Lessons From The Saanich Spyware Fiasco And New Privacy Laws To Be Aware Of

In our current information age, security over electronic information and protection against unauthorized access is fundamental to employers' businesses. To guard against endlessly multiplying electronic threats, employers must resort to electronic means and, understandably, often resort to broad and comprehensive software to protect their operations. However, the situation involving the District of Saanich earlier this year is a good reminder to all B.C. employers that cyber-protection cannot be used at the expense of employees' privacy. Moreover, recent amendments to the federal Personal Information Protection and Electronic Documents Act(PIPEDA), now make privacy law compliance of even higher importance in the federal sphere, by imposing higher standards and more serious consequences.

In the District of Saanich,shortly after Mayor Richard Atwell was sworn in, he was shocked to discover that the District's IT department had installed spyware on its staff computers (including his), which recorded employees' emails, instant messages, programs accessed and web history. Most shockingly, the software saved a screen shot of the user's computer every 30 seconds, and recorded every keystroke that employees made. The District claimed that the software was only intended as a security measure for protecting its computer systems from cyber-threats.

Following the news of the District's use of the software, B.C.'s Office of the Privacy Commissioner (OPC) conducted an investigation.On March 30, 2015, the OPC released its investigation report, condemning the District's use of the software. B.C.'s Privacy Commissioner, Elizabeth Denham, found that many of the functions of the software were unnecessary for maintaining system security and that the administration seemed completely unaware of the Freedom of Information and Protection of Privacy Act in its implementation of the program. The screenshot and keystroke records in particular contained personal information, which the District had no statutory authority to collect. The Commissioner

recommended that the District remove the software and delete all of the information that the software had recorded.The District fully complied.

Given that employers generally do not intend to violate their employees' privacy when they implement software to protect their businesses, the Saanich case is an important reminder to keep privacy legislation top of mind when adopting cyber-protections. Since almost all employees use work computers for incidental personal purposes, information gained through monitoring employees' workstations could "range from the mundane such as vacation planning through to the highly sensitive such as viewing medical laboratory results."Though programs like the one used by Saanich might be appealing in their comprehensiveness, they may err on the side of privacy violations when engaged to protect an employer's business.

To help employers comply with privacy legislation, we have drafted these best practices when considering tools or software that may have an effect on an employee's privacy rights:

1. Determine which privacy statutes apply to your organization: FIPPA for public sector employers, PIPA for private sector employers, and PIPEDA for employers who are federally regulated.
2. Appoint a "privacy officer" tasked with ensuring that your business complies with the relevant privacy statute.
3. Notify the employees of any collection, use or disclosure of their personal information.
4. Identify the purpose for which the information will be used, collected and disclosed and ensure that the overall purpose for collecting the information is reasonable.
5. Make sure that the type of information being collected is necessary for fulfilling the purpose of its collection.
6. Obtain the employees' consent – either deemed, express or opt out.
7. Train employees about their responsibilities under your business' privacy policies and the obligations under applicable privacy legislation.
8. Make a log of every time an administrator accesses or uses an employee's personal information, including when and why this was done.
9. Audit all personal information already in your possession, ensuring that it was legally collected, that it remains securely stored, and that the purpose it was collected for remains relevant and appropriate.

Though these practices will not address every circumstance in which employers need to walk the line between cyber-protection and employee privacy, paying heed to them will help to ensure your business is able to adequately protect its electronic systems without requiring employees to "check their privacy rights at the office door."