Surveillance & Privacy in the Workplace

David McKillop
PGD (HR), Advanced Diploma (FLBU), CHRP Candidate

Edited by: Marcel Faggioni
B.A (Hons), M.I.R., CHRL, Q.Med.
Member of Law Society of Canada

The idea of privacy and surveillance in the workplace has been a contentious issue amongst many employers and employees across Canada for quite some time. This has been further exemplified by a recent shift to remote/hybrid work and some employers are pursuing remote monitoring options to provide insight into how employees are managing their time at home. However, this does not come without drawbacks and begs questions such as "What do employers have the right to monitor? How can surveillance information be used? and at what point has your right to privacy been violated?" In this article, we will help shed some light on these issues and draw a line that identifies the rights of both employers and employees.

A recent study by Capterra, the firm surveyed over 750 employees in Canada and highlighted the following findings:

- 18% of respondents are unsure if employers are utilizing surveillance tools to monitor their activities
- 35% of respondents indicated their employer uses one employee monitoring tool
- 47% of respondents, indicated their employer is not utilizing employee tracking software
- Management level employees were more likely to report they were not under workplace surveillance compared to entry-level workers, suggesting that employee surveillance may be utilized more for front-line staff.

What does this mean?

The above-noted highlights suggest that there may be a transparency gap in communicating the organizations surveillance policies to employees. This issue in particular is concerning. In Ontario, the provincial government recently passed new legislation entitled "*Bill 88: Working for Workers Act, 2022*" which amended the *Employment Standards Act, 2000 (ESA)* to include the requirement of all employers with 25 or more employees to have an electronic monitoring policy in place by October 11, 2022, and implemented by November 11, 2022. Moreover, this legislation requires employers to inform their workers if and how they are being monitored electronically.

Ontario's Ministry of Labour has provided detailed guidance on what information must be incorporated into the electronic monitoring policy. It should also be noted that in Ontario, there are no concrete laws on what type of employee data may be monitored, although this is still subject to bargaining and can be enforced in a unionized environment through collective agreement provisions. Despite not having concrete laws, employers should still be weary on how far they wish to push the envelope. Any employee who believes their right to privacy has been breached can submit their concerns to the Office of the Privacy Commissioner of Ontario (OPC) which then may initiate an investigation. For more detailed information regarding privacy laws in Canada, see the official detailed summary by the Office of the Privacy Commissioner of Canada.

What is surveillance monitoring used for?

According to the Capterra study, the workplace processes most monitored include employee attendance (81%), time management (57%) and

workload management (53%). Other monitored areas in the report include computer activity (32%) and digital communications (23%). While this list is not exhaustive, it clearly highlights specific areas that are of high interest/concern to employers.

How is this impacting employee perception?

While an employee may have many concerns regarding surveillance and privacy, some of the perceptions highlighted by the Capterra report from the respondents' perspectives include:

- 65% of respondents do not believe that employee monitoring has an impact on their work output
- 19% of respondents believe it would decrease their work output
- 16% of respondents believe it would increase their work effort
- 39% of respondents agreed that utilizing monitoring software would give employers more insight to daily business operations
- 38% of respondents think it would help ensure staff are never underpaid
- 37% of respondents believe it would stop mistakes before they escalate
- 72% of respondents believe that surveillance practices could still lead to an invasion of privacy
- And 71% of respondents believe it could have a negative impact on trust

Of notable interest above is that just over 70% of employees believe that surveillance practices could lead to an invasion of privacy and have a negative impact on trust between the employer and the employee. For this reason, any employer considering implementing an employee monitoring tool should be cautious in its implementation and strongly consider if it is the most appropriate and necessary course of action.

Consideration for Employers

The main questions an employer should be prepared to answer before implementing any surveillance policy are " who, what, why, when, and how". In addition, employers should strongly consider what monitoring tools are available that will meet their needs, minimize the impact on employee privacy, and comply with surveillance and privacy legislation. Transparency in communication should also play a key role in ensuring employee buy-in and trust. Moreover, employers should ensure that all data collected is stored in a secure location and information on employee monitoring practices should be in an accessible location. PIPEDA's 10 fair information principles should also be considered. The OPC has also determined that the following purposes would be considered inappropriate and prohibited by a reasonable person (i.e., no-go zones):

- Collecting, using or disclosing personal information in ways that are otherwise unlawful
- Profiling or categorizing individuals in a way that leads to unfair, unethical or discriminatory treatment contrary to human rights law
- Collecting, using or disclosing personal information for purposes that are known or likely to cause significant harm to the individual
- Publishing personal information with the intent of charging people for its removal
- Requiring passwords to social media accounts for the purpose of employee screening
- Conducting surveillance on an individual using their own device's audio or video functions

Being mindful of the above questions and information, an employer will take great strides in minimizing any potential legal repercussions and employee relations ramifications.

Questions? We are here to help! Contact us at info@integrityconsultation.com