] Most importantly, it prioritizes protecting employee privacy rights while minimizing employer liberties with surveillance – emphasizing 'privacy by default'. As such, Québec's approach to regulating surveillance in the digital age emulates the worker-centred regulation we hope to achieve for employees who work from home.

The government of Ontario recently introduced **Bill 88, the Working for Workers Act (2022)**, which, among its provisions, requires employers with 25 employees or more, to provide a written policy on how, when, and for what purposes employees are electronically monitored. Although a step in the right direction, the Act has several limitations, not least of which include applying only in workplaces with 25 or more employees. The Act also lacks recourse should employees believe unreasonable surveillance is taking place.

INTERNATIONAL EXAMPLES

Internationally, there are several jurisdictions that have passed laws in the face of increasing digital surveillance.

The **UN Declaration of Human Rights (1948)**, reinforces the protection of an individual's right to privacy. Article 12 of the declaration states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [2]

In 2013 the UN General Assembly adopted a resolution to protect the right to privacy in

1 *Bill 64 enacted: Québec's Modern Privacy Regime.* McMillan LLP. (2021, October 15). Retrieved from https://mcmillan.ca/insights/bill-64-enacted-quebecs-modern-privacy-regime/

2 UN General Assembly. (1948) UN Declaration of Human Rights, 217 A (III). United Nations. Article 12. Retrieved from https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

the context of digital communication, surveillance, and data collection.[1] Since then, the United Nations High Commissioner for Human Rights has published a series of reports identifying and clarifying principles, standards, and best practices regarding the protection of the right to privacy in the ever-transforming digital age.[2]

In Australia, we see unique and innovative legislation through the **Workplace Surveillance Act NSW (2005)**, which offers a high degree of employee protection from monitoring and surveillance, controlling when and to what extent an employer can monitor their employees.[3] In Europe, the **General Data Protection Regulation of the European Union** goes beyond most existing legislation and acknowledges that worker notification and consent are limited in practice due to the significant power imbalances between employees and employers.[4]

These examples illustrate both the opportunities as well as the deficiencies of legislative frameworks dealing with privacy rights and surveillance. We draw on such examples because they provide valuable lessons in shaping a framework to protect employees who work from home. Key themes to take away from these lessons are the need for a worker-centred, rights-based framework; an emphasis on accountability and enforcement of regulation; and most importantly, that in order for regulation to be effective, it must be comprehensive and consistent in application.

1 UN News. (2013, December 19). *General Assembly backs right to privacy in digital age.* UN news. United Nations. Retrieved from https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age

2 UN General Assembly. (2018). *Report on the right to privacy in the digital age.* United Nations High Commissioner for Human Rights. Retrieved from https://www.ohchr.org/en/calls-for-input/reports/2018/report-right-privacy-digital-age.

3 Ellis, W. (2021, April 6). *Workplace Surveillance Act NSW .* Privacy Australia. Retrieved from https://privacyaustralia.net/workplace-surveillance-act-nsw/

4 West, D. M. (2022, March 9). *How Employers Use Technology to Surveil Employees.* Brookings. Retrieved from https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/

WHAT WE HEARD

Privacy Experts

Between May and June, I reached out to privacy officials from provincial and territorial governments across Canada. Several of these officials agreed to one-on-one conversations with me to discuss the issue of work-from-home surveillance and how this issue can be addressed through legislation in the Canadian context.

Similar themes emerged from each of the 45-minute conversations with these privacy officials, and each province shared their own unique perspectives of the issue of digital monitoring of employees working from home.

One deputy commissioner suggested that what is needed from legislation is clarity, especially with respect to where remote-work employees and their privacy rights stand. One commissioner remarked that lack of clarity produces lengthy and cumbersome conflict resolution processes, suggesting that a framework is not only needed to guide the use of digital monitoring but that it should also clearly outline the protocols for dispute resolution surrounding surveillance activities as well. The commissioner further remarked that good privacy law has good regulators and oversight, facilitating harmony by clearly delegating roles and responsibilities. One territorial commissioner provided a more detailed insight and urged that you must have an authorized purpose guiding the use of digital monitoring and that such a purpose should be constantly evaluated. Building on this idea was one province's promotion of the 'privacy impact assessment' to evaluate whether the collection, use or disclosure of personal information through use of the tools and software being used for surveillance would be compliant with the applicable federal or provincial privacy laws. Behind these two remarks is the general principle that anything that may potentially breach the privacy rights of workers should be under constant scrutiny to minimize the possibility of injury.

