OPC TAKES FIRM STANCE ON PRIVACY IN THE WORKPLACE: TAKEAWAYS FOR EMPLOYERS

Posted on June 7, 2023

Categories: Insights, Publications

For the first time in 19 years, the Office of the Privacy Commissioner of Canada ("**OPC**") has updated its '*Privacy in the Workplace*' guidance document (the "**Guidance**"), bringing it more in line with employee privacy expectations in the fluid digital age.[1] In particular, the Guidance now takes a firmer stance on employee rights, provides guidance for employee monitoring, and lists eight practical tips for employers to manage their employee personal information in accordance with federal privacy legislation.

The Guidance lays out the OPC's interpretation of privacy laws and obligations that apply to employee personal information, such as the Privacy Act for federal government institutions and the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") for federal works, undertakings, and businesses (such as banks, telecommunication companies and transportation companies). The Guidance applies to organizations' relationships with current, prospective and former employees. This bulletin will focus on the implications of the Guidance for federally regulated private sector employers (subject to PIPEDA), as well as how these implications should inform other private sector employers.

Limited Application

Canada's privacy laws apply in a haphazard manner to private-sector employees, because of the division of constitutional powers between the provincial and federal governments. Federally regulated employees are subject to PIPEDA. Employees based in British Columbia, Quebec and Alberta are subject to provincial privacy laws in those provinces.[2] In all other provinces, there is currently no omnibus privacy legislation applicable to employees. Instead, employers in these provinces may be subject to privacy requirements set out in the common law, contracts (including collective agreements), or narrow statutory requirements (such as Ontario's electronic monitoring policy requirement).

Despite only applying to the subset of Canadian employers that are federally regulated, the Guidance is a useful resource for all employers looking to improve their workplace privacy policies and procedures.

OPC Removes "Balancing" Language; Emphasizes Specific Legal Requirements

The older version of the Guidance discussed the need for 'balance' between the employer's need for information and the employee's right to privacy. The updated Guidance omits this language, instead emphasizing the specific legal requirements set out under PIPEDA. In particular, the Guidance notes that there are two primary exceptions to PIPEDA's consent requirement applicable to the employment relationship:

1. Consent is not required where the collection, use or disclosure of employee personal information is necessary in order to establish, manage, or terminate the employment relationship (though the employee must still be notified in accordance with PIPEDA);[3] and
2. Knowledge or consent is not required if the personal information was produced by an individual in the course of their employment, business or profession and the collection, use or disclosure is consistent with the purposes for which the information was produced.[4]

Unfortunately, the Guidance does not provide any specific examples of when these exceptions will apply, such as whether employee monitoring for data security purposes would be considered necessary for managing an employee relationship.

British Columbia and Alberta's provincial privacy legislation (which apply to provincially regulated employers in those provinces) provide a similar exception to (1) above. However, the exception extends to processing of personal information that is "reasonable" in order to establish, manage, or terminate the employment relationship, rather than "necessary."[5] Therefore, in those provinces, the potential scope of what falls under this exception is broader.

Employees Cannot Waive their Privacy Rights

The Guidance recognizes that some employers may be tempted to tell employees that their loss of privacy is a condition of employment, on the theory that by accepting their employment, the employee has provided a blanket consent for all the employer's information handling practices. The previous version of the Guidance said it was "questionable" whether this approach complied with PIPEDA's consent principles. The new Guidance clearly indicates that this approach does not align with consent requirements under PIPEDA, or with the general principle of only collecting personal information for appropriate purposes.

Where consent is required, it is crucial for employers to obtain consent in a clear, informed, and voluntary manner. Instead of an outright waiver, employers should seek employee consent to explicit, limited, and justified collections, uses, and disclosures of their personal information. Furthermore, employers must inform employees about the consequences of not providing the requested information and offer alternative solutions. Even if employees consent to waive their privacy rights, organizations still have an obligation to adhere to privacy laws. Consent does not justify the handling of personal information in a manner that contradicts legal

requirements.

Employee Monitoring under PIPEDA

The updated Guidance contains a new section on employee monitoring, which includes practices such as verifying or assessing employee presence at work, tracking employee productivity, ensuring appropriate use of networks, and tracking the location of company vehicles.

The Guidance indicates that employee monitoring should be specific, targeted, and appropriate in the circumstances. Employers should only undertake employee monitoring after an assessment of the privacy risks and any mitigating measures. Such an assessment should establish the necessity of the practice, and consider whether any less intrusive methods would achieve the same purposes. Employers must also establish accountability measures and retention guidelines. Given that employee access rights extend to personal information collected for monitoring, employers should also have mechanisms in place to deal with employee access requests.

Employers in Ontario should also be aware of the requirement for an electronic monitoring policy, as discussed in our previous bulletins here and here.

The OPC's Eight Tips for Employers

The Guidance provides eight practical tips for employers seeking to implement privacy policies and procedures in the workplace. We summarize these tips with additional commentary below.

1. **Examine all relevant legal obligations and authorities**. These may include commitments made in collective agreements, federal and provincial privacy laws and other legal areas, such as tort, human rights, and other workplace laws.
2. **Conduct a Data Mapping Exercise**. Employers should identify all types of employee personal information collected and processed by the organization. This kind of data mapping exercise often reveals gaps in safeguards and access controls, and is very useful for assessing the impact of a privacy breach.
3. **Conduct Privacy Impact Assessments (PIAs)**. A PIA is a formal risk management process to identify privacy requirements and impacts of programs and minimize privacy risks. While organizations subject to PIPEDA are not legally required to undertake a PIA, it is a useful way to ensure that new programs are developed with privacy in mind. The OPC's Guide to the Privacy Impact Assessment Process applies to the public sector organizations, but is transferable to private organizations too.
4. **Assess the Purposes of Processing Employee Information**. Employers planning to collect, use or disclose personal information should identify all purposes for doing so, and carefully assess the

appropriateness of such purposes. In line with other OPC investigations and guidance, such an assessment should take into account (i) the sensitivity of the personal information; (ii) whether the organization's purpose represents a legitimate need or bona fide business interest; (iii) whether the collection, use or disclosure would be effective in meeting the need; (iv) whether there are less privacy invasive means of achieving the same ends at comparable cost and with comparable benefits; and (v) whether the loss is proportional to the benefits gained.

5. **Limit collection**. Organizations should collect only the personal information that is absolutely necessary for a stated purpose.
6. **Be Transparent and Open**. Organizations should develop clear and transparent policies with respect to employee privacy and communicate these policies to employees prior to putting them into practice. Employee privacy policies should identify: (i) what personal information is being collected from employees; (ii) the purpose for which the personal information is being collected; (iii) how the personal information will be collected; (iv) how the information will be used, including potential consequences for employees; and (v) how long the personal information may be retained.
7. **Respect Key Privacy Principles**. Whether or not consent is strictly required, other privacy principles continue to apply to employers, including (i) accountability requirements; (ii) accuracy of personal information; (iii) limiting collection, use, disclosure, and retention; (iv) safeguards requirements; (v) openness and transparency requirements; and (vi) rights for employees to access information or challenge an organization's compliance.
8. **Be Aware of Inappropriate Practices/No-Go Zones**. Finally, the Guidance cautions employers to avoid seeking types of information that the OPC has identified as a no-go zone. For instance, employers should not request access to password-protected areas of their employees' social media accounts.

Key Takeaways for Businesses

- Be vigilant of different frameworks of privacy rules and laws in Canada including collective agreements, federal and provincial privacy laws and other legal areas, such as tort, human rights, and workplace laws.
- Seek advice on what constitutes 'personal employee information' and consider mapping out what personal information is collected from employees and for what purposes such information is used.
- Be aware of consent requirements under applicable privacy laws. Where consent is required, it must be clear, informed, and voluntary. Exceptions to consent are available under applicable privacy laws, but in some cases, they are limited and narrow.

Members of McMillan's Privacy and Data Protection team are available to assist firms with compliance reviews and to implement any changes required.

[1] *Privacy in the Workplace* was originally published in April 2004. See the new Guidance here.
[2] BC's *Personal Information Protection Act*, SBC 2003, c 63, Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5, and Québec's *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1.
[3] PIPEDA, s. 7.3.
[4] PIPEDA, s. 7 (1) (b.2).
[5] BC's *Personal Information Protection Act*, SBC 2003, c 63, s. 13; Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5, s. 15.

by Robbie Grant, Kristen Shaw, and Nandini Pahari (Summer Law Student)

A Cautionary Note