Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 101-2017

Saskatchewan Transportation Company

March 23, 2018

Summary: The Complainant emailed the Minister responsible for the Saskatchewan Transportation Company (STC) at a "saskparty.com" email address. The Minister responded from a "sasktel.net" email address which was a personal/business email account. The Complainant requested that the Commissioner investigate the matter. The Commissioner found that the Minister's office was not a "government institution" as defined by the former subsection 2(2)(b) of *The Freedom of Information and Protection of Privacy Act* (FOIP). As such, he found that he had no jurisdiction to investigate the matter. However, the Commissioner offered advice in the form of best practices with regards to the use of personal email for government-related activities.

I BACKGROUND

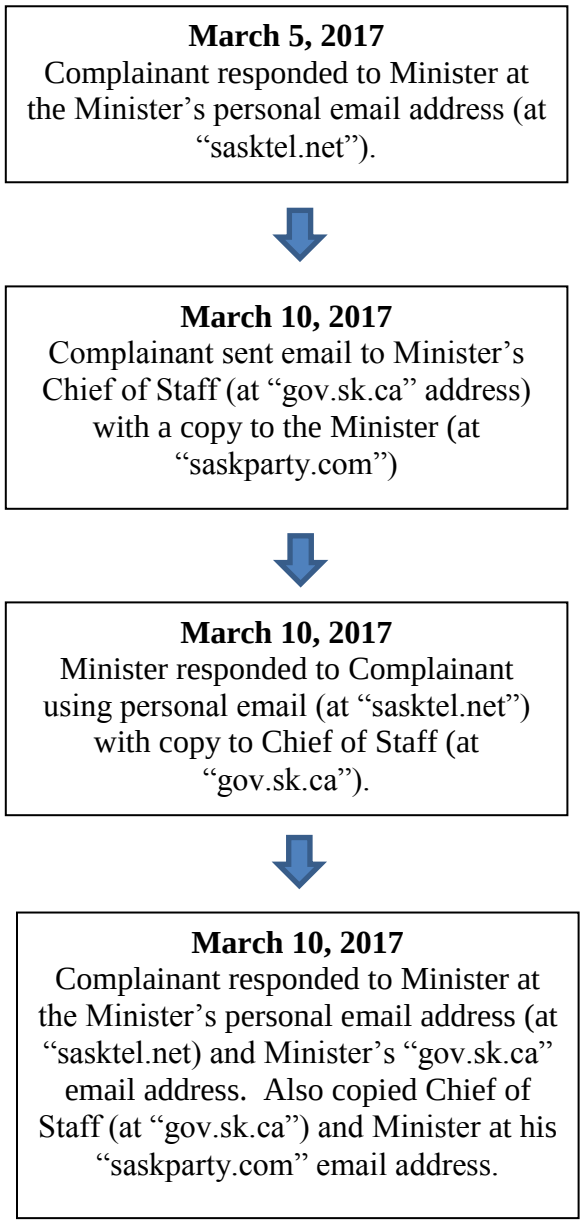
[1] On May 17, 2017, my office received a complaint from an individual asserting that the Minister responsible for the Saskatchewan Transportation Company (STC), responded to him using a personal email address. According to the complaint, the following occurred:

March 5, 2017
Complainant emailed Minister at his "saskparty.com" email address.

↓

March 5, 2017
Complainant received response from Minister from a personal email address (at "sasktel.net").

↓



[2] In this report, I refer to three different email addresses. The political email address means "saskparty.com". The government email address means "gov.sk.ca". The personal/business email address means "sasktel.net".

[3] Along with alleging his privacy was breached by the Minister using personal email and thus an unprotected server, the Complainant also included some of the following concerns:

- "…I am concerned the private email address used by the Minister may not be properly recorded in government record, which begs the issue of freedom of information access.

- I am concerned with both of whether both domains saskparty.com and sasktel.net have sufficient I.T. protections for government information transactions.

- I am concerned the Minister and his staff continued to use the sasktel.net address more than once in corresponding with me..."

[4] On May 19, 2017, my office notified Minister Hargrave's office that it would be undertaking an investigation into the complaint and requested a copy of its internal investigation report. On July 4, 2017, my office received a response which, in part, questioned my office's jurisdiction to investigate the matter.

II DISCUSSION OF THE ISSUES

[5] At the time of this complaint, STC was a "government institution" pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP). The STC will be dissolved on March 31, 2018.

1. Does my office have jurisdiction to investigate the matter?

[6] The Minister's office submits that my office does not have jurisdiction to consider the Complainant's allegation of a breach of privacy as a result of the Minister using a personal email address. The main thrust of this submission concerns subsection 2(2) of FOIP which exempted Ministers' offices as government institutions and therefore are not subject to FOIP.

[7] I note that on January 1, 2018, new amendments to FOIP came into effect which made Ministers' offices subject to the privacy provisions of FOIP. Subsection 3(4) of FOIP provides:

> **3**(4) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Executive Council and their employees as if the members and their offices were part of the government institution for which the member of the Executive Council serves as the head:
>
> (a) sections 24 and 24.1;
>
> (b) sections 25 to 30;
>
> (c) section 33.

[8] If the matter had occurred in 2018 following these amendments, the analysis would be different. However, given the fact it occurred in 2017, my office will address this issue based on the provisions existing in 2017 under FOIP.

[9] FOIP applies to government institutions. The Minister's office is questioning my office's jurisdiction based on the former subsection 2(2)(b) of FOIP which prior to the amendments established that a Minister's office was not a "government institution" and thus was not covered by FOIP:

> **2**(2) **"Government institution"** does not include:
>
> …
>
> (b) the Legislative Assembly Service or offices of members of the Assembly or members of the Executive Council;

[10] Under the former provision, a Minister's office was not a government institution, nor could it be said that it was part of one for purposes of FOIP.

[11] In Investigation Report 092-2015, I previously found that the Premier's office did not qualify as a government institution as defined by FOIP. This finding was based on the former subsection 2(2)(b) of FOIP.

[12] Therefore, I also find that the Minister's office was not a government institution as defined by the former subsection 2(2)(b) of FOIP. As such, my office has no jurisdiction to investigation this matter.

[13] However, as the matter involved a private business in Saskatchewan, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) may apply. The federal

Privacy Commissioner has jurisdiction over PIPEDA and organizations subject to it. The Complainant may wish to explore this avenue.

[14] Finally, this complaint involves the use of personal email for government related business. This has been an issue I have addressed in previous reports. Therefore, despite not having jurisdiction, there would be value in offering the following best practices.

2. Is there personal information involved?

[15] In order for the privacy provisions under Part IV of FOIP to be engaged, there must be personal information involved. It is important to note that it is not necessary to establish that all information involved is personal information. It is only necessary to establish that at least some of the information is.

[16] Subsection 24(1) of FOIP defines what qualifies as personal information. The Complainant's personal email address is present in the email chains. The email address contains the Complainant's name. I have found previously that personal email addresses qualify as personal information pursuant to subsections 24(1)(e) and (k) of FOIP, which provide 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:
>
> ...
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
>
> ...
>
> (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.

[Review Reports 157-2016 and 184-2016]

[17] Therefore, I find there is personal information of the Complainant's involved in this matter.

3. What are the best practices for protecting personal information when using email?

[18] The Minister's office advised that at the time of the incident, the Minister had three email accounts on his one Ministerial device and that his political party email was set to forward all emails to his personal/business email account. Further, my office was advised that during the time of the incident, the Minister's device was experiencing operating system problems which intermittently caused it to lock up, prevented him from accessing email and brought accounts together. In addition, my office was advised that the Minister sought IT assistance on more than one occasion to try to resolve the problems. I am advised that the final solution was to remove the accounts from the device and start again with only his Ministerial account and his MLA account remaining on the device. My office was advised that the Minister no longer has personal accounts on his ministerial device and that no accounts on the device forward to another account.

[19] The Minister has dealt with the issue and removed his personal/business account from his ministerial device. Citizens need to be assured that their personal information is not in the record holdings of a personal/business account. Neither should government records be. It is unclear if the email containing personal information has been recovered and deleted from the Minister's personal/business email account. If not, it should be, in order to contain the risk of unauthorized access to the Complainant's personal information.

[20] The use of personal email accounts by public servants for government-related activities raises various issues in terms of access to information and protection of personal information. I have addressed the issue in a number of previous review reports.

[21] In Review Report 051-2017, the issue of the former Premier using a personal email account and a "saskparty.com" email account for government business was addressed. I encouraged government leaders and employees to use the Government of Saskatchewan email system to do government-related activities.

[22] On May 15, 2017, in response to questions about the security of personal email accounts, the former Premier stated "As members of the House will know, I made a decision last week to simply be more focused and send all of my government-related emails on the government account. I think all of us in the House – officials and elected members – can redouble our efforts to do the same thing." (Hansard, May 15, 2017)

[23] In Review Report 184-2016, I addressed the issue of Global Transportation Hub (GTH) board members using personal email addresses to conduct government-related activities. Board members received sensitive government documents at personal email addresses. I recommended GTH board members use the Government of Saskatchewan email system for government-related activities. My office followed up with GTH on January 17, 2018, to get a progress report. GTH advised that it was working on sourcing and implementing a secure package for all board communications including the transmission of documents.

[24] In Review Report 216-2017, I again raised concerns when it was learned that public servants with the Ministry of the Economy (Economy) were using personal email accounts to conduct government-related activities. I recommended that Economy prohibit its employees from using their personal email addresses for government-related activities and require them to use government-issued email accounts only. In November 2017, Economy advised my office that it had implemented a policy prohibiting the use of personal email addresses for government-related activities.

[25] Other jurisdictions have also been dealing with this issue. For example, former British Columbia Information and Privacy Commissioner, Elizabeth Denham issued Investigation Report F13-04 which dealt with, in part, the use of personal email for government-related activities by government employees. In her Report she referred to the practice as "commonplace". Nova Scotia, Manitoba, Yukon, Ontario, Newfoundland and Labrador have also either issued reports or guidance documents on the issue.

[26] Personal email accounts pose information security risks for government records. For example, records could end up stored on email servers that are outside Canada. In instances where webmail services are used, such as Gmail or Hotmail, email content is

scanned and read in order to provide targeted advertising. Personal information in those records is not only stored outside Canada but it is also disclosed to the webmail provider. Government institutions are required under FOIP to take reasonable security measures to protect personal information from unauthorized access, collection, use or disclosure. When government records are stored in a personal email account with data servers located outside of Canada, the government no longer has control of how that information will be protected, disclosed, or accessed.

[27] In this case, the Minister's personal/business email account was a "sasktel.net" account. According to SaskTel's website, some SaskTel data is stored outside of Canada. Its website provides as follows:

> SaskTel uses Google Apps for email and collaboration and stores some data in the Google Cloud. It's important for you to understand that some SaskTel data is being stored outside of Canada and therefore may be subject to the laws of the countries where it resides…
>
> (https://www.sasktel.com/about-us/legal-and-regulatory/privacy-policy/data-storage-with-google)

[28] With the increased use of government assigned mobile devices and Bring Your Own Device (BYOD) programs, public servants are shifting from using the device for personal and government business increasing the risks of comingling information. Many public servants are unclear how to protect government records in such environments.

[29] Email is not confidential by default, and personal information included in an email could be subject to a breach or unauthorized disclosure. It is important to note that in many instances the technology used to send and receive email is not protected. Each delivery point between the recipient and the sender will store and forward the email and may do so in a plain, clear and readable format. While it may only be technical people at each delivery point who would have the ability to read the email, there is a possibility that the delivery point could be breached, resulting in personal information being exposed. (Canada's Health Informatics Association, *Putting it into Practice, 6E Working with Email*, 2010)

[30] Further, personal email providers might not have adequate protections for personal information. If the information is sensitive, encryption can ensure the email is not readable along its journey. Digital signatures ensure accuracy by preventing the email contents from being tampered with or altered. The email system should be secure and meet current industry standards. The International Organization for Standardization (ISO) is the leading authority on international standards. ISO recommends the following with regards to electronic messaging:

> **13.2.3 Electronic messaging**
>
> Control
> Information involved in electronic messaging should be appropriately protected.
>
> Implementing guidance
> Information security considerations for electronic messaging should include the following:
>
> a) protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization;
>
> b) ensuring correct addressing and transportation of the message;
>
> c) reliability and availability of the service;
>
> d) legal considerations, for example requirements for electronic signatures;
>
> e) obtaining approval prior to using external public services such as instant messaging, social networking or file sharing;
>
> f) stronger levels of authentication controlling access from publicly accessible networks.
>
> (ISO, *Information Technology*, ISO/IEC 27002, 2013)

[31] When outside the government network, emails may be intercepted, may not be backed-up and may not have strong passwords. The Government of Saskatchewan email system using the government network subjects those emails to the security measures in place within the government network, managed by the Ministry of Central Services (Central Services).

[32] A further consideration when using personal email is the principle of 'need-to-know' which underlies the privacy provisions of FOIP. *Need-to-know* means that only those with a legitimate need to know for purposes of delivering mandated services should have access to the personal information in the possession or control of a government institution. As soon as personal information is on an email account or server outside of the government network, maintaining the need-to-know principle becomes problematic when the information is potentially open to those outside the system (e.g. family, business partners and employees).

[33] Finally, the practice of using personal email for government-related activities threatens the proper functioning of FOIP which requires that public bodies respond to written access to information requests openly, accurately and completely. The use of personal email accounts by public servants makes this duty difficult to comply with because government may not be aware of the existence of emails on personal email accounts that are responsive to an access request.

[34] *The Archives and Public Records Management Act* (APRM Act) defines ministerial records as public records. As such, these records need to be retained, destroyed or transferred to the Provincial Archives of Saskatchewan as per the APRM Act. Using personal email for government-related activities runs contrary to this requirement as the records reside elsewhere. Government should be taking steps to ensure that it is consistently preserving records in the name of good governance as well as for the responsible preservation of documents that could be subject to future access to information requests.

[35] On January 1, 2018, new amendments to FOIP came into effect explicitly requiring government institutions to have adequate written policies and procedures that protect personal information against any reasonably anticipated threat or hazard to the security or integrity of the information. The policies and procedures must address administrative, technical and physical safeguards for personal information.

[36] The primary objectives of these policies and procedures can be found at subsection 24.1 of the newly amended FOIP:

> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> i. threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> ii. loss of the personal information in its possession or under its control; or
>
> iii. unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[37] In its submission, the Minister's office advised that Central Services was in the process of updating its government wide email management policy to more fully address classification and storage of government-related emails. It advised the updates will specifically address the use of personal/business email accounts while conducting government business.

[38] Further, it advised that once developed, part of the implementation of the email management policy anticipates an educational component which includes both online and in person training to public servants on the importance of information security, privacy and data protection. It added that this would include communicating with public servants in executive government that all government-related email messages must be stored on government-controlled systems. It anticipates providing advice and guidance to public servants on how to move any government-related email messages that may be located in their personal/business email accounts to a government-controlled system and how to destroy all copies that are located on those external systems. It also indicated that Central Services intends to engage my office in its training program.

[39] Finally, the Minister's office advised that the current Premier recently reminded his cabinet ministers of the importance of the issue of using personal email for government business by stating:

- that they are to use their government issued email address to conduct all government business;
- that any email sent by a member of the public to a private email account of a minister which involves government business should be sent to the appropriate email address to help ensure government business records are maintained as required under the APRM Act; and
- that forwarding any email with personal information to a private email account may not be permitted under FOIP and that the protection of privacy of Saskatchewan citizens is best served by using government servers.

[40] These are all very positive steps in addressing the broader issue of personal email being used for government-related activities. My office welcomes the opportunity to work with Central Services.

III FINDING

[41] I find I do not have jurisdiction in this matter, but have taken the opportunity to discuss best practices.

IV RECOMMENDATIONS

[42] I recommend the Minister follow best practice and not use his personal/business email address for any government-related activities. This would include continuing to ensure there is a clear separation between his personal/business email account and his ministerial and MLA accounts.

[43] I recommend the Minister or his staff follow best practice and review all emails on his "saskparty.com" and "sasktel.net" email accounts and ensure that all records created or held that relate to government business be moved into government controlled information

management systems with the original deleted from his "saskparty.com" and "sasktel.net" email accounts.

Dated at Regina, in the Province of Saskatchewan, this 23rd day of March, 2018.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner