MONITORING THE MAYOR – B.C. MAYOR ALLEGES THAT COMPUTER MONITORING VIOLATED HIS PRIVACY

Posted on May 21, 2015

Categories: Insights, Publications

A recent case involving the Mayor of the District of Saanich in British Columbia illustrates the fine balance that employers must achieve between protecting secure networks and complying with privacy laws.

The Information and Privacy Commissioner for British Columbia (the "Commissioner") has issued an investigation report on the use of security software by the District of Saanich (the "District"), which illustrates the importance of undergoing a privacy audit of new and existing programs and policies. With Canadian privacy law moving towards increased regulation and greater penalties in both the public and private spheres, companies and agencies seeking to limit liability must identify whether their programs and policies encroach on personal privacy.

The Commissioner's Investigation

The Commissioner's investigation concerned the District's use of monitoring software on employee computers, including on the Mayor's, and its compliance with the British Columbia *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In British Columbia the collection, use, or disclosure of employees' personal information is governed by FIPPA in the public sector and the *Personal Information Protection Act* ("PIPA") in the private sector.

In her report, the Commissioner recognized that public agencies have a responsibility to protect against significant internal and external threats to their computer systems and network. Such threats include malware, social engineering and unauthorized access by employees. The District sought to defend against these threats by installing monitoring software on employee computers that:

- captured screenshots of computer activity at 30 second intervals;
- documented keystroke patterns;
- copied every email sent and received;
- logged all websites visited;
- monitored and logged chat and instant messaging; and
- tracked file transfers, program activity, file modification, and other network activity.

The District argued that its use of the monitoring software was strictly to maintain the security and integrity of its computer systems. The District indicated that the information collected by the software would only be made accessible on the occurrence of a "security event", and even then, only to two people in the IT department.

While the District's surveillance software had a security purpose, the Commissioner noted that the software also recorded and retained the personal information of employees without their knowledge or consent. The District argued that it had not actually "collected" personal information within the meaning of applicable privacy legislation since it had not acted on any of the information obtained. The Commissioner disagreed and held that the District misunderstood the purpose of FIPPA. In finding that the use of the monitoring software was contrary to B.C. FIPPA, the Commissioner made the following observation:

> *One of the most disappointing findings in my investigation of the District of Saanich's use of employee monitoring software is the near-complete lack of awareness and understanding of the privacy provisions of B.C.'s Freedom of Information and Protection of Privacy Act.*
>
> *Public agencies, including municipal governments, have been subject to these comprehensive privacy laws for over 20 years. Yet the District went ahead and installed monitoring software, enabling automated screen shots and keystroke logging and other intrusive monitoring tools, without considering how these actions would measure up to their privacy obligations under the law.*

Key Takeaways from the Commissioner's Investigation

The Commissioner's findings demonstrate that violations of privacy law can often be unintentional and indirect. Complying with Canadian privacy law involves navigating through a complicated web of legislation, as each Canadian jurisdiction has public, private and, sometimes, industry-specific privacy legislation. Therefore, companies that operate across multiple jurisdictions may have to simultaneously comply with multiple statutes as well as the common law (and, in Quebec, the Civil Code). This complex web of regulation, combined with the broad scope of the Canadian privacy law regime, makes it difficult for companies and agencies to know whether their programs and policies—especially those not directly related to privacy issues—are compliant with applicable privacy law. While this may explain non-compliance, it does not excuse it. The Commissioner noted that:

> "[E]mployees do not check their privacy rights at the office door. There is a right to privacy in the workplace, which has been upheld by Canadian courts and must be respected by public bodies as they consider what security controls are necessary to protect information in government networks."

From a financial and reputational perspective, compliance with privacy laws and principles has become more important than ever. Not only can the cost of cooperating and responding to a privacy commissioner investigation be expensive, the current trend in Canadian privacy law is towards increasing penalties for non-compliance. Moreover, in a culture where employees and customers are increasingly sensitive to the unwanted use of their personal information, the reputational damage caused by non-compliance with privacy laws may be greater than any financial penalty.

While it is incumbent on companies to notify individuals of the collection, use or disclosure of their personal information, the provision of such notice is only feasible if organizations are aware of the inadvertent consequences of their programs and policies. Employers should draft these notices carefully, as they may later be held strictly to the uses and purposes of collection set out therein. For example, an Employer may not be able to use information collected for disciplinary purposes, where the notice stated that the information was being collected solely for security purposes.

As illustrated by the Commissioner's investigation into the District's use of security software, determining whether a particular policy triggers considerations under privacy laws may not always be intuitive. Companies seeking to limit their exposure to financial and reputational liability should audit their current and prospective policies and consult with their legal counsel to ensure compliance with applicable laws and avoid the risks associated with non-compliance.

by Lyndsay A. Wasser and Mitch Koczerginski

A Cautionary Note