Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

News Release

For Immediate Release
Jan. 13, 2015
Updated Jan. 14, 2015

Statement from B.C. Information and Privacy Commissioner regarding employee monitoring software and use of personal email accounts

VICTORIA—B.C. Information and Privacy Commissioner Elizabeth Denham issued the following statement about the use of employee monitoring software by public bodies, and the use of personal email accounts by public servants and officials:

“In light of recent stories in the news media, I wish to provide the following comments about how privacy laws apply to the use of employee monitoring software, and how freedom-of-information laws apply to the use of personal email accounts of public servants or officials. These comments are general in nature and do not reflect my Office’s view of any specific case.

On employee monitoring software:

“There are two types of system monitoring of employees: overt and covert. Overt monitoring is done with the knowledge of the employee and is typically described in an organization’s ‘acceptable use’ policies. Employees are notified of these policies on their first day of work, or if it is a new policy, before monitoring takes effect. This type of monitoring is typically for information and network security purposes – for example to protect against malware, visits to inappropriate websites, and installation of new devices or programs.

"However, employees still have privacy rights that are not surrendered at the office door. Even with notification, overt employee monitoring must be reasonable or necessary to the operations of the employer.

“The second type of monitoring is covert, which is done without an employee’s knowledge. This type of monitoring could take the form of tracking Internet use, logging keystrokes, or taking screen captures at set intervals as part of ongoing monitoring. The threshold for covert monitoring is very high, and may be part of a specific workplace investigation once all other less intrusive measures have been exhausted.

“Decisions about whether employee monitoring is authorized under privacy law are context-specific and will depend on the circumstances of each case. That being said, there have been no cases brought before this Office where covert monitoring was found to be justified under privacy law.

“This Office examined the use of covert monitoring software in Order F07-18, where a university installed spyware on an employee’s computer to track their activities. In this case we found that data collected by the spyware didn’t meet the necessity test and therefore did not comply with privacy law.

On the use of personal email by public servants and officials:

“I would also like to take this opportunity to remind public bodies of their obligations under freedom-of-information and privacy laws when using personal email accounts.

“We have been very clear that the *Freedom of Information and Protection of Privacy Act* applies to work-related emails sent to or received from the personal email accounts of public servants and public officials. While nothing in freedom-of-information law directly prohibits them from using personal email accounts, doing so can make it difficult to search for records responsive to an access request. In addition, the use of personal email can create privacy and security risks if personal information is accessed or stored outside of Canada, contrary to legal requirements.

“My Office has published detailed guidance that describes how B.C.’s freedom-of-information law applies to personal email accounts, and the risks presented by the use of such accounts for government business.”

The OIPC guidance document *Use of Personal Email Accounts for Public Business* can be accessed online at www.oipc.bc.ca.