Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F15-01

USE OF EMPLOYEE MONITORING SOFTWARE BY THE DISTRICT OF SAANICH

Elizabeth Denham
Information and Privacy Commissioner for BC

March 30, 2015

CanLII Cite: 2015 BCIPC No. 15
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 15

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

In the context of information technology and information management, public bodies have two related and important responsibilities: to maintain a high level of security over its data and networks, and to respect the personal privacy of employees and citizens.

We all expect governments and businesses to secure networked systems against known vulnerabilities. Threats to a public body's information assets from both internal and external sources have been well-documented by information technology specialists and are the subject of regular public comment by the press.

But employees 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.

Best practices call for "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. Privacy law sets a very high threshold for the use of routine monitoring tools such as keystroke logging, workstation mirroring or tracking of personal messages.

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.

Had the District taken the time to identify and evaluate the privacy impacts of this software, decision-makers may well have implemented a different solution that addressed information security risks while ensuring compliance with privacy laws.

My office has issued many guidance documents to ensure public bodies consider personal privacy when implementing new programs, initiatives and technologies. For example, "Accountable Privacy Management in BC's Public Sector", issued

in 2013, is a scalable guidance document that gives public bodies a blueprint to implement comprehensive privacy controls step-by-step. My office has also encouraged public bodies to use Privacy Impact Assessments to mitigate the privacy risks of new technology that engages personal information, which in some circumstances are required by law.[1]

My expectation is that this report will prompt the District of Saanich and other B.C. municipalities to consider the privacy rights of citizens and employees as they exercise their management responsibilities and decision-making, particularly in the IT sector.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

1 FIPPA requires public bodies to submit privacy impact assessments for data-linking initiatives and common or integrated programs. In addition, government ministries are required to complete privacy impact assessments for any program that involves the collection, use, or disclosure of personal information.

EXECUTIVE SUMMARY

This investigation report examines the use of employee monitoring software by the District of Saanich ("District") and whether its use was compliant with the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The Commissioner initiated this investigation in light of the many unanswered questions about the District's use of monitoring software.

The Office of the Information and Privacy Commissioner ("OIPC") investigated the following issues in this investigation:

1. Did the District collect the personal information of employees and citizens through its use of monitoring software?
2. Does the District have the authority under FIPPA to collect the personal information recorded by the monitoring software?
3. Did the District notify employees of the collection of their personal information as required by FIPPA?
4. Did the District use or disclose personal information collected by the monitoring software in accordance with FIPPA?

As part of this investigation, the OIPC conducted interviews with managers and employees at the District, reviewed District policies, and conducted a site visit to determine the scope and set-up of employee monitoring software on District computers. The OIPC also surveyed other local governments and information technology ("IT") experts to determine current industry best practice regarding IT security and employee monitoring.

The Commissioner's findings in this investigation are:

1. The District did collect the personal information of employees and citizens through its use of monitoring software. In fact, because of how the software was configured, the District collected all personal information that a user entered into their workstation.

2. The District did not have the authority under FIPPA to collect the personal information recorded by the monitoring software.

3. The District did not notify employees of the collection of their personal information as required by FIPPA.

4. It could not be determined whether the District used or disclosed personal information collected by the monitoring software in compliance with FIPPA because the District had not activated the functionality to monitor user access through logs that show user activity.

The Commissioner's recommendations in this report include that the District disable various employee monitoring software functions such as keystroke logging, screenshot recording, program activity logging, email recording, and user logon functions and that the District destroy all personal information collected by the monitoring software from these functions.

The Commissioner also recommended that the District update various policies to provide employees with notice of the collection of their personal information as required by FIPPA and that the District implement the capability to generate logs of administrator level access to all IT systems which collect, store, use or disclose personal information.

A key recommendation is that the District implement a comprehensive privacy management program to ensure it is able to meet all of its obligations under FIPPA. This program should include the appointment of a Privacy Officer who should conduct a comprehensive audit of the District's compliance with FIPPA as well as the provision of training to all employees in relation to the District's access to information and privacy obligations under FIPPA.

While conducting this investigation, our Office became aware that in light of employee surveillance technology, municipalities and other public bodies could benefit from guidance about employee privacy rights under FIPPA. As a result, our Office will be issuing a general set of employee privacy guidelines in the near future.

1.0 PURPOSE AND SCOPE OF REPORT

1.1 Introduction

Public bodies are facing an increasing number of internal and external threats to their information technology ("IT") systems. These public agencies have an obligation to protect the data stored in their information systems against threats such as malware, social engineering and unauthorized access by employees.

Increasingly, public bodies are turning to new and emerging technologies, including automated surveillance tools, to address and mitigate these threats. Software solutions, such as Spector 360, give public bodies powerful tools to monitor an employee's activities in the workplace. However, these tools must be balanced against an employee's right to privacy.

Employers commonly allow employees to use workplace IT systems for some personal use. With that allowance, employees are afforded certain privacy rights related to that personal use. These privacy rights are protected by Canadian common law, provincial privacy legislation and the jurisprudence of privacy commissioners and labour tribunals.

In British Columbia the collection, use, or disclosure of the personal information of employees is governed by the *Freedom of Information and Protection of Privacy Act* ("FIPPA") in the public sector and the *Personal Information Protection Act* in the private sector.

On January 12, 2015, Mayor Richard Atwell of the District of Saanich publically stated, among other things, that the District had installed software on his office computer that was collecting his personal information without his knowledge or consent.

Mayor Atwell's statement was followed by a series of public comments by Saanich Council and the District, including an inaccurate assertion that employees do not have a reasonable expectation of privacy at work.[2]

On January 20, 2015, after closely following these events and in light of the many outstanding questions and concerns being raised by members of the public, I initiated this investigation to determine whether the District's use of monitoring software to track employee activity on its computer systems was compliant with FIPPA.

