SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT F-2013-003

Ministry of Highways and Infrastructure

Summary: The Office of the Saskatchewan Information and Privacy Commissioner (OIPC) received an email from the Chief Privacy Officer at Saskatchewan Government Insurance (SGI) in September 2010 stating that an employee of another government institution, the Ministry of Highways and Infrastructure (MHI), had "incorrectly accessed" SGI's database. According to MHI's internal Privacy Breach Report, an employee of MHI was travelling to work when an incident occurred between him and another driver. After the incident, the MHI employee used his user privileges to view the other driver's personal information on the SGI database and used the information to contact the other driver. MHI's Privacy Officer was notified of the privacy breach. Instead of MHI providing breach notification, SGI notified and apologized to the affected individual. The Commissioner found that it should have been MHI that took responsibility for the privacy breach. The Commissioner made recommendations to MHI on how to prevent similar privacy breaches from occurring again in the future, including auditing its employees' use of the SGI database.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, ss. 2(1)(d)(i), 24, 24(1)(e), 24(1)(k), 24(2)(e), 25, 28, 29, 33; *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1, s. 17(1)(a); *The Health Information Protection Act*, S.S. 1999, c. H-0.021, s. 16; *The Motor Carrier Conditions of Carriage Regulations* c. M-21.2 Reg. 5, s. 2(b.1).

Authorities Cited: Saskatchewan OIPC Review Report: 92-018; Saskatchewan OIPC Investigation Reports: F-2012-001; H-2013-001; H-2010-001.

Other Sources Cited: Saskatchewan OIPC, *Helpful Tips: Privacy Breach Guidelines*; Ministry of Justice, Access and Privacy Branch, *Personal Information Sharing Agreements (Government to Government) Best Practices Guidelines*; Public Sector Chief Information Officer Council, Privacy Subcommittee, *Government-to-Government Personal Information Sharing Agreements: Guidelines for Best Practice*; Ministry of Health, Pharmaceutical Information Program.

I BACKGROUND

[1] My office received an email dated September 23, 2010 from the Chief Privacy Officer at Saskatchewan Government Insurance (SGI) stating that an employee of another government institution had improperly viewed information from the SGI database. The email read:

> I am following up on my email of September 3, 2010 regarding a possible breach of SGI's database.
>
> Our investigation revealed that a third party government ministry's staff member incorrectly accessed SGI's database. I understand that Ministry has contacted your office to advise of the breach. That staff member has been subject to discipline by the government agency and SGI has pulled that staff persons [sic] entitlement to access our database.
>
> The complaint [sic] (the customer whose information was accessed) has been advised of the breach an apology has been extended and the customer is informed that corrective measures have been taken to prevent a further incident.

[2] The Privacy Officer at the Ministry of Highways and Infrastructure (MHI) followed-up SGI's email by sending an email to my office, also dated September 23, 2010:

> In follow up to [name of SGI's Chief Privacy Officer], the Ministry of Highways and Infrastructure has not notified your office regarding this breach. In past discussions with [name of SGI's Chief Privacy Officer], this incident was going to be communicated to your office by SGI.

[3] I responded by email to MHI's Privacy Officer on the same date as follows:

> I appreciate the notification from SGI but it appears that it wasn't a breach by an SGI employee but a breach by an employee of your Ministry and therefore your Ministry would be responsible and accountable for same.
>
> I assume that you have done an internal breach investigation. Can you please provide us with a copy of that investigation report?

[4] My office received a memorandum dated September 23, 2010 which enclosed a copy of MHI's internal Privacy Breach Report dated September 9, 2010.

[5] Below is an account of the incident according to the MHI Privacy Breach Report.

[6] On September 2, 2010, an employee of MHI was travelling to work in his personal vehicle on a Saskatchewan highway when he had an incident with another driver. The other driver (the Driver) was not driving a commercial vehicle. The incident was not work-related. This will be significant in the discussion portion of this Investigation Report.

[7] The employee, a Traffic Officer of the Transport Compliance Branch (TCB) at MHI, apparently wanted to know why the Driver was upset during the incident on the highway. Therefore, the employee looked up the Driver's personal information on the SGI database and contacted the Driver.

[8] The Driver called the Royal Canadian Mounted Police (RCMP) and SGI to complain. The TCB of MHI was contacted by the RCMP. SGI contacted the MHI Privacy Officer.

[9] In regards to what personal information was involved in this particular privacy breach, MHI reported in the MHI Privacy Breach Report the following: "The information obtained from the electronic SGI database would include the driver's name and address, driving history and associated vehicles registered to the driver."

[10] I wrote a letter to MHI dated October 19, 2010 that stated the following:

> **…my concern is the way that notification to the affected individual and to our office was handled. The fact that your organization hasn't communicated with the affected individual and apparently hasn't accepted responsibility for notification is inconsistent with privacy best practices.** If the SGI notice isn't clear about who was responsible for the breach, I would recommend that you immediately provide such a notice together with an apology from your Ministry.
>
> [emphasis added]

[11] In its letter dated November 4, 2010, MHI describes SGI as the "owner" of the information and provides an explanation as to why SGI sent notification to the affected individual, instead of itself:

> **We are unable to provide you with a copy of the notification to the affected individual which you requested.** When the incident occurred, Saskatchewan Government Insurance (SGI) was the only government representative contacted. At no time was the Ministry of Highways and Infrastructure (MHI) in discussion with the affected individual. This is part of the reason MHI collaborated with SGI on an apology strategy. It was agreed by both SGI and MHI that the person contacted would offer the apology on behalf of the government and on behalf of MHI. **The decision to have the owners of the data (SGI) provide notification was deemed more appropriate since MHI had not been provided the complainant's private information and the individual would be assured their private information had not been circulated to more people.** SGI has confirmed that the complainant was satisfied with a verbal apology.
>
> [emphasis added]

[12] My office requested further information from MHI in a letter dated September 14, 2011. The letter read:

> Thank you for indicating the measures MHI has taken to review policy with Traffic Control Board (TCB) staff via reading and signing off on TCB SGI policy, reviewing training lesson plans regarding compliance, and by providing local training. A question that still remains is whether policy is sufficient and clear enough to assist employees in their awareness of allowable uses of the SGI database. Please forward a copy of MHI's policy as well as a copy of the information sharing agreement between the MHI and SGI that would drive this policy. Secondly, is there a better means of obtaining the information needed by TCB and/or MHI to do its mandated work other than through the SGI database? Alternately, is there a better computer access limitation system that would authorize only the information necessary to perform required tasks?

> Another consideration is the importance of staff awareness of the Privacy Officer and their role with the MHI. Please advise what steps were taken to advise Traffic Officers who have access to the SGI database about *The Freedom of Information and Protection of Privacy Act* (FOIP) and that you are the Privacy Officer responsible for overseeing its' administration. I note that the importance of compliance with SGI policy will be reviewed, but no mention is made of a FOIP review or information about the role of the Privacy Officer at MHI. This would include information about where to direct individuals who have questions or concerns about collection, use or disclosure of personal information or privacy in general.

[13] My office received a letter dated October 19, 2011 from MHI which enclosed relevant documents including *The Agreement Concerning Driver/Vehicle Registration Information* (the Agreement) between SGI and MHI signed June 8, 2009, a policy, and service directives. These documents will be discussed below.

II ISSUES

1. Is the information in question "personal information" as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act*?

2. Did the Ministry of Highways and Infrastructure properly collect and use the personal information in question?

3. Which government institution is responsible for the breach?

4. Did the Ministry of Highways and Infrastructure respond appropriately to the privacy breach?

III DISCUSSION OF THE ISSUES

[14] Section 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP)[1] defines a "government institution" as follows:

[1] *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (hereinafter FOIP).

> **2**(1) In this Act:
>
> …
>
> (d) **"government institution"** means, subject to subsection (2):
>
> (i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or

[15] Therefore, MHI is a government institution for the purposes of FOIP.

[16] My authority to investigate the identified issues is found in section 33 of FOIP which states as follows:

> **33** The commissioner may:
>
> …
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.

1. Is the information in question "personal information" as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act*?

[17] Section 24 of FOIP defines "personal information" as follows:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> (c) **Repealed.** 1999, c.H-0.021, s.66.
>
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;

(e) the home or business address, home or business telephone number or fingerprints of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

(k) the name of the individual where:

(i) it appears with other personal information that relates to the individual; or

(ii) the disclosure of the name itself would reveal personal information about the individual.

(1.1) "Personal information" does not include information that constitutes personal health information as defined in *The Health Information Protection Act*.

(2) "Personal information" does not include information that discloses:

(a) the classification, salary, discretionary benefits or employment responsibilities of an individual who is or was an officer or employee of a government institution or a member of the staff of a member of the Executive Council;

(b) the salary or benefits of a legislative secretary or a member of the Executive Council;

(c) the personal opinions or views of an individual employed by a government institution given in the course of employment, other than personal opinions or views with respect to another individual;

(d) financial or other details of a contract for personal services;

> **(e) details of a licence,** permit or other similar discretionary benefit **granted to an individual by a government institution**;
>
> (f) details of a discretionary benefit of a financial nature granted to an individual by a government institution;
>
> (g) expenses incurred by an individual travelling at the expense of a government institution.
>
> (3) Notwithstanding clauses (2)(e) and (f), **"personal information"** includes information that:
>
> (a) is supplied by an individual to support an application for a discretionary benefit; and
>
> (b) is personal information within the meaning of subsection (1).
>
> [emphasis added]

[18] According to section 17(1)(a) of *The Freedom of Information and Protection of Privacy Regulations*,[2] only the Driver's name and address can be considered "driver licence information".

[19] Previous Saskatchewan Information and Privacy Commissioner McLeod stated in his Report 92-018:

> Where the predominant purpose is to record information about a motor vehicle, it would seem to me that the name and address of the person in whose name the vehicle is registered should be considered to be information about a vehicle rather than personal information about an individual within the meaning of the Act.[3]

[20] The Driver's name and address in SGI's database would be considered driver's license information and therefore *not* personal information in accordance with section 24(2)(e) of FOIP.

[21] However, other information viewed by the MHI employee would be considered personal information. This would include the Driver's history and vehicles registered to the

[2] *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01 Reg. 1.
[3] Office of the Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC) Report 92-018 at p. 5.

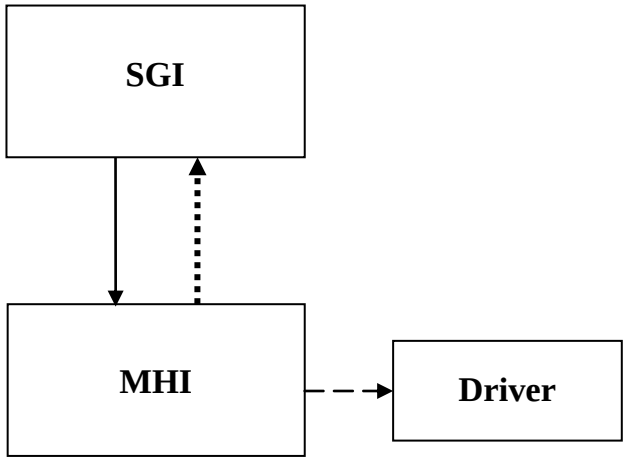
Driver because the information is about an identifiable individual that is personal in nature.

[22] MHI's Privacy Breach Report states that the employee used the information viewed from the SGI database to contact the Driver. Presumably, the MHI employee contacted the Driver by telephone. In accordance with sections 24(1)(e) and 24(1)(k) of FOIP, the telephone number of the Driver is the Driver's personal information.

2. Did the Ministry of Highways and Infrastructure properly collect and use the personal information in question?

[23] I need to determine whether MHI's "collection"[4] and "use"[5] of the information in question was proper.

[24] Below is a diagram to illustrate MHI's collection and use of personal information in this case:



Arrow	Description
→	SGI disclosed Driver's personal information to MHI
⇢	MHI collected Driver's personal information from SGI
- - →	MHI used Driver's personal information to contact Driver

[4] I defined the term "collection" in my Investigation Report F-2012-001 at [16] and [17], available at: www.oipc.sk.ca/reviews.htm.
[5] I defined the term "use" in my Investigation Report H-2013-001 at [36], available at: www.oipc.sk.ca/reviews.htm.

[25] The personal information involved in this file is stored in a database in the possession or control of SGI. Therefore, when MHI views information from the database, SGI is disclosing[6] the personal information and MHI is collecting it. This would be similar to what is described in my Investigation Report H-2010-001 where the Ministry of Health (Health) is the trustee of personal health information stored in the Pharmaceutical Information Program (PIP)[7] database. Every time a pharmacist views personal health information from PIP, it is a disclosure by Health and a collection by the pharmacist:

> [89] Saskatchewan Health is the trustee responsible for PIP and the action of pharmacists uploading prescription data to the [electronic health record] is a disclosure by those pharmacists. Saskatchewan Health, in the same transaction, is collecting personal health information. When a pharmacist downloads or views PIP data, this is a disclosure of personal health information by Saskatchewan Health and a collection by the pharmacist or pharmacy.[8]

[26] The purposes for which MHI collects and uses personal information from SGI are outlined in the Agreement between SGI and MHI. The Agreement states:

> Information
>
> 1.1 SGI will provide:
>
> a) Driver Licence and registration information (hereinafter "the information") as defined in section 17 of [T]he Freedom of Information and Protection of Privacy Regulations, R.R.S., c. F-22.01 Reg 1;
>
> b) Photo identification information as defined in clause 31(b) of [T]he Traffic Safety Act S.S. 2004, c. T-18.1; and
>
> c) Traffic Accident Information System (TAIS), Carrier Profile System and Transportation Permit Issuing System.
>
> Use of Information
>
> 2.1 **The Ministry will use the information only for the purpose of the business arising from its Transport Compliance and Operations Divisions**, as follows:
>
> a) To support authorized law enforcement investigations and related proceedings undertaken by the Transport Compliance Branch in accordance with federal and provincial legislation relating to commercial vehicle operations;

[6] *Ibid.* at [36] I defined the term "disclosure".
[7] Ministry of Health, Pharmaceutical Information Program, available at: www.health.gov.sk.ca/pip.
[8] SK OIPC Investigation Report H-2010-001 available at: www.oipc.sk.ca/reviews.htm.

b) To validate vehicle registrations and confirm driver qualifications for trucking program participation currently managed by the Partnership, Programs and Services Branch.

c) To investigate abandoned vehicles which are subject to the ministry's jurisdiction and the responsibility of the Operations Division.

[emphasis added]

[27] Since SGI is disclosing personal information to MHI, MHI is collecting personal information when it views information from the SGI database.

[28] Section 25 of FOIP states the following in regards to a government institution collecting personal information:

> **25** No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

[29] The MHI Privacy Breach Report stated that the employee collected the personal information of the individual from the SGI database "to ascertain why [the Driver] was upset since they never had an opportunity to meet and discuss the situation." Clearly, such a purpose is not related to an existing or proposed program or activity of MHI. Further, the MHI Privacy Breach Report stated that TCB Traffic Officers are only authorized to use the SGI database for the purpose of carrying out their duties of commercial vehicle enforcement. Therefore, the collection of the personal information, in this case, is in contravention of section 25 of FOIP.

[30] As stated earlier, the employee used the Driver's information from the database to contact the Driver for what appears to be personal reasons. Since I found that the purpose for the collection is in contravention of section 25 of FOIP, any consequential use cannot be justified under FOIP.

[31] Further, such a use is also in violation of the Agreement between SGI and MHI. The applicable portions of the Agreement state as follows:

4.5 The Ministry acknowledges and confirms that the information disclosed or accessed by it is confidential and **is being disclosed to the Ministry for the business purposes of the Ministry identified in this agreement.** The Ministry acknowledges that SGI and the Ministry have a statutory obligation to protection information under its control. Accordingly the Ministry agrees to take all reasonable steps to establish and maintain safeguards of the information, and to ensure that the information received will not be used in any way inconsistent with the laws or regulations of the Province of Saskatchewan, or Canada. Accordingly, the Ministry agrees:

a) to protect information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification in accordance with any safeguards and appropriate to the sensitivity of the information.

…

c) to only use information for the Ministry's business purposes as identified in this agreement;

…

j) not to use information for its own benefit or the benefit of third parties, other than allowed for by this agreement;

k) not to disclose information or the fact of its existence and use by the Ministry to any third party, without the written consent of SGI;

l) not to disclose information to any other person other than employees of the Ministry, and then only on a need-to-know basis, and **to use its best efforts to inform those individuals of the requirements of [*The Freedom of Information and Protection of Privacy Act*]**, and to ensure that they are all bound by confidentiality obligations in favour of the Ministry.

m) to instruct its employees and agents who have access to any information of the restrictions placed upon such access, use and disclosure of the information by this agreement and **that unauthorized use, disclosure or copying thereof may result in both criminal and civil liabilities;**

…

o) otherwise to abide by and adhere to the provisions and requirements of [*The Freedom of Information and Protection of Privacy Act*] and any other applicable legislation.

…

6.1 **The Ministry agrees that it is fully and solely responsible for the actions of each of its employees, agents, partners, consultant and other persons with respect to the use, disclosure and storage of information received from SGI,** whether or not that person is or was acting within the scope of his or her employment, agency, consultancy or other relationship with the Ministry.

[emphasis added]

[32] The Agreement clearly states that information collected by MHI from the SGI database is to be used in accordance with FOIP. So, not only was the use of the contact information of the affected individual, the Driver, unauthorized under FOIP, it was unauthorized under the terms of the Agreement.

[33] I find that the collection and use of the personal information in question was a privacy breach.

3. Which government institution is responsible for the breach?

[34] SGI was the government institution which issued an apology to the Driver. However, it was MHI which collected and used personal information in the SGI database for an unauthorized purpose that breached the Agreement and FOIP. Therefore, MHI would be the government institution responsible for the breach.

[35] SGI was the government institution that assumed responsibility for the privacy breach by apologizing to the Driver. MHI explained that it was "[d]eemed most appropriate for SGI, as owner of the information, to contact the complainant."

[36] Leaving aside the issue of whether anyone, other than the data subject, can 'own' the personal information, it is inappropriate for another government institution to take responsibility for a privacy breach committed by another.

[37] Further, the Agreement states MHI is "fully and solely responsible for the actions of each of its employees…with respect to the use, disclosure and storage of information received from SGI", as quoted earlier.

[38] My office's publication *Helpful Tips: Privacy Breach Guidelines* (Privacy Breach Guidelines),[9] recommends steps that can be taken to prevent privacy breaches from occurring again. It is unclear as to how a similar privacy breach can be prevented if SGI,

[9]SK OIPC *Helpful Tips: Privacy Breach Guidelines*, available at: www.oipc.sk.ca/resources.htm.

and not MHI, assumes responsibility for the privacy breach by issuing an apology to the Driver.

[39] As quoted earlier, I stated the following in my letter dated October 19, 2010 to MHI:

> **…my concern is the way that notification to the affected individual and to our office was handled. The fact that your organization hasn't communicated with the affected individual and apparently hasn't accepted responsibility for notification is inconsistent with privacy best practices.** If the SGI notice isn't clear about who was responsible for the breach, I would recommend that you immediately provide such a notice together with an apology from your Ministry.
>
> [emphasis added]

[40] This case is an unusual circumstance in that it appears that one government institution is purporting to assume accountability it does not have, yet the other government institution is shedding accountability in favour of the first government institution.

[41] MHI should have taken primary responsibility for this privacy breach and issued the apology to the Driver.

[42] I should note though that SGI had secondary responsibility in this particular case. It must take necessary steps to ensure that before disclosing personal information to a third party (i.e. MHI) that there is an agreement in place and that the third party is complying with the agreement.

4. Did the Ministry of Highways and Infrastructure respond appropriately to the privacy breach?

[43] My office's Privacy Breach Guidelines publication provides five steps to be taken by public bodies when responding to privacy breaches:

Step 1: Contain the Breach
Step 2: Investigate the Breach
Step 3: Assess and Analyze the Breach and Associated Risks
Step 4: Notification: Who, When and How to Notify
Step 5: Prevention[10]

[44] It appears that MHI partially completed the above steps. For example, the Traffic Officer's access privileges to information within the SGI database were restricted. MHI completed its Privacy Breach Report, containing a brief description of the privacy breach and the personal information involved. It also discussed some safeguards relevant to the situation, and next steps to be taken to manage the privacy breach.

[45] However, MHI failed to assess and analyze the breach and associated risks (Step 3), it failed to notify the Driver (Step 4), and it failed to create a comprehensive strategy to mitigate similar privacy breaches from occurring in the future (Step 5). Below, I will further discuss these three steps.

Step 3: Assess and Analyze the Breach and Associated Risks

[46] Step 3 of my office's Privacy Breach Guidelines provides guidance to government institutions on how to assess and analyze a breach and its associated risks.

[47] Section 28 of FOIP states that a government institution must not use personal information under its control without proper authority. Similarly, section 29 of FOIP states that a government institution must not disclose personal information in its possession or under its control without authority. In order to comply with the two provisions, a government institution must have physical, technical and administrative safeguards in place to ensure, as much as possible, that personal information will not be unintentionally used or disclosed without proper authority.

[48] Section 16 of *The Health Information Protection Act* (HIPA),[11] imposes on trustees the duty to protect as follows:

[10] *Ibid.* at pp. 5 to 12.

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[49] I note that FOIP does not have a provision such as above, but nonetheless the duty to protect information is implicit in FOIP.[12]

[50] Section 16 of HIPA identifies three types of safeguards: administrative, technical, and physical. However, it appears that the MHI Privacy Breach Report only contemplates two of three types of safeguards: physical and technical.

a. Physical Safeguards

[51] In this particular incident, physical safeguards do not appear to be at issue.

b. Technical & Administrative Safeguards

[52] MHI stated the following in its "Safeguards" section of the Privacy Breach Report:

> Describe **technical** security measures *(encryption, password, other)*:

[11] *The Health Information Protection Act*, S.S. 1999, c. H-0.021.
[12] *Supra* note 4 at [89], I made a similar comment with respect to FOIP.

> All computer access within TCB is password protected so that only authorized TCB staff can access the computer. SGI issued user ID & password must be entered in order to access the SGI database.
>
> [emphasis added]

[53] In terms of technical safeguards, MHI's Privacy Breach Report stated that user IDs and passwords are used to protect the information in the SGI database. However, there is no mention of any form of monitoring or auditing by MHI.

[54] The Ministry of Justice, Access and Privacy Branch released an advisory for government institutions and local authorities in December 2008 entitled *Personal Information Sharing Agreements (Government to Government) Best Practice Guidelines*.[13] It referred to guidelines called *Government-to-Government Personal Information Sharing Agreements: Guidelines for Best Practice* (Information Sharing Agreement Guidelines) developed by the Privacy Subcommittee on behalf of the Public Sector Chief Information Officer Council. The Information Sharing Agreement Guidelines state the following in regards to audits:

> **It is best practice to monitor the effectiveness of the agreement. This is done through IT audit trails, self-assessments, audits, verification systems and measurement techniques related to your government's obligations in the agreement.**
>
> You would not normally engage in auditing of activities and responsibilities of the other party, relying instead on their commitment in the agreement to adhere to their legal and policy structure. Alternatively, this can be achieved through the use of providing assurances that the obligations are being met by means of self-assessments and written certificates of compliance exchanged periodically throughout the term of the agreement. However, your ISA [information sharing agreement] should include the right to investigate matters related to the other party in the event you deem it necessary and provide for termination if not satisfactory.
>
> It should be noted that monitoring itself could represent a privacy risk depending upon how it is conducted. Ensure that your oversight team has the proper credentials and authority to conduct monitoring and that the same safeguards used to protect personal information are used for agreement monitoring.

[13]Ministry of Justice, Access and Privacy Branch, *Personal Information Sharing Agreements (Government to Government) Best Practices Guidelines*, dated December 2008, available at: www.justice.gov.sk.ca/PISAG2G.

> Finally, do not forget to review your ISA files, on a regular basis, to ensure that each ISA is supported by complete, accurate and up-to-date records, and that you have followed sound information management practices (e.g., documenting all disclosures).[14]
>
> [emphasis added]

[55] The Agreement between MHI and SGI, referred to earlier, states as follows:

> Restrictions and Audit
>
> 3.1 The Ministry will not use any information provided hereunder for any purpose not specified in this agreement without the prior written approval of SGI.
>
> 3.2 It is understood between the parties that the Ministry will be subject to audit by SGI. **In this regard, the Ministry agrees to comply with SGI's reasonable requests for audit information and documentation to ensure compliance with this agreement.**
>
> Confidentiality, Disclosure and Safeguarding of Information
>
> 4.1 The parties agree that it is essential to the success of SGI that its business, affairs and information be kept in the strictest confidence.
>
> 4.2 "Information" means the information SGI will provide pursuant to paragraph 1.1 to the Ministry, or accessed by the Ministry, for the purposes of its business under this agreement, and includes photo identification information, and includes the definition of personal information under *The Freedom of Information and Protection of Privacy Act*.
>
> **4.3 "Safeguards" means any method or combination of methods that have been agreed between the parties to protect information from loss or theft, as well as unauthorized access, disclosure, copying, use or modification.**
>
> 4.4 The Ministry expressly acknowledge that, in the course of fulfilling its respective obligations under this agreement, it will be in receipt of, or be given access to, information from SGI.
>
> 4.5 The Ministry acknowledges and confirms that the information disclosed or accessed by it is confidential and is being disclosed to the Ministry for the business purposes of the Ministry identified in this agreement. **This Ministry acknowledges that SGI and the Ministry have a statutory obligation to protect information under its control.** Accordingly the Ministry agrees to take all reasonable steps to

[14]Public Sector Chief Information Officer Council, Privacy Subcommittee, *Government-to-Government Personal Information Sharing Agreements: Guidelines for Best Practice*, at p. 27, available at: www.iccs-isac.org/en/practice/privacy.htm.

establish and maintain safeguards for the information, and to ensure that the information received will not be used in any way inconsistent with the laws or regulations of the Province of Saskatchewan, or Canada. Accordingly, the Ministry agrees:

a) to protect information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification in accordance with any safeguards and appropriate to the sensitivity of the information.

b) to have its employees use safe user practices including, but not limited to, following appropriate access restrictions, guarding passwords, and changing passwords on a frequent and regular basis;

c) to only use information for the Ministry's business purposes as identified in this agreement;

d) to notify SGI immediately, in writing of any security breaches relating to information disclosed by SGI or accessed by the Ministry;

e) to information SGI of any request by an individual in respect of the existence, use or disclosure by the Ministry of information disclosed by SGI or accessed by the Ministry;

f) to inform SGI of any complaint regarding the information handling practices of the Ministry or in respect of any information;

g) to co-operate fully with SGI in respect of any inquiry or complaint from an individual or the Information and Privacy Commissioner of Saskatchewan in respect of the information;

h) upon request of SGI, to cease any and all use of the information disclosed to the Ministry by SGI, or accessed by the Ministry and to return the information to SGI or destroy the information in a manner agreed to by SGI;

i) upon SGI's request, to amend or update information disclosed by SGI where SGI had identified that there is an inaccuracy or incompleteness of information;

j) not to use information for its own benefit or the benefit of third parties, other than allowed for by this agreement;

k) not to disclose information or the fact of its existence and use by the Ministry to any third party, without the written consent of SGI;

l) not to disclose information to any other person other than employees of the Ministry, and then only on a need-to-know basis, and to use its best efforts to information those individuals of the requirements of [*The Freedom of Information*

> *and Protection of Privacy Act*], and to ensure that they are all bound by confidentiality obligations in favour of the Ministry.
>
> **m) to instruct its employees and agents who have access to any information of the restrictions placed upon such access, use and disclosure of the information by this agreement and that unauthorized use, disclosure or copying thereof may result in both criminal and civil liabilities;**
>
> n) to promptly notify SGI of any order, subpoena, demand, warrant or any other document purporting to compel the production of any information, including an order made pursuant to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT), and to tender to SGI a copy of its proposed response to the demand. Unless the demand has been time-limited, quashed or extended, the Ministry shall thereafter be entitled to comply with the demand to the extent permitted or required by law. If so requested by SGI, and at the expense of SGI, the Ministry shall cooperate with SGI in the defence of the demand.
>
> **o) otherwise to abide by and adhere to the provisions and requirements of [*The Freedom of Information and Protection of Privacy Act*] and any other applicable legislation.**
>
> 4.6 The Ministry's obligations under this agreement take effect as of the date of this agreement and survive until terminated by an agreement in writing between the SGI and the Ministry.
>
> **4.7 All records of the Ministry pertaining to the information disclosed by SGI, or accessed by the Ministry shall be open to inspection by SGI at any reasonable time for the purpose of ensuring compliance with this agreement.**[15]
>
> [emphasis added]

[56] It appears that SGI may audit MHI's use, but it is not apparent how MHI audits or monitors its own employees to ensure that they are only collecting and using information in compliance with FOIP and the Agreement. Without auditing and monitoring capabilities, it is unclear how MHI protects personal information accessed from the SGI database from unauthorized use. Further, in section 3.2 of the Agreement, it appears that MHI has agreed to provide "audit information and documentation" at SGI's request so that SGI can ensure MHI's compliance with the Agreement. It is unclear how MHI

[15]This quote of *The Agreement Concerning Driver/Vehicle Registration Information* (hereinafter the Agreement) between Saskatchewan Government Insurance and the Ministry of Highways and Infrastructure is for the purpose of completing an analysis of the administrative safeguards, and not for the purpose of analyzing the Agreement itself.

provides "audit information and documentation" without any apparent auditing or monitoring capabilities.

[57] Further, in my Investigation Report H-2010-001, I recommended random audits be done on a sustained basis of activities by pharmacists in their use of PIP. In that particular Investigation Report, I found that the pharmacist had viewed personal health information in PIP without proper authority.[16] Similarly, in this present case, the employee viewed information in the SGI database without proper authority. Therefore, in our letter dated November 23, 2012 to MHI, my office recommended that MHI carry out, on a sustained basis, random audits of its employees to ensure employees only view information within the SGI database in accordance with the Agreement between SGI and MHI. Since the database belongs to SGI, MHI should be working with SGI to the extent necessary so that MHI is able to audit and monitor its employees for compliance with FOIP and the Agreement between SGI and MHI.

[58] MHI responded in its January 8, 2013 letter by stating the following:

> SGI's database has built in measures that allow them to generate reports based on a block of time for any or all user searches which can be used to compare against other internal databases ensuring all queries are conducted specifically for government business. **MHI is currently reviewing the amount and frequency of reporting it would like to receive from SGI.**
>
> [emphasis added]

[59] My office sought clarification from MHI in a letter dated January 25, 2013, as follows:

> We require clarification if MHI is only considering receiving such reporting from SGI *or* if it is committed to implementing a process in which reports will be sent to MHI on a regular basis for the purposes of proactive, regular yet random auditing on its employees use. If it is committed, then we will require MHI to provide timelines as to when such a processed [sic] will be implemented.

[60] MHI responded in its April 15, 2013 letter by stating:

[16] *Supra* note 8 at [95] to [97] and [121].

> The Privacy, Access and Ethics Department of SGI informed the ministry that audit reports are available. However, the ministry was also informed the reports would be "incomprehensible" to parties external to SGI and SGI is not prepared to grant access to those audit reports to any external parties.

[61] I am confused by MHI's response. In its January 8, 2013 letter, it stated that it was reviewing the amount and frequency of reports generated by SGI that it would like to receive. However, in its April 15, 2013 response, it stated that the reports were incomprehensible to parties external to SGI and that SGI was not willing to provide such reports to external parties.

[62] Ultimately, my concern is that MHI does not have in place adequate safeguards, including auditing capabilities of its employees' collection and use of information from the SGI database. On April 23, 2013, my office emailed MHI seeking a resolution:

> If the audit reports are "incomprehensible" to external parties, then we need to know what the Ministry of Highways and Infrastructure (MHI) is doing on its own end to audit its employees. For example, MHI could create an internal logging process where an employee logs/records the personal information he/she views on the SGI database. The employee's supervisor could review such logs to ensure employees are only viewing the personal information in the SGI database they need to complete job duties. Also, the internal log could also be sent to SGI to be compared against SGI's audit reports. If there are discrepancies between MHI's internal log and SGI's report, then that could be cause for MHI to investigate and make sure the employee is only viewing personal information on the SGI database to fulfill job duties.

[63] I never received a satisfactory response from MHI to alleviate my concern.

[64] Finally, according to the Privacy Breach Report, MHI stated the following:

> TCB Traffic Officers are only authorized to use the SGI database for the purpose of carrying out their duties of **commercial vehicle enforcement**.
>
> [emphasis added]

[65] Under *The Motor Carrier Conditions of Carriage Regulations*,[17] a commercial vehicle is defined as follows:

[17] *The Motor Carrier Conditions of Carriage Regulations* c. M-21.2 Reg. 5.

> **2** In these regulations:
>
> …
>
> (b.1) **"commercial vehicle"** means any of the following vehicles:
>
> (i) a vehicle registered in Class A, C, D or LV having a gross vehicle weight exceeding 5 000 kilograms;
>
> (ii) a vehicle registered in Class PB or PS with a seating capacity, according to the manufacturer of that vehicle, of more than 10 persons including the driver;

[66] In its Privacy Breach Report, MHI reported that the Driver was not driving a commercial vehicle:

> The Transport Compliance Branch (TCB) Traffic Officer queried the SGI system to obtain the name of a driver that he had an incident with on [a Saskatchewan highway] when driving this own vehicle and travelling to work. The reason given by the officer for trying to contact the breached individual was only to ascertain why he was upset since they never had an opportunity to meet and discuss the situation. **The driver of the vehicle that was queried was not driving a commercial vehicle at the time of the above mentioned incident.** TCB Traffic Officers are only authorized to use the SGI database for the purpose of carrying out their duties of commercial vehicle enforcement.
>
> [emphasis added]

[67] However, the employee was still able to obtain the Driver's personal information by querying a non-commercial vehicle. It is not clear the extent of the SGI database that employees of MHI can access. They should be able to view only the information they require to fulfill job duties and only to the extent authorized by FOIP and the Agreement between SGI and MHI. In the case of TCB Traffic Officers, it appears they are only required to access information about commercial vehicles, not non-commercial vehicles. Therefore, in its letter dated November 23, 2012, my office recommended that MHI should work with SGI to come up with a technical solution that ensures TCB Traffic Officers may only conduct queries and access commercial vehicle information, and not information about non-commercial vehicles.

[68] MHI responded in a letter to my office dated January 8, 2013, stating:

> SGI's database is not set up to differentiate between the different classes of plates. Based on discussions with SGI significant time and expense would be required to implement this recommendation and is not realistic to implement. Therefore, the ministry's traffic officers continue to require full access to the database.

[69] My office, in its letter dated January 25, 2013, sought further information from MHI as to how it concluded that significant time and expense would be required to comply with my office's recommendation:

> We require details of how MHI came to such a conclusion that developing a technical solution so that MHI employees can only technically query and view information they require on the SGI database will not be realistic to implement. For example, how did MHI come to the conclusion that significant time and expense would be required? Would such time and expense cause undue hardship. If so, how? Provide details of who was consulted and their opinions of what would be required to develop a technical solution.

[70] MHI responded to my office in its April 15, 2013 letter stating:

> The Privacy, Access and Ethics Department of SGI states **SGI is not prepared to undertake technical changes necessary to limit the access of the ministry's Transport Patrol Officers to commercial vehicles only as it would only benefit a small group of users.** SGI states it is not possible to provide a cost to such an undertaking but that "the time and resources needed to do this would be significant".
>
> [emphasis added]

[71] I disagree that making technical changes would only benefit a small group of users. It would benefit all Saskatchewan residents who may have their personal information stored in the SGI database, and would ensure that only those who have a need-to-know may view their personal information.

[72] However, in the immediate case before us, if MHI is unable to have technical safeguards implemented, then administrative safeguards must be emphasized to compensate. In regards to safeguards, the Information Sharing Agreement Guidelines state:

1.5.4 Security measures

A major consideration for privacy risks are the security measures taken to safeguard the information. This includes the location of databases, storage methods, methods of transfer, use of technology and personnel assigned.

You should consult your security policy and security officials to identify security measures and procedures applicable to your jurisdiction and specific circumstances.

For instance, the Government of Canada requires that departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE) to protect the electronic communication of classified and Protected C information. Departments should encrypt Protected A and B information, when use of encryption is supported by a Threat and Risk Assessment. However, departments must encrypt Protected B information prior to transmitting it across the Internet or a wireless network.

Security can go beyond technical and physical measures. Administrative safeguards include limiting access to individuals who have the necessary authorization, allowing access only to those who have signed a written commitment to the privacy and security of the information and limiting access to staff and management who have received training in security awareness, practices and procedures.

Since good privacy is dependent upon responsible security safeguards, it is essential this factor is addressed by the ISA.[18]

[emphasis added]

[73] Administrative safeguards are not discussed in the "Safeguards" section of the MHI Privacy Breach Report but are discussed in the "Mitigation and Prevention" section of the Privacy Breach Report. It states as follows:

> An internal Service Directive will be sent to all TCB staff which will require them to read the TCB SGI policy and sign off electronically that they have read and understood the policy. Follow-up local training with all staff will be conducted via their Regional Managers. TCB officer training lesson plans will be reviewed to ensure the importance of compliance is emphasized.

[74] Written policies and procedures are a form of administrative safeguards. Further, training employees and ensuring they understand and comply with policies and procedures are another form of administrative safeguards.

[18] *Supra* note 13 at p. 16.

[75] In a letter to my office dated October 19, 2011, MHI stated the following:

> All our officers have completed an on line [sic] Access and Privacy Training Course for Saskatchewan Government Employees and a record of completion is on each individual officer's file. All our officers have also completed a test with a passing mark of 100% showing that they have read and understand all the attached information. The attached **five** documents explain how we inform and educate our officers in the use and restrictions of the SGI database.
>
> 1. a copy of the agreement that Highways has signed with SGI in regards to the use and restrictions of their database
>
> 2. policy 505-6-2 from **June 15 2004** which discusses our procedures for using the SGI database that includes a signature from our staff ensuring they have read and understood the SGI Information Systems Policy
>
> 3. Service Directive 2007-15 was a reiteration of policy 505-6-2 sent out **November 22 2007**
>
> 4. Service Directive 2008-18 was an update advising our staff of a SGI policy change **November 7 2008**
>
> 5. Service Directive 2010-04 was another update notification for the SGI database **February 10 2010**
>
> 6. Test results showing that our officers have read and understand [sic] all the above and completed an exam based on the information
>
> [emphasis added]

[76] The second item in the list is Policy 505-6-2 entitled *Transport Compliance Policy and Procedures Manual* (the Policy). The Policy states as follows:

> **ACCESS TO SYSTEM DATA BANK FILES:**
>
> Access to MVD [Motor Vehicle Division] Inquiry, IRE [Inter-Provincial Record Exchange System], Transportation Permit Issuers' System, or Carrier Profile information is accomplished through direct access via an internet connection or through requests to the Saskatchewan Environment's Provincial Enforcement Centre (EC).
>
> MVD Inquiry and/or IRE provides on-line computer access to the following files or categories in accordance with the terms and conditions of the SGI agreement:

- vehicle registration information
- driver licensing information (including photo identification)
- driver/carrier sanctions (suspensions, history)
- carrier profile information

Access to vehicle permit information from the Transportation Permit Issuer's System is obtained through requests, either by fleet net radio or telephone, to SGI's Permit Office.

CONFIDENTIALITY AND DISSEMINATION OF INFORMATION:

MVD Inquiry, IRE responses, Carrier Profile, and Transportation Permit information must be protected against disclosure to unauthorized agencies or individuals. Transport Compliance is not to further disseminate MVD Inquiry, IRE, Carrier Profile or Transportation Permit information except where that use is consistent with the carrying out of agency duties and responsibilities. MVD Inquiry, IRE, Carrier Profile or Transportation Permit information is to be used only for activities as provided by this agency through legislation.

Under no circumstances are any SGI information system inquiries or queries to be conducted for non-official use or for personal reasons.

All MVD Inquiry, IRE, Carrier Profile, and Transportation Permit hard copy waste must be burned, shredded or mulched to prevent disclosure to unauthorized persons.

As a condition of employment, all personnel are to read and sign page 2 of the document "Acknowledgement of Restrictions Respecting the Handling of SGI Information". This document is located in Appendix A of this section.

Upon termination of services, all personnel are to read and sign page 3 of the "handling of SGI Information" form located in Appendix B of this section. The signed form(s) will be placed in the respective personnel file.

Anyone found to have abused his/her access privileges will be subject to disciplinary measures.

PROCEDURE:

All information shall be guarded and considered confidential. The approved 10 codes shall always be used for this purpose.

Queries will be run when an officer is in the lawful execution of their duty. Random queries are not considered necessary for the purposes of achieving the [Transport Compliance Branch] mandate.

> **SYSTEM SECURITY / COMPLAINT PROCEDURES:**
>
> **Complaints of access violations shall be reported to the Director of Transport Compliance Branch. The Director will forward information concerning policy violations to SGI Information Systems branch and to the Assistant Deputy Minister, Policy and Programs Division. Transport Compliance shall investigate thoroughly and expediently all complaints of access violations. If the complaint is resolved, the results of the investigation, including corrective or disciplinary action taken, shall be reported to the Manager, Information Systems Branch, SGI.**
>
> [emphasis added]

[77] The Policy makes it known that using information in the SGI database for personal reasons is not allowed and subject to "disciplinary measures". However, any training and education of the Policy, appears to have taken place *before* the privacy breach occurred. For example, the service directives were sent out in 2007 and February 2010. The privacy breach occurred on September 2, 2010. Certainly, it is commendable to send out the service directive to make employees aware of the Policy. However, since the privacy breach occurred *after* the service directive was sent, there is an obvious need for more rigorous training on the policy to prevent similar breaches from occurring again. To that end, the MHI Privacy Breach Report stated that "[a]n internal Service Directive will be sent to all TCB staff which will require them to read the TCB SGI policy and sign off electronically that they have read and understood the policy". However, my office has not received any new service directive that was sent out after the privacy breach occurred.

[78] Further, it appears that MHI has a reactive approach to the misuse of information from the SGI database. For instance, complaints must be directed to the Director of TCB. Auditing, as discussed earlier as a technical safeguard, is a proactive measure to ensure compliance with the Policy, the Agreement and FOIP. MHI should be bearing the responsibility of ensuring its employees are using the information properly through audits, rather than relying on complainants whose personal information may have been breached to initiate action.

[79] The sixth item listed at [75] was never provided as an attachment to my office. However, as stated earlier, MHI states all employees receive 100% when they complete the "on line [sic] Access and Privacy Training Course of Saskatchewan Government Employees." Such training is commendable. However, it appears that such training is a one-time training for employees only. Ongoing and/or annual access and privacy training certainly would be beneficial in ensuring that access and privacy remains at the forefront of employees' minds, especially if their job duties require them to manage personal information.

[80] In its January 8, 2013 letter, MHI stated that it was considering providing additional privacy training to its employees:

> We currently have training in place for all new employees. All employees last received the training in 2010. Currently we do not have a policy that requires annual training but we are giving additional consideration to that as an option.

[81] In a letter dated January 25, 2013, my office stated it required a commitment from MHI to provide its employees with ongoing privacy training:

> If MHI and SGI are unable to develop a technical solution to ensure that MHI employees can only access the information they require on the SGI database, then it is imperative that MHI ensures employees receive frequent and regular privacy training that is comprehensive and that this training is provided along with regular auditing and monitoring. **Our office requires a commitment from MHI that it will require employees who have access to the SGI database to take regular and ongoing privacy training. Please advise if it will make such a commitment. If so, we will require details of how frequent training will be provided and to whom.**
>
> [emphasis added]

[82] MHI responded by stating the following in its April 15, 2013 letter:

> The Highway Transport Patrol of the ministry is tasked with the enforcement of commercial vehicle weight and dimensions; they are the only employees with access to the SGI database. Currently the ministry requires all new Transport Patrol Officers to take privacy training.

> **The ministry is prepared to have all employees with access to the SGI database to take privacy training on an annual basis.**
>
> [emphasis added]

[83] The training should be specific to the employees' duties and identify exactly what personal information and for what purposes he/she may collect, use and/or disclose that information. Since it appears there are limited technical measures to prevent employees from viewing all sorts of personal information in the SGI database, MHI should also explicitly state the parameters to which an employee should be viewing personal information from the SGI database and the consequences of overstepping such parameters.

Step 4 – Notification: Who, When and How to Notify

[84] Step 4 of our Privacy Breach Guidelines provides guidance to government institutions on deciding whether or not to provide notification of a privacy breach to affected individuals and how to contact them.

[85] SGI took on the responsibility of notifying the Driver. MHI stated the following in the MHI Privacy Breach Report in regards to notifying the Driver:

> SGI will be the agency that contacts the complainant **and informs him what steps have been taken to rectify the situation.**
>
> [emphasis added]

[86] It is unclear how SGI would be able to inform the Driver of the steps taken to ensure that the MHI employee, or any other employee, does not misuse information again in the future. It is MHI, not SGI, that is responsible for the actions of MHI employees.

[87] In my letter dated October 19, 2010 to MHI, I stated my concern was that MHI apparently had not accepted responsibility for notifying the Driver.

[88] In reply, MHI provided a letter dated November 4, 2010 to my office, which stated the following:

> We are unable to provide you with a copy of the notification to the affected individual which you requested. When the incident occurred, Saskatchewan Government Insurance (SGI) was the only government representative contacted. At no time was the Ministry of Highways and Infrastructure (MHI) in discussion with the affected individual. This is part of the reason MHI collaborated with SGI on an apology strategy. It was agreed by both SGI and MHI that the person contacted would offer the apology on behalf of the government and on behalf of MHI. The decision to have the **owners** of the data (SGI) provide notification was deemed more appropriate since MHI had not been provided the complainant's private information and the individual would be assured their private information had not been circulated to more people. SGI has confirmed that the complainant was satisfied with a verbal apology.
>
> [emphasis added]

[89] Certainly, the MHI employee should never have accessed the Driver's personal information, stored in the SGI database, for the reason noted. However, it was an MHI employee who accessed the personal information and misused it. It was MHI who breached FOIP and the Agreement between MHI and SGI.

[90] Therefore, MHI is the government institution which is responsible for the privacy breach, and should have apologized to the Driver for the misuse of personal information, not SGI.

Step 5 - Prevention

[91] Step 5 of my office's Privacy Breach Guidelines provides guidance as to how government institutions may help prevent similar privacy breaches from occurring again in the future.

[92] As a short-term strategy, MHI's Privacy Breach Report stated that the employee "was advised he would be restricted in his officer duties and his access to SGI information suspended." Further, as a long-term strategy, it stated that:

> An internal Service Directive will be sent to all TCB staff which will require them to read the TCB SGI policy and sign off electronically that they have read and

> understood the policy. Follow-up local training with all staff will be conducted via their Regional Managers. TCB officer training lesson plans will be reviewed to ensure the importance of compliance is emphasized.

[93] However, MHI provided no evidence that a service directive was circulated after the breach.

[94] Further, its letter dated October 19, 2011 to our office, MHI stated the following: "We have recognized when there have been breaches in the past and officers have been suspended from work as a result and their access privileges revoked."

[95] Disciplinary action, as stated in the Policy, is a necessary measure to take to ensure employee compliance when appropriate. However, the above quote provides my office with limited information and many questions. For example, the above quote seems to imply that privacy breaches have occurred multiple times in the past. Is the misuse of the information in the SGI database a chronic issue? What happens to employees when their suspension is served and they come back to work? Is there a re-training program? Is their access and use of personal information from the SGI database audited to ensure they are in compliance with the Policy, FOIP and the Agreement?

[96] Further, it is unclear to my office what disciplinary action was taken against the employee in this particular case. MHI's Privacy Breach Report stated the following:

> The Traffic Officer who did the query was identified immediately after the breach and brought before the Director of TCB and the Manager of Professional Standards and Quality Assurance. The incident was reviewed, statement taken, and **the Traffic Officer was informed that there would be an investigation into the incident.** The Officer cooperated; immediately admitting to his actions, admitting he was aware of the privacy policy and admitted to know what he did was wrong. **The next day the officer was advised he would be restricted in his officer duties and his access to SGI information suspended.**
>
> [emphasis added]

[97] Presumably, the results of the "investigation" referred to in the above quote would inform what disciplinary action would be appropriate for the employee. However, MHI did not

provide any details as to what disciplinary action it took against the employee, other than to restrict his duties and suspending his access privileges to the SGI database. It did not provide any information as to how it followed-up with the employee to ensure he complied with FOIP, the Policy, and the Agreement between MHI and SGI.

[98] Based on the fact MHI provided no evidence it circulated a service directive to its employees after the breach, as well as the lack of information as to how it managed the employee, I am unclear as to what MHI's long-term strategy is to help prevent similar breaches from occurring again.

[99] My office sent a letter dated November 23, 2012 to MHI recommending the following:

> We recommend that the Ministry of Highways and Infrastructure audit its employees' use of the SGI database randomly on a sustained basis to ensure employee are using personal information from the Saskatchewan Government Insurance database in accordance with *The Freedom of Information and Protection of Privacy Act* and the agreement between Saskatchewan Government Insurance and the Ministry of Highways. **Further, for employees who have been disciplined for the misuse of information in the Saskatchewan Government Insurance database, we recommend that the Ministry of Highways and Infrastructure regularly audit such employees for a reasonable period of time.**
>
> [emphasis added]

[100] MHI responded to my office in its letter dated January 8, 2013:

> MHI is currently reviewing the amount and frequency of reporting it would like to receive from SGI. **Any MHI employee who has misused information from the SGI database has had their privileges revoked requiring no further auditing.**
>
> [emphasis added]

[101] My office sought clarification in a letter dated January 25, 2013:

> We require clarification as to how employees with their privileges revoked fulfill their job duties. **Are the privileges revoked permanently?** Or, if the privileges to the SGI databases were not required to fulfill their job duties in the first place, then we require an explanation as to why privileges were provided in the first place.
>
> [emphasis added]

[102] MHI responded to my office in a letter dated April 15, 2013:

> No, privileges are suspended indefinitely but not permanently. **Employees with their privileges revoked depend on their colleagues to make any necessary inquires on their behalf.** Employees who have had their privileges revoked will be required to again complete privacy training and make written application to their supervisor for reinstatement of access privileges.
>
> All transport officers are required to have access to the SGI database to perform the full range of their job duties.
>
> [emphasis added]

[103] It is inexplicable how making an employee, whose privileges have been revoked, dependent on another employee to collect information from the SGI database on his/her behalf is congruent with the need-to-know principle.[19] Such an approach encourages employee snooping as employees would be viewing information he/she does not need to complete his/her job duties.

[104] It is reassuring that employees who have misused their privileges must complete privacy training and make written application to their supervisors to have their privileges reinstated. However, without auditing capabilities, MHI did not provide my office with evidence that it has sufficient measures to prevent and detect employee misuse.

IV FINDINGS

[105] I find that the Ministry of Highways and Infrastructure is the government institution with primary responsibility for this privacy breach.

[106] I find that the Ministry of Highways and Infrastructure did not adequately respond to and manage the privacy breach.

[19] *Supra* note 5 at [55].

[107] I find that the Ministry of Highways and Infrastructure collected and used personal information in contravention of *The Freedom of Information and Protection of Privacy Act*.

V RECOMMENDATIONS

[108] I recommend that the Ministry of Highways and Infrastructure work with Saskatchewan Government Insurance so that the Ministry of Highways and Infrastructure has auditing and monitoring capabilities of its employees' use of the Saskatchewan Government Insurance database.

[109] I recommend that the Ministry of Highways and Infrastructure audit its employees' use of the Saskatchewan Government Insurance database randomly on a sustained basis to ensure employees are using personal information from the Saskatchewan Government Insurance database in accordance with *The Freedom of Information and Protection of Privacy Act* and *The Agreement Concerning Driver/Vehicle Registration Information*.

[110] I recommend that the Ministry of Highways and Infrastructure work with Saskatchewan Government Insurance to implement a technical solution so that its employees may only collect and use the information they require to complete their job duties.

Dated at Regina, in the Province of Saskatchewan, this 28th day of November, 2013.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner