LEGAL UPDATE

- A Labour Relations Services Publication -

Vol. 03, April 1, 2015

INFORMATION AND PRIVACY DECISION – USE OF EMPLOYEE MONITORING SOFTWARE BY THE DISTRICT OF SAANICH

On March 30, 2015, Information and Privacy Commissioner for British Columbia, Elizabeth Denham, released the investigation report pertaining to the use of employee monitoring software by the District of Saanich. The investigation was triggered by a public statement made by Mayor of Saanich, Richard Atwell, claiming that the District of Saanich ("District") had installed software on his computer that was collecting his personal information without his knowledge. Upon investigation of the employee monitoring software and consideration of its compliance with the Freedom of Information and Protection of Privacy Act ("FIPPA"), *the report concluded that the District was collecting personal information of employees and citizens, without authority under FIPPA and without notifying employees of the collection of their personal data as required by FIPPA. The Commissioner made five (5) recommendations and committed to issue a general set of employee privacy guidelines in order to provide municipalities and other public bodies with guidance about employee privacy rights under FIPPA.*

HOW DOES THIS IMPACT ME?

While the recommendations of the investigation report pertain to the District, the findings by Commissioner Denham provide an important reminder that public bodies have an obligation to protect data stored in their networks as well as to respect the personal privacy of employees and citizens. Noting that "employees do not check their privacy rights at the office door", public bodies, including municipalities, must meet all information and privacy obligations under FIPPA, especially when implementing necessary security controls. This Legal Update publication focuses on employment implication, highlights FIPPA obligations and interpretations, provides a number of privacy and security best practices, including an overview of IT practices in six municipalities, and clarifies what personal information should and should not have been collected by the District. The report should be reviewed by Privacy, IT, Corporate Service, Human Resource professionals and/or City Managers.

BACKGROUND

In November 2014, the District decided to procure and install software to provide "comprehensive monitoring and recording of all actions undertaken by key District employees and officers". Spector 360 was purchased and installed on the workstations of "high-profile" employees as they were considered the likeliest targets of IT security breaches. This was considered an interim measure until a district-wide system could be configured and installed.

Between November 26 and December 3, 2014, Spector 360 was silently installed (i.e., installation without any user input on the target computer) on 13 employee workstations, configured to capture the following information:

1. *automated screenshots at 30-second intervals;*
2. *monitoring and logging of chat and instant messaging;*
3. *a log of all websites visited;*
4. *recording all email activity (a copy of every email is retained for 30 days);*
5. *a log of file transfer data to track the movement of files on and off the District network;*
6. *a log of every keystroke made by a user;*
7. *a log of program activity, recording which windows were open and which window had the focus of the user;*
8. *a log of when the user logged in and logged out;*
9. *tracking of every file created, deleted, renamed, or copied; and*
10. *a record of network activity including applications that are connecting to the internet, when the connections are made, the internet address they connect to, ports being used, and the network bandwidth consumed by those connections.*

The district mayor made a public statement about the spyware on January 12, 2015, triggering the investigation by the BC Privacy Commissioner.

Upon review of the software, the information collected, the District's policies, and other relevant documents, the Commissioner determined the District had displayed a "near-complete lack of awareness and understanding" of FIPPA and issued five (5) recommendations.

FINDINGS & RECOMMENDATIONS

Prior to analyzing the District's security practices, the Commissioner reviewed the standard security practices of six municipalities. Commonly used security products were identified, including:

1. firewalls (creates a barrier between two networks);
2. intrusion detection and prevention systems (monitors network traffic to

identify and block unauthorized access and malware);
3. anti-malware software (prevents malware from being downloaded/installed);
4. event log analysis (records and analyzes IT events for security threats);
5. email filtering; and
6. web filtering.

None of the municipalities surveyed used keystroke logging or screenshot recording for employee monitoring or IT security. These technologies are generally reserved for use in specific investigations where the employer has reasonable grounds to believe there is an employment/security issue, and where other less privacy invasive alternatives would not be effective.

Next, the Commissioner reviewed the information collected by the District. She considered the following issues pertaining to the Districts' use of monitoring software: (1) collection of employee personal information; (2) authorization under FIPPA to collect personal information; (3) notification regarding the collection of employee personal information as required by FIPPA; and (4) use or disclosure of personal information in accordance with FIPPA.

Finding 1: ***The District collected personal information of employees and citizens using its monitoring software.***

The District argued that it did not collect personal information as Section 27.1 of FIPPA states "personal information received by the public body is not collected by the public body for the purposes of the *Act* if the information does not relate to a program or activity of the public body and the public body takes no action with respect to the information."

The Commissioner found the District incorrectly interpreted the provision as the information was not passively "received" (e.g., personal information delivered by mail or fax, later to be destroyed). Rather, the information was "purposefully collected" through an "expressly authorized" program. The District workplace policy permitted the use of computers for incidental personal reasons and Spector 360 was configured to collect all information that a user entered into their workstation. Information collected could include information such as personal banking data, private passwords, medical laboratory results, as well as the personal information of any individual contacting the computer user.

Finding 2: ***The collection of personal information in keystroke logs and screenshots, program activity, email, and user logon information was not authorized by FIPPA.***

The collection of personal information by a public body must be authorized by FIPPA. After thorough analysis of Section 26, which states situations where personal information may be collected, the Commissioner examined the necessity of personal information collected by the district for IT security purposes.

In reaching her determination, Commissioner Denham relied upon R. v. Cole[i], a Supreme Court of Canada case that considered employee's expectations of privacy in the workplace. The Court decided that "private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter."* As Spector 360 collected large volume of highly sensitive personal information such as keystrokes and screenshots, the Commissioner determined the collected data was getting at the "biographical core". This information was not deemed necessary for the purpose of IT Security and, in fact, created a security risk by creating a "honeypot" of data stored in one location, an easy target for attackers.

The following table (Table 1) outlines the conclusion of the Commissioner regarding the necessity of the Districts collection of personal information for IT security purposes.

TABLE 1: THE NECESSITY OF PERSONAL INFORMATION FOR IT SECURITY (DISTRICT OF SAANICH)

Necessary Classes of Information	Unnecessary Classes of Information
1. a log of all websites visited; 2. a log of file transfer data to track the movement of files on and off the company network; 3. tracking of every file created, deleted, renamed, or copied; and 4. a record of network activity including applications that are connecting to the internet, when the connections are made, the internet address they connect to, ports being used, and the network bandwidth consumed by those connections.	1. screenshots; 2. keystroke logs; 3. a log of program activity, recording which programs are open and which program had the focus of the user; 4. a record of when the user logged in and logged out; and 5. recording of all email activity.

The report issued the following recommendations, which in practicality resulted in destroying all information collected by the software:

- Recommendation 1:
  Disable the keystroke, logging, screenshot recording, program activity logging, e-mail recording, and user logon functions of Spector 360.

- Recommendation 2:
  Delete all personal information collected by the activities listed above.

Finding 3: ***The District did not provide adequate notice to employees regarding collection of their personal information in accordance with FIPPA.***

FIPPA requires that when public bodies collect personal information, the individual must be provided notice of the collection, with a few narrow exceptions. While the District did have a Network Access Form, it did not comply with the express requirements of s. 27 (2) of FIPPA.

> *s. 27(2) A public body must ensure that an individual from whom it collects personal information is told*
>
> *a) the purpose for collecting it,*
> *b) the legal authority for collecting it, and*
> *c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*

- Recommendation 3:
  Update the workplace policy pertaining to the collection of personal information, as required by s. 27(2) of FIPPA.

Finding 4: ***The investigation was unable to reach a finding regarding the access and use of Sector 360 information, as the District did not monitor access.***

- Recommendation 4:
  Implement the capability to generate logs of administrator level access to all IT systems which collect, store, use or disclose personal information.

Finally, upon review of privacy management in general, the Commissioner found that District employees were "almost entirely unaware" of the Districts obligations under FIPPA. FIPPA exists to make public bodies more accountable to the public and protect personal privacy, including unauthorized collection, use or disclosure of personal information. Given the "deep lack of understanding about the most basic tenants of the Act", the Commissioner issued the following recommendations:

- Recommendation 5:
  Implement a Privacy Management Program to meet all obligations under FIPPA, including the appointment of a Privacy Officer. The Privacy Offer should complete an audit of compliance regarding FIPPA requirements and compile a registry of all personal information collected. Provide training to all employees in regards to FIPPA requirements.

LESSONS LEARNED

It is expected that local governments will respect the privacy rights of their employees, be informed of all requirements under FIPPA, and operate secure network systems. The District of Saanich contravened FIPPA requirements when they silently installed spyware onto 13 workstations, triggering an investigation by the Office of the Information and Privacy Commission of BC. After reviewing the resulting report, it is worth repeating the following lessons:

1. Only collect personal information that is absolutely necessary.
2. Consider both privacy and security in order to ensure compliance with provincial privacy law.
3. A Privacy Management Program should be implemented and monitored to ensure practices are consistent with FIPPA.
4. Utilize "defense in depth" security solutions that are a blend of employee training and awareness, policy, and the deployment of security products and services such as network segregation, firewalls, and encryption, to name a few. Reactionary security devices such as Spector 360 have limited functionality.
5. Utilize resources currently available, such as guidance documents created by the Information & Privacy Commissioner (i.e., Accountable Privacy Management in BC's Public Sector, 2013[ii])

While the Commissioner surveyed the practices of six municipalities and determined that they were not in contravention of FIPPA, this report provides other public bodies the opportunity to review practices and policies to ensure compliance.

QUESTIONS?

If you have any comments or questions about this update please contact Karen Jewell, Program Manager at 604-432-6228 or by email at Karen.jewell@metrovancouver.org.

SOURCES

Information and Privacy Commissioner Investigation Report F15-01.
http://saanich.ca/living/about/news/2015/documents/IR-F15-01-DistrictofSaanich-30Mar2015_000.pdf

---

[i] R. v. Cole, 2012 SCC 53, [2012] 3 S.C.R. 34.
[ii] Accountability Privacy Management in BC's Public Sector, 2013. <https://www.oipc.bc.ca/guidance-documents/1545>