Demonstrated through these conversations, the need to update digital privacy legislation is a pertinent and ongoing discussion among the Privacy Commissioners across Canada. As themes like harmony, clarity, and purpose play into how digital privacy legislation takes shape, it is important that these themes capture not only the general Canadian worker population but also the unique circumstances and challenges of employees working from home.

Round Table Discussions

On May 24th, 2022, our team convened a round table discussion with privacy experts to discuss the issue of employers using surveillance technology to monitor employees who work from home, but our facilitated session very quickly moved into a discussion of how remote work surveillance is a manifestation of a larger surveillance problem.

Round Table Participants

Adam Molnar, PhD, Assistant Professor of Sociology and Legal Studies at the University of Waterloo. Adam's research involves interdisciplinary approaches to technologies of surveillance, privacy, and strategies of regulatory governance.

Bianca Wylie, writer, with a dual background in technology and public engagement. Bianca is a partner at Digital Public and the co-founder of Tech Reset Canada. She worked for several years in the tech sector in operations, infrastructure, corporate training, and product management.

Debra Mackinnon, PhD, Assistant Professor at Lakehead University. Debra's research interests include surveillance studies, urban studies, critical criminology, science and technology studies, smart cities, wearables and qualitative research methodologies.

Joe Masoodi, Senior Policy Analyst at Toronto Metropolitan University. Joe's research interests are situated at the intersection of data security, privacy, and surveillance. As part of this project, he is leading a national survey on remote work surveillance practices across work industries in Canada.

Valerie Steeves, PhD, Full Professor in the Department of Criminology at the University of Ottawa. Her main area of research is human rights and technology issues. Dr. Steeves has written and spoken extensively on privacy from a human rights perspective and is an active participant in the privacy policy-making process in Canada.

KEY TAKEAWAYS

The expert panel highlighted the following key considerations going forward with a framework:

01 It is important to preserve a high-level focus. This is an issue that impacts nearly all Canadian workers, whether they work from home or not. As such, a framework needs to be inclusive of all individuals impacted by this issue, and the broader scope of society.

02 Employees and individuals impacted by surveillance must be involved in the process, whether that is participation in shaping regulation or in the discussions employees have with their employer about the use of digital monitoring and data handling.

03 The implications of bringing legislation into existence need to be considered. Legislation should not perpetuate or normalize the use of digital monitoring and should advance a philosophy of 'privacy as default'.

04 The federal government has a key role to play in developing a national framework.

05 Best practices can provide helpful guidance on what to do and what not to do. Modeling a framework from best practices should not begin with examples of legislation, rather, it should begin with a conceptualization of legislation based on meaningful values, principles, and human rights for Canadians.

A HIGH-LEVEL FOCUS

The expert panel began by characterizing the issue of digital monitoring as affecting more than just employees working from home. They suggested that it is imperative to understand how far reaching and profound the impacts of employer surveillance of employees is in order to effectively and comprehensively regulate it. This means understanding that employees who work remotely and employees who don't are vulnerable to the same risks and injuries to their privacy rights and wellbeing. As such, you cannot comprehensively address the issue of the digital monitoring of employees working from home without addressing the broader scope of digital monitoring issues that affect Canadian workers more broadly.

Another reason the expert panel recommended this high-level approach was due to the perceived psychological and sociological impacts of digital monitoring both at home and outside the home. They suggested that surveillance of this sort perpetuates a culture that runs contrary to the relational society we should be fostering. Professional ecosystems that rely on digital monitoring and surveillance foster an environment that lacks trust and respect for privacy and the result is that this disposition leaks into the structure of our society, jeopardizing its relationality. One of the panellists noted that this is why it is important to acknowledge the distinction between surveillance and management; the latter is relational and takes the person into account, whereas the data produced from the former does not capture the social contexts in which we live.

THE IMPORTANCE OF EMPLOYEE PARTICIPATION

When considering the many risks and harms of the use of digital monitoring on employees, the expert panel suggested that the best mitigating tool would be to enhance employee participation in deciding how, when, and where their information can be collected, used, and disclosed. Moreover, the argument was made that notification is not enough to constitute transparency. The reason for this is that even when an employee is aware that they are being monitored, they do not necessarily know to what end. 'Loss prevention' and 'performance monitoring' are vague umbrella terms that can capture a plethora of risks associated with the uses of the data that may not always be in the employee's best interest. Data can be sold to whatever global buyer is interested, it can be retained for an indefinite amount of time, and as discussed earlier, it can be used to selectively dismiss the least efficient/ productive workers. As such, employees

need a high degree of transparency to comprehensively understand the risks and harms they are being exposed to.

The panel reasoned that digital monitoring needs to be beneficial to both the employer and the employee, with an emphasis on the latter because of the significant and disproportionate impacts of the risks and harms. So far, the use of surveillance has been guided only by the motives and intentions of employers, serving functions like loss prevention, and promoting productivity and efficiency. For the employee, it is purportedly beneficial to have these performance tracking tools for career advancement, promotions, and even to make a case for working from home. Shifting to a relational understanding, does digital monitoring truly benefit employees? Because of the associated risks outlined above, tools like digital monitoring are unlikely to benefit employees in the ways they would like to see. That is why employee participation is key: the employee must have the opportunity to determine what is in their best interest, and how they would like to see digital monitoring benefit them.

PRIVACY AS DEFAULT

The panel cautioned heavily that bringing legislation into existence runs the risk of normalizing digital monitoring or inviting those not currently using it to implement it in the workplace. They argued that it should never be the norm or default to use digital monitoring.

Rather, they suggested taking a minimalist approach. If digital monitoring is not mutually beneficial, or if it only serves the interests of employers, it should not be used. This approach mitigates the potential risks to employees through the ways in which digital monitoring and data collection can be harmfully leveraged by employers. Additionally, this minimalist intention sets a positive example going forward as surveillance technology continues to advance and proliferate, becoming more harmful and invasive. The expert panel emphasized that when discussing reasonableness and limits, we should err towards 'privacy as default'.

THE GOVERNMENT'S ROLE

Among the panellists, there was a consensus that the federal government ought to play a role in regulating surveillance and digital monitoring. Given the significance, scope, and reach of the issue – impacting virtually all Canadian workers, whether working from home or not – it is within the Government's capacity and interest to play a leading role.

Arguably, the Government plays a role in regulating nearly all areas of life because it is in the interest of its constitutional mandate to protect its people. Thus, it follows that when something as profound and fundamental as the privacy rights of Canadians are at stake, the Government has a duty to protect these rights as well as the integrity of the nation's democratic status.

Despite jurisdictional difficulties, this issue can confidently be characterized as a national problem, requiring action on a national scale. Left up to provincial governments, regulations have been dramatically inconsistent and insufficient at providing employees with the protection they need. Left up to private institutions and employers, they are guided by their best interests, which seldom constitute employee privacy rights.

BEST PRACTICES AND EXAMPLES OF GOOD LEGISLATION

Members of the expert panel suggested that before looking at best practices it helps to start by exploring the problems for which digital monitoring and surveillance are perceived to provide solutions. The reason for this is that this type of framing will help to limit the use of surveillance to where it's necessary and prevent it from being invasive or a threat to privacy rights.

At the heart of this issue is the protection of the fundamental privacy rights of individuals. As such, a principles-based and human rights-based approach is necessary. The expert panel suggested looking at frameworks guided by these values, citing the Finestone Charter (also known as Bill S-21), the Privacy Rights Charter, and the Australian Privacy Charter (1994). Both legal frameworks have a focus on human rights as opposed to data protection and as such provide good models from which to draw best practices.

Another note made was that principles-based and human rights-based approaches like these provide high-level direction and steer regulation away from being too narrow or addressing some aspects of the issue and not others. These frameworks can provide the relational meaning to digital monitoring and surveillance that has historically been absent while addressing the issue at a higher level to include both employees who work from home and those who don't.

Survey Findings

From April 4 until June 1, 2022, an online survey portal was promoted at the various town halls, on social media platforms and through personal connections and networks. The survey questions and results are available on our website at www.michaelcoteau.libparl.ca. There were 330 responses to the English survey and 7 responses to the French survey.

There are limits to the survey results. Based on the distribution methods, we assume that predominantly like-minded individuals with concerns about digital monitoring responded to the survey. Moreover, it is more likely that those who felt strongly about in-home employee monitoring responded to the survey. As a result, the online survey is not considered statistically significant, nevertheless it provides some valuable directional feedback and qualitative insights on the nuances of the issue.

MP Michael Coteau and Nova Scotia MLAs Ali Duale and the Hon. Tony Ince, with MP Lena Metledge Diab who hosted a roundtable consultation in Halifax.

KEY TAKEAWAYS FROM THE SURVEY INCLUDE:

A significant minority of the survey respondents (33.7%) agreed with the statement: "Employers should not be allowed to monitor employees who work at home at all." These respondents do not accept any remote work surveillance. The balance of the respondents would accept some remote monitoring of employees under some conditions. For most of our analysis of the survey results we excluded the 113 respondents who did not accept any monitoring so that we could analyse the balance of the results.

Most respondents had a more nuanced view but would accept a limited role for surveillance of employees who work from home, with a larger majority accepting surveillance during work hours, on employer-owned equipment.

A very small number of respondents would give employers carte blanche to conduct surveillance as and when they see fit. This was apparent in responses to various questions:

- In response to **Question 3: Under what circumstances should an employer be able to monitor employees who work from home?** 1.8% would accept monitoring at any time of the day and 9.6% would accept monitoring on any devices, whether they are owned by the employer or not, provided the monitoring was work related.
- In response to **Question 8: Should there be a time limit on how long the employer can keep the information collected through monitoring software?** 11.9% felt that information gathered should be kept as long as the employer wants.

On the issues of transparency and consent, a significant majority of respondents felt that monitoring should be disclosed at the start of employment and or when surveillance software is installed. Most respondents felt that employees should be able to refuse monitoring.

On the issue of the type of surveillance, it was clear from the results that allowing employers to review monitoring data after-the-fact (e.g. browser history) was more acceptable to respondents than real-time surveillance such as keystrokes and mouse movements. There was little or no support for employers being able to activate their employees' cameras remotely.

There was no consensus on who should be regulating the issue of employer surveillance of individuals who work from home, although the federal and provincial governments were identified by most respondents.

DISCUSSION

Through the course of our public focus groups almost all participants agreed that privacy protections needed to be enhanced as a result of the increase in working from home. But the discussions and viewpoints were varied and helpful in framing the issues.

THE CASE FOR AND AGAINST SURVEILLANCE OF EMPLOYEES WHO WORK FROM HOME:

Digital monitoring of employees who work from home has been justified by some in our consultations on the basis that it is a practice that normally exists in the workplace, and so it should follow the employee when they work from home. From an employer's standpoint, monitoring is said to increase productivity and guarantee a level of security and minimize risk in an environment that is otherwise out of the employer's control. Productivity loss, efficiency, and security are also raised as issues for employers relying on surveillance.

Tracking and collecting 'productivity data' – what employees are doing, how quickly, and how productive they are, where time is allocated – purportedly gives employers a way of enforcing accountability.[1] Moreover, this automated style of monitoring is seen to be more efficient and easier to use than traditional methods of evaluation like employee engagement surveys.[2]

But there are counter arguments to this productivity rationale, namely that employer-employee relationships should be based on relational issues. Surveillance and monitoring do not replace the need for genuine communication, coaching, leadership and two way accountability for results. The argument runs that productivity should be about results, certainly for the individual employee, but also for the team, and for the enterprise or organization as a whole.

Statistics Canada looked at the issue of productivity gains and losses over the course of the pandemic, including the effects of employees working from home.

With the onset of the pandemic, there was a visible increase in labour productivity, according to a research study conducted by Statistics Canada.[3]

1 Slaughter, G. (2020, May 20). *Companies are Finding New Ways to Track Workers at Home, But Are They Going Too Far?* CTVNews. Retrieved from https://www.ctvnews.ca/business/companies-are-finding-new-ways-to-track-workers-at-home-but-are-they-going-too-far-1.4944907

2 Kropp, B. (2019, May 3). *The Future of Employee Monitoring.* Gartner. Retrieved from https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring

3 Wang, W. (2021, May 26). *Impacts of the COVID-19 pandemic on productivity growth in Canada.* Statistics Canada. Retrieved from https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021005/article/00004-eng.htm

> *In our focus group discussions and in the round table with experts we heard that all employees are not and should not be treated the same.*

It was found that this growth was spurred by significant structural changes in certain industries, namely in those that could preserve operations during the lockdowns. These are industries that shifted largely to working from home.

The report outlines that there were two potential scenarios for the way a shift to working from home may have impacted productivity. In the first case, it would contribute to an increase in productivity with workers having a better work-life balance, eliminating commute times, and generally being more comfortable and focused in their work environment. The second potential was for a loss in productivity due to a lack of face-to-face communication, knowledge flow, and managerial oversight (cue digital monitoring). However, in this latter scenario where there is a decrease, it was also demonstrated that a direct effect of working from home could still potentially increase productivity and reduce capital and labour costs; it would reduce demand for office space and equipment and would enlarge the pool of eligible workers, reducing hiring costs.

The impacts of working from home on labour productivity can vary and depend on the relative strengths of each of these potential negative and positive outcomes. The Statscan report cautions that the data currently available is insufficient to make a conclusive argument that remote work has led to this productivity growth. Further research is required in this area.

In our focus group discussions and in the round table with experts we heard that all employees are not and should not be treated the same. One size surveillance does not fit all: that the definition of 'productivity' for creatives or knowledge workers is not the same as productivity for call-centre employees; that loss prevention strategies should be customized based on an employee's access to intellectual property or financial instruments; or that new employees in a probationary period might need greater scrutiny to help them to improve.

For so-called 'production workers' who work remotely, their piecework can be monitored using automated technology and artificial intelligence, but it can just as easily be counted at the end of the shift, or at the end of the week or against monthly targets. Likewise, for white collar employees with sales and marketing responsibilities, their success can be measured based on financial or sales results, no need to monitor their screens or clicks in real-time.

And for creatives or intellectual property workers, knowledge workers, engineers, academics, researchers or administrative support staff, the value in their work could never adequately be measured by measuring screen time or clicks.

The use of technology to measure 'time on task' – too much time on an in-bound order

processing call, or too little time sitting at the computer doing administrative work – is an employer's proxy for getting work done. But how is this supervision measured against the intrusiveness and stress on employees? And who decides?

It is conceivable that digital monitoring can serve an employee positively in a few ways: employees can leverage the surveillance data to push for a raise or demonstrate a case for working from home permanently, but given the choice, how many employees would opt for their employer monitoring their eye movements, their screen shots, or their trips to the fridge?[1]

Given the myriad ways that workers can and should be evaluated working from home or in a traditional workplace it is unconvincing that using technology to monitor employees who work from home outweighs the privacy intrusion.

> ***...those most deeply impacted by surveillance and monitoring are the least likely to be able to say no to it for fear of dismissal or demotion.***

Thus, digital monitoring in its current form and context presents some issues. First, it requires a trade-off between employee privacy and accountability. This can erode trust between the employee and employer and place unnecessary stress on the employee, leading to dissatisfaction and a greater likelihood of burnout.[2] This is especially true when monitoring fosters overly competitive and toxic work environments.[3] Digital monitoring can in fact be counterproductive to productivity and profits – there is a risk of losing employees when surveillance is prioritized over their privacy. Thus, it can strip away some of the characteristics that make up a positive, inclusive, and diverse work environment.

Second, it is important to consider the disproportionate effects surveillance may have on Canadians. The imbalance in authority created through digital monitoring may place employees in a tough spot, unable to say no to monitoring. In fact, those most deeply impacted by surveillance and monitoring are the least likely to be able to say no to it for fear of dismissal or demotion.[4] [5]

---

1 Slaughter, G. (2020, May 20). *Companies are Finding New Ways to Track Workers at Home, But Are They Going Too Far?* CTVNews. Retrieved from https://www.ctvnews.ca/business/companies-are-finding-new-ways-to-track-workers-at-home-but-are-they-going-too-far-1.4944907

2 Blackman, R. (2021, August 30). *How to Monitor Your Employees - While Respecting Their Privacy.* Harvard Business Review. Retrieved from https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy

3 Slaughter, G. (2020, May 20).

4 Ibid.

5 Johnson, E. (2021, April 12). *School custodian refuses to download phone app that monitors location, says it got her fired | CBC news.* CBCnews. Retrieved from https://www.cbc.ca/news/gopublic/tattleware-privacy-employment-1.5978337

A high wage, higher income executive working from home might be able to afford a living space with a private office or work space, and might be able to afford a care provider for their children but lower-wage individuals working from home might not. The same level of monitoring would be more invasive for the lower wage employee as well as those residing with the employee (kids, spouse, roommates, etc.). The lower wage employee would also have less bargaining power in negotiating monitoring with their employer. Thus, digital monitoring can hamper employees' capacities to exercise their rights, and in some cases, invade the privacy rights of more than just the employee. Considering employees from different socio-economic, racial, and cultural backgrounds can provide insight into the distinct susceptibility to invasiveness.

CREATING A LEVEL PLAYING FIELD FOR EMPLOYERS:

In my discussions with employers and business organizations it became apparent that if the issue of monitoring of remote workers is to be regulated by government, then Canada needs a system that will facilitate compliance and enhance competitiveness with other jurisdictions. Employers want clear rules, they prefer similar regulations across Canada, and they want rules that will align with international standards.

We cannot draw a straight line between working-from-home privacy harms and their impacts on different socio-economic or ethno-cultural groups, as this requires further study, but there is the potential for a very real power imbalance in the workplace for lower wage workers that cannot be ignored.

In addition to the surface-level issues around whether surveillance is necessary or effective, lie more complex issues around how surveillance data are stored and protected, whether employers can keep the information and for how long, and whether they can sell the data to another party.

THE PATH FORWARD:

In addressing the issue of employer surveillance of employees who work from home there appear to be two broad approaches that can be taken: a human rights-based approach that identifies the privacy rights of an individual at home as paramount, and the harm-reduction approach, that seeks to set limits and trade-offs to minimize any harms that might accrue to individuals and their families.

Our recommendations outlined in the next chapter make it clear that the privacy rights of individuals at home are paramount and that they can only be abridged in limited circumstances, under clear conditions and with the consent of the employee. This approach will no doubt be debated by public officials, citizens, privacy experts, and by employers and employees who work from home, but we think that it reaches the right balance.

THE NEED FOR A PAN-CANADIAN FRAMEWORK:

On the matter of jurisdiction, it is maybe a truly Canadian trait that one of the first hurdles we had to address was the issue of which level or area of government was responsible: was this an issue of privacy as a human right, which is enshrined in the UN Declaration of Human Rights, or is this a labour matter, which falls to provincial and territorial legislatures to protect? Is this a matter of international commerce and competitiveness, or does it fall under the regulation of telecommunications?

In the end, I am proposing a two pronged answer to the jurisdictional issue. My approach is rooted in my experience as a former Ontario government Minister with responsibility for six different portfolios, and the recognition that provincial and territorial legislatures and Quebec's National Assembly have a vital role to play in protecting employees. But I am also a federal Member of Parliament, with a view to building solutions that protect Canadians regardless of where they live, where they work and whether or not they have the power to defend their basic human rights.

My approach and the recommendations outlined in the next section make it clear that the federal government, federal Crown Corporations and agencies ("the broader federal government"), each have a leadership role to play as employers, regulators, and purchasers

of goods and services to protect employees from unwarranted intrusion into their home.

The broader federal government, working with its public sector union partners, can set clear constraints on the monitoring of their employees at home. It does not need legislation to act on this matter right away.

When the federal government procures goods or services, issues licenses, or establishes regulations within federal jurisdiction, it can build on existing privacy and data protections to require explicit protections for employees who work from home as a condition of a contract or license.

Federally regulated industries and employers subject to the Canada Labour Code could be made to comply with privacy protections. This would require an amendment to the Canada Labour Code.

> *The broader federal government, working with its public sector union partners, can set clear constraints on the monitoring of their employees at home. It does not need legislation to act on this matter right away.*

To further enshrine the federal role, I am also recommending that the Parliament of Canada approve legislation to protect the privacy of individuals in their homes and limit the monitoring by employers. Over the next several months, following the release of this report, I will be proposing legislation in the form of a Private Member's Bill to do just that.

In order to make sure that Canadians from every corner of the country are adequately protected from unwarranted surveillance, I am also recommending that the Government of Canada and provincial and territorial governments negotiate a framework agreement that protects individuals in their homes where they live, regardless of their employer. This would have the benefit of giving employers a level playing field across the country and provide a common standard when it comes to surveillance practices, technology, data capture and storage.

With many Canadians experiencing and seeking a permanent transition to working from home or hybrid work arrangements, the gaps in monitoring regulation and legislation protecting employee rights cannot persist. As the monitoring and surveillance landscape evolves, so too must the set of protections that safeguard the rights of those who are subject to surveillance.

RECOMMENDATIONS

01 It is recommended that the Government of Canada and federal Crown Corporations and federal agencies play leadership roles as employers, regulators, and purchasers of goods and services to clearly establish the paramountcy of the right of individuals to privacy in their home and that digital monitoring by employers of employees who work from home only be used in limited circumstances with the following provisions:

A The employer must notify the employee in advance that monitoring will occur and every time monitoring is undertaken.

B The monitoring activity is only permitted if it is necessary to:

- protect the privacy, safety and wellbeing of other employees, customers, clients, suppliers or investors;
- enhance employee training or improve work processes;
- investigate allegations of unsafe or illegal practices in the workplace;

C The following limits also would apply:

- Employers cannot collect ambient audio or visual information using audio or video recording technology; “Ambient audio or visual information” means the background sounds or visual images, including images of people or surroundings or background noise or conversations, that can be captured, heard or seen by an observer.
- Employers may only collect information that is generated during regular paid work hours on employer supplied equipment;
- Employers must evaluate any software used to monitor employees who work from home to ensure it complies with the policies of the company and to ensure that it complies with relevant privacy legislation;
- Employers must use the least intrusive method of surveillance for the least amount of time required to meet the objectives of the monitoring activity;
- Employers must have a policy related to the monitoring of employees who work from home and the policy must include:
    1. The involvement of employees in the development of the policy;
    2. Criteria for the capturing, use, storage, transfer and destruction of employee data from surveillance

3. Disclosure of the evaluation of any software used to monitor employees who work from home.
4. A process for seeking the informed consent of employees affected by the policy and a process for employees to challenge decisions made as a result of the policy;
5. The policy must be available to all employees.

- The information collected by employers:
  1. must not be sold or transferred to any other person or company;
  2. must be destroyed after 120 days or as otherwise provided in regulation;
  3. must be stored in Canada;
  4. is subject to other limits established by regulation;

02 It is recommended that the Government of Canada and the provincial and territorial governments in Canada negotiate a framework to establish the paramountcy of the right of individuals to privacy in their home and to limit the electronic surveillance of employees who work from home with a view to:

A Limiting the scope of employer surveillance to situations where the monitoring activity is only permitted if it is necessary to:

- protect the privacy, safety and wellbeing of other employees, customers, clients, suppliers or investors;
- enhance employee training or improve work processes;
- investigate allegations of unsafe or illegal practices in the workplace;

B Requiring employers to notify employees when monitoring is being undertaken and to seek their informed consent for the monitoring;

C Restricting the storage, transfer and sale of surveillance data collected by employers;

D Providing a common set of rules and standards for employers to follow across Canadian federal, provincial and territorial jurisdictions (creating a “common standard”).

Michael Coteau
Member of Parliament
Don Valley East
December 2022