[2] Media Release, January 13, 2015, "Software Installed to Protect Integrity of Saanich Computer System", available at: http://www.saanich.ca/documents/January17mediareleasere_IT_1.pdf.

In the course of this investigation, my staff conducted interviews with managers and employees at the District, reviewed District policies, and conducted a site visit to determine the scope and configuration of Spector 360 on District computers. They also surveyed other local governments and IT experts to determine industry best practices in security and employee monitoring.

While conducting this investigation it became clear that municipalities and other public bodies could benefit from additional guidance about employee privacy rights under FIPPA. As a result, I will be issuing a general set of employee privacy guidelines in the near future as a stand-alone document.

1.1 Investigation Process

As the Information and Privacy Commissioner for British Columbia I have a statutory mandate to monitor the compliance of public bodies with FIPPA to ensure the purposes of that Act are achieved.

The purposes of FIPPA, as stated in s. 2(1), are to make public bodies more accountable to the public and to protect personal privacy. The measures to protect personal privacy include preventing the unauthorized collection, use or disclosure of personal information by public bodies.

Under s. 42(1)(a) of FIPPA, I have the authority to conduct an investigation to ensure compliance with FIPPA.

In order to determine the timeline for the procurement, installation and deployment of Spector 360, and the implementation of the District's employee monitoring policy, my staff provided the District with a series of written questions and interviewed key administrators and employees.

During the course of this investigation, my staff conducted individual interviews at the District of Saanich with the Acting Chief Administrative Officer, the Director of Corporate Services, the Manager of IT, the Assistant Manager of IT, and the Systems Analyst who installed Spector 360 on employee computers. These interviews focussed on the purpose for installing Spector 360, the circumstances that led to its acquisition and installation, and the determination of which employees' computers would be monitored.

In addition, my staff interviewed the District's former Chief Administrative Officer ("CAO"), Mayor Richard Atwell, and the IT security consultant who conducted an audit of the District's IT security in 2014.

The District provided my office with documents describing the acquisition and installation of Spector 360, as well as all email between District administrators and IT managers leading up to the acquisition and installation of the software. My staff reviewed the relevant IT policies governing the use of District computers and IT resources by employees as well as the District policy for access to the information collected by Spector 360.

2.0 OIPC Document Review and Interviews

2.1 Chronology of Events

Through interviews and review of documents the following chronology of events was established relating to the selection and implementation of Spector 360. This chronology is the basis for my analysis of the District's compliance with FIPPA.

May 2014: The District contracted with an IT security consultant to perform an information security audit ("IT Audit") on the District's IT infrastructure. The IT Audit revealed security shortcomings which District IT staff have been working to address since that time.

The District stated in a January 14, 2015 media release,[3] Spector 360 was purchased in response to one of the recommendations in the IT Audit. My staff reviewed the IT audit report and it did not make any specific recommendation that could be interpreted to recommend the purchase and installation of employee-monitoring software.

The Audit's author, also interviewed by my Office, confirmed that he did not make any such recommendation nor did he intend to make any recommendation that could be interpreted to recommend the installation of monitoring software such as Spector 360.

Nov. 15, 2014: Richard Atwell was elected as the mayor for the District of Saanich.

Nov. 17 to 19, 2014: The Director of Corporate Services continued discussions with the Manager of IT about the need to remedy outstanding IT security issues, and the need to accelerate resolution of some of those issues prior to the new Mayor taking office.

[3] Media Release Backgrounder, January 14, 2015, "Saanich Computer System"; available at: http://www.saanich.ca/documents/MediaRelease-SaanichComputerSystem.pdf.

According to the Director of Corporate Services, the motivation for this renewed focus on IT security was the perception by District Directors that the new mayor was experienced in the area of IT and would be able to identify and criticize current weaknesses in the District's IT security.

After discussions with the Manager of IT, the Director of Corporate Services decided to procure and install software which would provide for comprehensive monitoring and recording of all actions undertaken by key District employees and officers.

The Director of Corporate Services opted to secure the workstations used by employees and officers of the District who are deemed to be "high-profile" and therefore likely targets for an IT security breach.

The Director of Corporate Services stated that this strategy was adopted so that the District Directors would be able to reassure the Mayor that steps had been taken to secure the District's IT infrastructure.

The Assistant Manager of IT stated that deploying monitoring software only on the workstations of high-profile users was considered an interim measure until the District was able to install and configure a district-wide Intrusion Detection System ("IDS") and Intrusion Prevention System ("IPS") capability that would protect all District workstations. The Assistant Manager stated that this was considered an effective interim step because the district-wide IDS/IPS solution would be too expensive to rapidly implement.

Nov. 19, 2014: The Director of Corporate Services met with the Chief Administrative Officer, the Chief of the Fire Department, and the Directors of Legislative Services, Planning, Parks and Recreation, and Finance. The use of a security strategy focussed on high-profile users was discussed and the Directors were advised that protection and monitoring software would be installed on the following employee workstations:

1. the Mayor;
2. two shared workstations for Councillors;
3. the CAO;
4. the Directors of Corporate Services, Legislative Services, Planning, Parks and Recreation, Finance, and Engineering;
5. the Chief of the Fire Department; and
6. two executive administrative assistants.

Immediately after this meeting the Director of Corporate Services directed the Manager of IT to research and procure protection and monitoring software.

The Manager of IT then directed the Assistant Manager of IT to research and source software that could be installed on selected workstations and record all user activity.

The Assistant Manager understood that the goal was to have a forensic auditing capability. The software was also to have the ability to determine whether user accounts were accessing areas which they were not supposed to be accessing.

Nov. 20, 2014: After researching available options through an online search, the Assistant Manager reported back to the Manager of IT, recommending that the District acquire Spector 360.

The Manager of IT reported to the Director of Corporate Services that available alternatives had been researched and that he recommended Spector 360. The Manager stated that this program would provide IT staff with information to assist in identifying and mitigating a security breach.

Nov. 21, 2014: Spector 360 was purchased.

Nov. 26 to Dec. 3, 2014: District IT staff installed Spector 360 on 13 employee workstations.

Spector 360 was installed with the default configuration, which provided for:

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.

Data collected by the Spector 360 tool was encrypted and stored on a virtual server located at Saanich City Hall. The virtual server is dedicated to Spector 360. The server was configured to retain the data for a period of three months. There is no backup copy of this information.

The Manager of IT and the Assistant Manager both described the implementation and configuration of Spector 360 as providing a reactive approach to IT security, helping to enable rapid remediation after a security breach.

District IT staff were directed by the Assistant Manager of IT to use a "silent" installation, which refers to installation without any user input on the target computer and were specifically directed to configure the software to enable keystroke logging and timed screenshots.

With regard to the specific direction to enable screenshots, the Assistant Manager stated that there were concerns from IT staff that frequent screenshots could result in a possible drain on IT resources. However, in consultation with the vendor for Spector 360 it was determined that the software could be configured to enable screenshots with negligible effect on IT resources.

With regard to the specific direction to enable keystroke logging, District IT staff had expressed concerns about the privacy implications of keystroke logging. The Assistant Manager directed staff to enable keystroke logging because it had been specifically authorized by District management.

Dec. 1, 2014: Richard Atwell is sworn in as the mayor for the District of Saanich.

Dec. 2, 2014: The Manager of IT emailed the Director of Corporate Services requesting express authorization for the installation and activation of Spector 360, including the keystroke logging function.

The Director confirmed in an email that the program was authorized and that the District Directors and the CAO were aware that monitoring software was being installed on their workstations. She further indicated that it would be left with the CAO to decide whether or not the two executive assistants would be informed. The email did not mention whether or not the Mayor or Councillors would be made aware of the installation of Spector 360.

The CAO told my staff that he informed the executive assistants about the installation of security software in a general way, but did not specifically describe the software or its functions.

The Director of Corporate Services told my staff that the Mayor was asked to sign the Network Access Terms and Conditions Form, which advises employees that their use of district IT resources could be monitored. However, the District

was unable to provide my office with a copy of that form signed by the Mayor, and the Mayor told my staff that he had not been provided with the form.

The Assistant Manager said that the District has only accessed the information collected by Spector 360 three times since it installed the software. He stated that the first time was shortly after the initial installation in order to ensure that the software installed on each workstation was operating correctly. The Assistant Manager said this was the procedure that was recommended by the software vendor. The Assistant Manager stated that the second and third times were to disable Spector 360 and to access the information during my staff's site visit, where the District reviewed the information which had been collected. My staff was unable to confirm that these were the only times that information was accessed because the District did not maintain access logs for the software or server.

Dec. 11, 2014: Mayor Atwell was informed by a third party about the installation of Spector 360 on his District workstation.

Dec. 12, 2014: Mayor Atwell met with the Manager of IT, the Assistant Manager of IT, and Director of Corporate Services to enquire about the software.

Dec. 15, 2014: Mayor Atwell complained to Saanich police about the use of Spector 360 by the District, and asked the police to determine whether the use of the software was in contravention of the *Criminal Code of Canada*.

Saanich police sought an opinion from outside legal counsel on the legality of Spector 360. As a result of that opinion it was determined by Saanich Police that the use of Spector 360 was not a contravention of the Criminal Code. This opinion did not appear to consider whether the use of Spector 360 was in contravention of other federal or provincial law.

Jan. 12, 2015: Mayor Atwell informed the public that the District had installed spyware on his computer.

Jan. 19, 2015: The Director of Corporate Services directed the Manager of IT to disable Spector 360 pending a resolution of the concerns about its use by the District.

Jan. 20, 2015: I initiated this investigation into the use of Spector 360 by the District.

Jan. 21, 2015: Spector 360 is disabled by the Assistant Manager.

2.2 Documents reviewed

My staff requested that the District provide our Office with copies of:

1. the external consultant's security audit report referenced in the media;
2. current and previous policies and notices to employees relating to the software;
3. the service level agreement for Spector 360;
4. the Saanich Police Department's opinion resulting from its examination of the legality of the use of Spector 360;
5. any Council minutes (in-camera and public) addressing the use of employee monitoring software;
6. all documents pertaining to the procurement, setup and implementation of employee monitoring software;
7. copies of all logs and reports regarding any electronic capture of data by Spector 360;
8. the log of database logons for Spector 360, including the list of login accounts, as well the records for each account;
9. all email between the CAO, the Director of Corporate Services, the Manager of Information Technology, and the Assistant Manager of IT leading up to and during the acquisition and installation of Spector 360; and
10. any other documents related to this issue, including emails (using either District or personal accounts), texts, and instant messages.

The District does not have a service level agreement for Spector 360 and was therefore unable to provide it to my office. The District was also not able to provide access logs or a log of database logons for the Spector 360 software or server because that functionality was not put in place by the IT department.

The Director of Corporate Services provided my Office with a statutory declaration that District employees had conducted a thorough search for records in the custody or control of the District which were responsive to my request for documents, and all of those records were provided to my Office.

Our review of these documents supported the timeline and positions taken by the District employees whom my staff interviewed.

DISTRICT POLICY FOR ADMINISTRATION AND CONTROLS OF SPECTOR 360

The District provided our Office with its policy on the use of Spector 360. The policy states that the software is used "to ensure the security and integrity of computers for high profile individuals and protect District information from unauthorized access, theft and destruction."

Access to the software and server is restricted to the Manager and Assistant Manager of IT and may only occur as a result of a "security event". Such an event will be identified and agreed to by the CAO or Director of Corporate Services and access is only authorised through written approval by the CAO or Director of Corporate Services.

Security events that may trigger access to Spector 360 "for the purpose of identifying, investigating and remediating security risks and threats to computers and information associated with high-profile individuals" include:

1. unauthorized physical access to computers and technology equipment;
2. lost or stolen computers and technology equipment;
3. known, suspected or potential penetration and hacking;
4. known, suspected or potential data theft;
5. internal tampering, hacking or fraud;
6. impersonation and social engineering; and
7. human error.

2.3 IT Security and Public Bodies

Public bodies face IT security threats on two broad fronts: internal and external.

Internal threats include the intentional efforts by employees to damage IT systems or gain access to information which they are not authorized to access.

External threats are more diverse and evolve quickly. These can be transient or persistent, targeted or random, and can be motivated by gain or by sport. A common example of an external threat is "malware"—software intended to

damage computer systems or surreptitiously gather information to be used elsewhere, such as banking account numbers and passwords. It can be placed on a computer system through the actions of external attackers or by malicious or unwitting employees. Malware is a constant threat faced by any public body, organization or an individual's computing device and manifests itself in many ways for many different purposes.

At the non-technical end of the spectrum of external security threats is social engineering, where an external attacker tricks an employee in order to gain access to an IT system, often by masquerading as IT support from within the organization. This is a very effective method to gain unauthorized access to systems and data and is difficult to defend against when done by sophisticated attackers.

Regardless of the source of the threat, the damage done by internal or external persons is not always immediately apparent. Unlike a physical object, when data is stolen or compromised it is typically copied and the original data remains.

In light of the diversity of threats facing a public body, best practices call for 'defense in depth' and are a considered blend of operational capability, well-trained employees, sound security policy, and the deployment of up to date security products or services.

In order to ascertain common practices for IT security, as well as an understanding of how employee monitoring and IT security software is used by other local governments, my Office asked six municipalities of various sizes about their IT security practices. Our survey found the security products commonly used include:

1. firewalls which create a barrier between two networks, typically separating internal and external network devices and computers;

2. intrusion detection and prevention systems which monitor network traffic and attempt to identify, report, and block malware or unauthorized access;

3. anti-malware software which attempt to prevent malware from being downloaded, installed or executed;

4. event log analysis which records IT system events and analyzes them for likely security threats;

5. email filtering; and

6. web filtering.

None of the local governments surveyed use keystroke logging[4] or screenshot[5] recording for employee monitoring or IT security. One municipality had the capacity to take screenshots on some employee devices but that capability is only used to help locate stolen portable devices. The use of keystroke logging and screenshot recording is generally reserved for use in specific investigations, where the employer has reasonable grounds to believe there is an employment or security issue, and where other less privacy invasive alternatives would not be effective.

The software deployed by the District, Spector 360, is described by its manufacturer as follows:

> Spector 360 is a comprehensive user activity monitoring solution that enables companies to log, retain, review and report on employee activity. Spector 360 creates a definitive record of an employee's digital behavior, and in doing so provides organizations with the ability to see the context of user actions.[6]

Two important elements of this comprehensive monitoring are the capacity to record every keystroke that is typed by a user and to record screenshots of what is displayed on the workstation monitor at set time intervals.

3.0 ISSUES IDENTIFIED

The issues in this investigation are:

1. Did the District collect the personal information of employees and citizens through its use of monitoring software?
2. Does the District have the authority under FIPPA to collect the personal information recorded by the monitoring software?
3. Did the District notify employees of the collection of their personal information as required by FIPPA?
4. Did the District use or disclose personal information collected by the monitoring software in accordance with FIPPA?

[4] Keystroke logging creates a record of each of the keys struck on a keyboard.
[5] Screenshot recording archives a digital picture of what is displayed on a workstation monitor. The screenshot is taken at a set time interval.
[6] http://www.spector360.com/.

4.0 ANALYSIS

4.1 Application of FIPPA

FIPPA applies to the collection, use, or disclosure of personal information by a public body. The definition of a public body in Schedule 1 of FIPPA includes a "local public body", which in turn includes a "local government body". Schedule 1 further defines a local government body as a "municipality". The District of Saanich is a municipality and is therefore a public body and subject to FIPPA.

4.2 Personal Information

ISSUE 1: Did the District collect the personal information of employees and citizens through its use of monitoring software?

Personal information is defined by FIPPA as "recorded information about an identifiable individual other than contact information". If, through its use of the Spector 360 program, the District collected personal information, then its actions are subject to FIPPA.

The District argued in its submission to my Office that it did not collect personal information in its use of Spector 360 because:

> [S]ection 27.1 of FOIPPA states that 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. Therefore, any personal information recorded because of Spector 360 that is not used is not considered collected under section 27.1 of FOIPPA.

This position misunderstands the purpose of s. 27.1 of FIPPA. Section 27.1 clarifies that a public body that has received personal information (for example by mail or fax), has not collected that personal information for the purposes of FIPPA where the information does not relate to a program or activity of the public body.

Where the public body does nothing with it other than to read it and then delete, return or destroy the information, it does not assume custody or control of the

personal information under FIPPA. That is not the case with the information collected by Spector 360; that information was not passively "received" by the District but rather was purposefully collected through a program that was expressly authorized by the Director of Corporate Services. Therefore, s. 27.1 is not applicable in this instance.

The Saanich workplace policy on the "Use of Saanich Materials, Equipment, Facilities and Resources" states that "[e]mployees may use Saanich computers for incidental personal reasons, outside of scheduled hours of work, provided that such use is consistent with professional conduct outlined within these guidelines and not for personal financial gain." Therefore the District's policy allows for some personal use of workplace computers and of the internet.

My staff reviewed the information that was recorded by Spector 360 during a site visit to the District. They observed that the software had been configured to record the activities of District employees, including recording and retaining screenshots of computer activity at 30 second intervals and every keystroke taken on a workstation's keyboard, and retaining copies of every email sent or received.

This configuration collected all personal information that a user entered into their workstation, including images of personal internet use, such as internet banking, private passwords, or medical laboratory results, as well as the personal information of any constituents who contacted the Mayor, the District Directors, or the executive assistants to the Mayor and Councillors.

Therefore, I find that the District collected the personal information of employees and citizens using Spector 360.

4.3 Collection of Personal Information

ISSUE 2: Does the District have the authority under FIPPA to collect the personal information recorded by the monitoring software?

The collection of personal information by a public body must be authorized by FIPPA. In order for such collection to be authorized it must satisfy s. 26 of that Act. Subsections (a) to (h) of s. 26 set out the potential authorities for collection under FIPPA.

The District provided four explanations for how its collection of personal information using Spector 360 was authorized by s. 26 of the Act, citing s. 26(a), (b), (c) and (d).

The relevant portions of s. 26 are:

> **Purpose for which personal information may be collected**
>
> 26 A public body may collect personal information only if
>
> (a) the collection of the information is expressly authorized under an Act,
>
> (b) the information is collected for the purposes of law enforcement,
>
> (c) the information relates directly to and is necessary for a program or activity of the public body,
>
> (d) with respect to personal information collected for a prescribed purpose,
>
> (i) the individual the information is about has consented in the prescribed manner to that collection, and
>
> (ii) a reasonable person would consider that collection appropriate in the circumstances,

According to the District, these subsections authorize its collection of personal information. I will address each of these arguments in turn.

Section 26(a)

Section 26(a) of FIPPA authorizes the collection of personal information where that collection is expressly authorized under an Act. The requirement that the collection be *expressly* authorized means that the Act being cited must clearly state that the *collection of personal information* is permitted, authorized, or required.

The District cites s. 30 of FIPPA as the Act that authorizes collection, which states that a "public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal." The position of the District is that personal information was collected by Spector 360 in order to secure the personal information in the custody of the District. However, s. 30 does not refer to the collection of personal information, and cannot be said to

expressly authorize its collection. Instead, s. 30 of FIPPA is simply a requirement that a public body have reasonable security measures in place to protect personal information in its custody or under its control.

Section 26(b)

Section 26(b) of FIPPA authorizes the collection of personal information for the purposes of law enforcement. My Office has interpreted that section to require that the public body collecting the personal information must have a common law or statutory law enforcement mandate.

The District has a statutory law enforcement mandate pursuant to s. 8 of the *Community Charter*, however, that mandate is limited to the subjects enumerated in s. 8(3)(a to m) of that Act, which includes such things as regulating municipal services and protection of the natural environment. The District's mandate does not include the regulation of illegal or unauthorized access to computer networks.

The regulation of illegal or unauthorized access to computer networks is more appropriately within the jurisdiction of law enforcement agencies charged with the enforcement of the *Criminal Code of Canada*[7] such as a municipal police department. Therefore, the District cannot claim a law enforcement purpose for its collection of personal information by Spector 360 because it does not have a statutory or common law mandate to enforce the *Criminal Code of Canada*.

Section 26(c)

Section 26(c) of FIPPA authorizes the collection of personal information where the information relates directly to and is necessary for a program or activity of the public body.

This subsection has two components: the information must relate directly to a program or activity of the public body and be necessary for that program or activity.

Does the information **relate directly** to the program or activity of the District?

The District submits that it is collecting personal information using Spector 360 for the purpose of "identifying, investigating and remediating risks or threats" to its IT infrastructure and to the information stored on District servers. This is clearly a valid purpose for an activity of the District, and as the District has

[7] Section 342.1 of the *Criminal Code of Canada* is commonly interpreted to prohibit unauthorized access to a computer system.

already pointed out, s. 30 of FIPPA requires that it take reasonable security measures to protect personal information stored on District servers.

As described above, Spector 360 collects information about nearly every aspect of the employee's use of their workstation. The District states that this information can assist it to rapidly respond to a breach of its network and take steps to remedy the intrusion. However, while the information collected by Spector 360 may help IT staff to identify information illegitimately accessed by an employee, it would not be effective against most malware, which would access information silently, without keystrokes or user action, and without any evident on-screen activity.

The effectiveness of Spector 360 for protecting IT security is further limited by the fact that it is neither a preventative nor a detective tool. It is not configured in such a manner as to restrict access to sensitive IT resources, or to detect instances of suspected intrusion or unauthorized access. Nor was it configured to alert IT staff of any suspicious activity.

Spector 360's utility is limited to providing a detailed description of the actions of the employee. To that extent it can only provide District IT staff with the ability to review those actions after a security breach has already taken place.

It should also be noted that by specifically collecting information about the activities of key officers and employees within the District, and storing it in one location on the network, the District creates an additional security risk. Any tool that monitors network traffic or collects confidential information in one place is a primary target for attackers. This is particularly the case where, as with the District's implementation of Spector 360, logs that monitor administrator access to the server are not enabled.

Despite these significant weaknesses with respect to Spector 360's ability to enhance the District's IT security, in consultation with IT security consultants I have determined that the following seven classes of personal information recorded by Spector 360 are at least minimally related to the securing of the District's IT resources:

1. recording of all email activity (a copy of every email sent or received is retained for 30 days);
2. a log of all websites visited;
3. a log of file transfer data to track the movement of files on and off the company network;
4. a record of when the user logged in and logged out;

5. a log of program activity, recording which programs are open and which program had the focus of the user;
6. tracking of every file created, deleted, renamed, or copied; and
7. 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.

However, two of the classes of information: collecting screenshots and keystroke logs; are not obviously related to the protection of District IT resources.

I note here that Spector 360's capability to monitor and log chat and instant messaging sessions, while enabled by the District, was not actually collecting personal information because the District does not use chat or instant messaging on its workstations. While this information was not collected it is very unlikely that this class of personal information could be considered to be related to IT security.

In Order F07-18,[8] an OIPC Adjudicator considered whether the collection of personal information by the University of British Columbia ("UBC") using software to take screenshots of the computer activity of an employee was related to a program or activity of UBC. The Adjudicator found that information about whether the employee was accessing non-work related websites during hours for which he was being paid was information which was directly related to UBC's management of its human resources.[9]

However, information that revealed the specifics of the employee's non-work related activities was not related to any program or activity of UBC:

> Information which reveals the complainant's specific activities on non-work related websites is not, in this case, directly related to UBC's human resources activities. As UBC notes, this is not a case involving an allegation that an employee accessed inappropriate material on the internet. The specifics of the complainant's banking transactions, or his personal correspondence, are not relevant to any program or activity of UBC's. (…)[10]

Similarly, personal information collected by the District about the activities of its employees while engaged in "incidental personal" computer use, as allowed by the District's "Use of Saanich Materials, Equipment, Facilities and Resources Use Policy" ("Use Policy"), does not relate to the security of its IT infrastructure.

[8] Order F07-18, University of British Columbia (Re), 2007 CanLII 42407 (BC IPC).
[9] At para. 62.
[10] At para. 63.

Screenshots and keystroke logs that provide a detailed description of the personal activities as well as correspondence to the District from citizens, do not relate to the District's IT security.

Therefore, the routine, continuous collection of personal information in keystroke logs and screenshots using Spector 360 is not directly related to a program or activity of the District.

Is the information **necessary** for an operating program or activity of the District?

Whether or not the collection of personal information is related to a program or activity of the District does not, on its own, determine whether it is authorized by s. 26(c); the personal information must also be necessary for that program.

The standard of "necessary" within FIPPA is to be applied as a rigorous standard.[11] It is not sufficient for the collection of personal information to be merely convenient, but neither does it need to be impossible to carry out the program or activity without the information. The public body should be prepared to demonstrate that the collection is demonstrably necessary to accomplish the specific need or purpose.

In Order F13-04,[12] I reviewed the factors that go into determining whether information is necessary. In that Order I considered the collection of GPS data related to the location of UBC Campus Security vehicles. As those vehicles were generally occupied by only one employee, and UBC had a record of which employee was in each car, the GPS information was the personal information of the employee. In determining necessity, I considered the sensitivity of the personal information being collected, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection.[13] I will follow the same approach here.

In consultation with my Office's IT Analyst and other IT security consultants, I have determined that collecting the personal information within the following four classes of workstation activity are necessary for the purpose of IT security within the context of the District of Saanich:

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;

[11] Order F13-04, University of British Columbia (Re), 2013 BCIPC 4, at para. 51.
[12] Order F13-04, University of British Columbia (Re), 2013 BCIPC 4.
[13] Order F13-04, at para. 54.

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.

As I have discussed above, Spector 360 is primarily an employee monitoring tool, and is of minimal value to the protection the District's IT security. However, the collection of the information in these four classes would arguably assist District IT staff in determining, after the fact, whether and to what extent an employee had illegitimately accessed information. That information would provide a detailed description of the employee's actions that led to a security breach and would enable District IT staff to more efficiently respond to such a breach.

However, I am not persuaded that the following five classes of information collected by Spector 360 are also necessary, particularly where the other four classes of information are already being collected:

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.

As described above, Spector 360 is comprehensively collecting information about the employee's use of their workstation, down to individual keys typed on the keyboard. As employees are allowed by the District to use workstations for personal use, Spector 360 is collecting the personal information of employees that relates to their private lives, unrelated to their employment. Similarly, the recording of screenshots at 30-second intervals will record personal information displayed on employees' web browsers.

The personal information that is accessed online during the routine daily activities of any individual can range from the mundane such as vacation planning through to the highly sensitive such as viewing medical laboratory results. The Supreme

Court of Canada recently considered the issue of employees' expectation of privacy on workplace computers in *R. v. Cole*:[14]

> [47] Computers that are used for personal purposes, regardless of where they are found or to whom they belong, "contain the details of our financial, medical, and personal situations" (*Morelli*, at para. 105). This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices "reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet" (*ibid*.).
>
> [48] This sort of private information falls at the very heart of the "biographical core" protected by s. 8 of the *Charter*.

While *Cole* was in the context of a criminal investigation and the question before the Court was one of unreasonable search and seizure under the *Charter of Rights and Freedoms*, I consider the observations regarding employee use of the internet to be relevant to my consideration of the sensitivity of personal information collected by a monitoring tool such as Spector 360. In *Cole*, the employer allowed employees the limited use of workplace computers for personal use. It was this policy that gave rise to an employee's reasonable expectation of privacy. As described above, the District's policy in this case also allows for the limited personal use of District workstations for personal use.

The District is therefore not only collecting very large amounts of personal information through its use of Spector 360, but some portion of that information is also very sensitive personal information, going to the "biographical core" of its employees.

The collection of keystroke logs, screenshots, program activity logs, all email sent and received, and a record of when the user logged in and logged out is intended by the District to facilitate a forensic capability that would enable District IT staff to accurately determine the cause of a security breach and take remediation measures. However, considering the minimal value of this information to the protection of IT security, I have determined that that purpose is already accomplished by the collection of the four classes of workstation activity which I have discussed above. In light of the volume and sensitivity of the personal information collected in the keystroke logs, screenshots, program activity, email, and user logon information, I find that their collection is not necessary for the purpose of IT security.

[14] *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34.

Section 26(d)

Section 26(d) of FIPPA authorizes the collection of personal information with respect to personal information collected for a prescribed purpose. Those prescribed purposes are enumerated in s. 9 of the FIPPA Regulation,[15] neither of which apply to the collection of personal information by the District using Spector 360.

I find that the collection of personal information in keystroke logs and screenshots, program activity, email, and user logon information using Spector 360 is not authorized by FIPPA.

RECOMMENDATION 1:

The District of Saanich should disable the keystroke logging, screenshot recording, program activity logging, email recording, and user logon functions of Spector 360.

RECOMMENDATION 2:

The District of Saanich should securely delete all personal information collected by the keystroke logging, screenshot recording, program activity logging, email recording, and user logon functions of Spector 360.

Given that the personal information I have recommended be deleted is intermingled with all other information collected by Spector 360, it would be impractical to remove the personal information alone. The District has advised me that it has no use for any of the information collected to date. Therefore, the District should destroy all information collected by the monitoring software.

[15] http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/155_2012#section9.

4.4 Notice to Employees

ISSUE 3: Did the District notify employees of the collection of their personal information as required by FIPPA?

When a public body collects personal information, FIPPA requires that the individual the information is about be provided notice of the collection, with a few narrow exceptions.

Section 27(2) of FIPPA sets out the content of that notice:

> 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.

The District submits that it provides notice to employees through its "Network Access Terms and Conditions Form" ("Network Access Form"):

> (…) all employees, prior to accessing the Saanich Network must execute a Network Access Terms and Conditions Form. This form makes reference to Saanich's Administrative Policy -- Use of Saanich Materials, Equipment, Facilities and Resources (attached). This policy outlines specific standards that guide the use of all Saanich equipment.

The Network Access Form does not discuss the collection of any personal information. However, as discussed above, the Use Policy does address the collection and disclosure of "communications system data":

> The District may access, inspect, retrieve, review, read, copy, store, archive, delete, destroy and distribute or disclose to others (including courts and law enforcement authorities) all communications system data and uses, including e-mail, voice mail and Internet use, without any further notice and as the District in its sole discretion may consider necessary or appropriate.

Employees are required to read and sign the Network Access Form prior to gaining access to District IT resources, and that form refers to the Use Policy.

Neither document contains the elements which are expressly required by s. 27(2) of FIPPA. Specifically, District employees are not provided with notice of the District's purpose for collecting their personal information, the District's legal authority for collecting it, or with the contact information of an officer or employee of the District that an employee could contact to enquire about the collection.

I find that the District did not provide adequate notice to employees of the collection of their personal information to meet the requirements of s. 27(2) of FIPPA.

RECOMMENDATION 3:

The District of Saanich should update its policy for the Use of Saanich Materials, Equipment, Facilities and Resources to provide employees with notice of the collection of their personal information, as required by s. 27(2) of FIPPA.

4.5 Use and Disclosure of Personal Information

ISSUE 4: Did the District use or disclose personal information collected by the monitoring software in accordance with FIPPA?

The District was unable to provide our office with administrator access logs to the Spector 360 software or server, as that functionality was not put in place by the IT department. This is a common security failing that my Office is frequently advising organizations and public bodies to rectify. While IT security software is often configured to record a log of registered users, it is frequently not configured to record "Super User" or administrator-level access.

Therefore, while my staff found no evidence to contradict the District's claim that it did not access or use the personal information it collected using Spector 360, they were unable to conclusively confirm this without the type of audit logs that would be most relevant to that question. In the next section of this report I will discuss the need for the District to implement a comprehensive privacy management program to remedy this and other significant gaps in its ability meet its obligations under FIPPA.

The District informed my staff that the information collected by Spector 360 was not used or accessed after the initial installation, other than to demonstrate the information being collected to my staff. As the information was not used or accessed it was also never disclosed outside of the District. Our interviews and review of documentary evidence have not contradicted this.

However, as the District did not have the capability to monitor access to Sector 360 through access logs, I am unable to make a finding regarding the use or disclosure of this personal information by the District.

RECOMMENDATION 4:

The District of Saanich should implement the capability to generate logs of administrator level access to all IT systems which collect, store, use or disclose personal information.

5.0 PRIVACY MANAGEMENT PROGRAM

During the course of this investigation my staff found that District employees and officers were almost entirely unaware of the District's obligations under Part 3 of FIPPA, which governs the protection of individuals' privacy and places limits on the District's ability to collect, use or disclose personal information. To the extent that the District had processes in place to meet the requirements of that Act, those processes were limited only to those which are needed to comply with the access to information obligations in Part 2 of FIPPA. With respect to the FIPPA obligations that are the subject of this investigation, the District has not taken any steps to meet the requirements of Part 3.

The District's submissions to my office demonstrate a deep lack of understanding about the most basic tenets of the Act, such as what constitutes the collection of personal information by the District. The District of Saanich must implement a privacy management program[16] to ensure that all personal information in its custody or under its control is adequately protected and that any collection, use, or disclosure is compliant with FIPPA.

Key components of a privacy management program which the District would immediately benefit from include the appointment of a Privacy Officer who would

[16] My Office has produced several comprehensive guidance documents that assist public bodies and organizations to implement such a program. "Accountable Privacy Management in BC's Public Sector", available at: https://www.oipc.bc.ca/guidance-documents/1545.

be responsible for ensuring all District programs and activities operate in compliance with FIPPA.

In addition, District employees must be provided with training in relation to all requirements of the Act.

The Privacy Officer should undertake a comprehensive audit of the District's compliance with FIPPA. That audit should include a registry of all personal information in the custody or under the control of the District, and of the programs or activities that collect, use, or disclose that information.

The personal information registry will guide a determination of which of those programs or activities should be subjected to a privacy impact assessment ("PIA") based on volume and sensitivity of personal information. If the District had completed such a PIA for Spector 360 prior to its procurement and installation, it would have identified the concerns raised in this report, and would have ensured that all employees had notice of the collection of their personal information.

My Office will follow up with the District in six months regarding its implementation of my recommendations.

RECOMMENDATION 5:

The District of Saanich should implement a comprehensive privacy management program to ensure it is able to meet all of its obligations under the *Freedom of Information and Protection of Privacy Act*. This program should include the appointment of a Privacy Officer.

The Privacy Officer should conduct a comprehensive audit of the District's compliance with the *Freedom of Information and Protection of Privacy Act*, and compile a registry of all personal information in the custody or under the control of the District.

The District should provide training to all employees in relation to all requirements of the *Freedom of Information and Protection of Privacy Act*.

6.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

6.1 Summary of Findings

I have made the following findings in this investigation:

1. **The District collected the personal information of employees and citizens using Spector 360.**

2. **The collection of personal information in keystroke logs, screenshots, program activity logs, email, and user logon information using Spector 360 is not authorized by FIPPA.**

3. **The District did not provide adequate notice to employees of the collection of their personal information to meet the requirements of s. 27(2) of FIPPA.**

4. **The District did not have the capability to monitor access to Sector 360 through access logs. Therefore, I am unable to make a finding regarding the use or disclosure of this personal information by the District**

6.2 Summary of Recommendations

RECOMMENDATION 1

I recommend that the District of Saanich disable the keystroke logging, screenshot recording, program activity logging, email recording, and user logon functions of Spector 360.

RECOMMENDATION 2

I recommend that the District of Saanich destroy all personal information collected by the keystroke logging, screenshot recording, program activity logging, email recording, and user logon functions of Spector 360.

RECOMMENDATION 3

I recommend that the District of Saanich update its policy for the Use of Saanich Materials, Equipment, Facilities and Resources to provide employees with notice of the collection of their personal information, as required by s. 27(2) of FIPPA.

RECOMMENDATION 4

I recommend that the District of Saanich implement the capability to generate logs of administrator level access to all IT systems which collect, store, use or disclose personal information.

RECOMMENDATION 5

I recommend that the District of Saanich implement a comprehensive privacy management program to ensure it is able to meet all of its obligations under the *Freedom of Information and Protection of Privacy Act*. This program should include the appointment of a Privacy Officer.

The Privacy Officer should conduct a comprehensive audit of the District's compliance with the *Freedom of Information and Protection of Privacy Act*, and compile a registry of all personal information in the custody or under the control of the District.

The District should provide training to all employees in relation to all requirements of the *Freedom of Information and Protection of Privacy Act*.

7.0 CONCLUSION

Public bodies and organizations have a legal obligation to consider privacy issues in any assessment of appropriate IT security measures. While FIPPA requires that public bodies take reasonable security measures to protect personal information, it contains many more requirements intended to ensure that public bodies collect only the minimal amount of personal information that is necessary.

One of the easiest ways to ensure compliance with the requirements in FIPPA is to reduce the amount of personal information requiring protection by only collecting that which is absolutely necessary. Indeed, as has been seen in this investigation, security measures taken by the District may have resulted in a net reduction to IT security by concentrating the personal information of key employees and officers in one location, creating a "honeypot" for external attackers. It is critically important that public bodies consider both privacy and security in order to ensure compliance with provincial privacy law.

The information collected by keystroke logging and screenshot capturing will not help prevent or detect a security breach. It will only facilitate a purely reactive security strategy, helping IT staff to close security holes after a breach has already occurred; in effect closing the proverbial barn door after the horses have left. While this strategy can tell you what was stolen by an internal user, it is not an effective security control against malware or external attackers. All of the major IT threats faced by public bodies can be more effectively protected against with other more commonly used software tools.

The level of employee surveillance that results from keystroke logging and screenshot capturing should be restricted to use in specific investigations, based on reasonable grounds for suspicion of wrongdoing, and only when other less privacy intrusive measures have been exhausted.

Above all, this investigation demonstrates the need for public bodies to have an effective privacy management program in place to help avoid instituting practices that will place them in contravention of FIPPA, and waste valuable resources in terms of time and money.

The District of Saanich's senior staff and staff of other municipalities must become knowledgeable of the privacy rights of their employees, elected officials and citizens and use the analytical tools available to identify the privacy impacts of programs and initiatives. It is my hope that the District and other municipalities move forward in a more privacy responsible manner.

8.0 ACKNOWLEDGEMENTS

The District of Saanich cooperated fully with my Office's investigation.

I would like to thank Bradley Weldon, Senior Policy Analyst, and David Nicholson, IT Policy Analyst, who conducted this investigation and contributed to this report.

In addition I would like to thank Vern Byggdin, Byggdin Ventures Inc., and Michael Argast, Director, TELUS Security Solutions who contributed their technical knowledge and expertise to this investigation.

March 30, 2015

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia