Ontario Introduces Electronic Monitoring Legislation



On February 28, Ontario issued Bill 88, the *Working for Workers Act, 2022*, a first of its kind workplace electronic monitoring legislation requiring Ontario employers to give notice of "electronic monitoring."
The new requirements

Bill 88, will bring a new part to the *Employment Standards Act, 2000* (the ESA) titled "Written Policy on Electronic Monitoring."

The ESA will require all employers with 25 or more employees to create and publish an electronic monitoring policy within six months after Bill 88 receives Royal Assent. The proposed policy must identify whether an employer electronically monitors employees and, if so, provide:

- a description of how and in what circumstances the employer may electronically monitor employees, and
- the purposes for which information obtained through electronic monitoring may be used by the employer.

The policy must be dated, track amendment dates and must include other information that may be required by regulation. Employers must provide copies to new and current employees as well as employees assigned by temporary help agencies.

Bill 88 does not define "electronic monitoring," and likely applies to technologies deployed on corporate networks, personal devices governed by "bring your own device" policies, as well as any work tools with embedded sensors (*e.g.*, telematics and similar technologies).

The requirement to disclose the "circumstances" in which monitoring is employed suggests that the disclosure requirement applies to monitoring that occurs on a periodic or non-routine basis, *i.e.*, as part of an investigation or audit.

Commentary

If passed without amendment, the proposed legislation will impose a modest requirement on employers. Employers should consider the following six points.

1. **No limitation.** Bill 88 does not impose a limit on electronic monitoring, which is permissible in Ontario absent an express contractual or collective agreement

restriction. Such monitoring restrictions are rare in most sectors. Note that unionized employers continue to face the possibility of grievances alleging that monitoring constitutes a privacy violation under their collective agreements, though most unionized employers are already transparent about their use of monitoring technologies.

2. **List network security tools.** Bill 88 does not distinguish between monitoring via software installed on "endpoints" (workstations and handhelds) and other network devices, and most employers now compile and use a wide range of data for network security purposes. Employers should list applications regardless of where they are installed on the network.
3. **Pick the right level of disclosure.** Organizations typically keep security controls confidential to protect against adversary behavior called "threat shifting" – the shifting of tactics to circumvent existing, known controls. The disclosure that Bill 88 requires is unlikely to create a security risk; however, employers should be aware of the risk and not take the Bill as an invitation to disclose too much. We see no reason, for example, to identify software make to comply. A simple table that sets out the information as follows should suffice:

Tool	Circumstances	How	Purpose
Endpoint detection and response	Continuous	"EDR" monitors the use of workstations (programs run, files read and written, etc.) and compares it against a baseline to detect abnormalities and potential unauthorized use.	Network security
Vehicle telematics	All fleet vehicles during on shift use	On board sensors detect and report on vehicle location, driver behavior (hard braking, rapid acceleration, etc.) and engine diagnostics. For more information see our Vehicle Telematics Policy.	Fleet management and driver safety and security

4. **Anticipate questions.** Although a monitoring policy does not need to be too detailed, employers should anticipate employee questions and prepare to be transparent. For example, employees may ask if an application is hosted on premise or in the cloud, and where cloud data is stored.
5. **Update your asset map.** Every employer ought to employ "information technology asset management" – a process for governing their network hardware and software. Organizations with strong asset management practices will have little difficulty identifying how employees are "monitored." For employers with less than strong asset management practices, Bill 88 is an invitation to improvement and the rooting out unmanaged applications.
6. **Update your acceptable use policy.** Given the new electronic monitoring policy may need to be produced to prove compliance, it is best written as a stand-alone policy, and an adjunct to any existing "acceptable use policy" – a policy that sets enforceable rules for employee use of a network. It is a suitable time, however, to update acceptable use policies. Employers should consider moving the privacy provision from their acceptable use policies to their new electronic monitoring policies such that their new policies become the single document that establishes employees' expectation of privacy. Since the Supreme Court of Canada decision that recognized a limited employee expectation of privacy (in R v. Cole), we recommend that employers stipulate all purposes for which they may require access to network data, including information in user accounts – *e.g.*, to maintain the network, to investigate misconduct and to support the continuity of work.

Bill 88 imposes new requirements, but also creates an opportunity to revisit and improve several key aspects of network security and information governance. We would be pleased to assist.

by Daniel J. Michaluk and Shane Morganstein
Borden Ladner Gervais LLP