Office of the Information and
Privacy Commissioner of Alberta

Investigation Report F2016-IR-02

Investigation into the unauthorized disclosure of public officials' cellphone records

August 10, 2016

Service Alberta and Executive Council

Investigations F8688 and 000712

Table of Contents

Introduction

[1] On August 25, 2014, the *Edmonton Sun* newspaper published an article highlighting former Deputy Premier Thomas Lukaszuk's data roaming charges from a trip to Poland and Israel in 2012.[1] The article included records showing the data roaming charges, which had been provided to the newspaper anonymously.

[2] Also on August 25, 2014, then-Premier Hancock expressed concern about the leak and said his government would look into whether internal government documents were leaked for political purposes. A spokesperson stated the government was "in the early stages of examining what options might be available to look into the matter."[2]

[3] At the same time, it was reported the Calgary Police Service was investigating the source of the leak as the documents that were sent to the newspaper apparently originated from an address in Calgary.[3]

[4] On October 22, 2014, Mr. Lukaszuk provided more detailed copies of the billing records to the Office of the Information and Privacy Commissioner (OIPC). This material had been included in the anonymous disclosure made to the newspaper and the newspaper had used it to establish the facts for the August 25, 2014 article.

[5] On November 20, 2014, then-Leader of the Opposition, Danielle Smith, publicly called for the Information and Privacy Commissioner (Commissioner) to investigate the matter.[4] Ms. Smith later wrote to the Commissioner on December 4, 2014 to ask for an investigation.

[6] On December 10, 2014, the Commissioner notified the Minister of Service Alberta that she was conducting an investigation into the disclosure of the data roaming records of the former Deputy Premier and other public officials (file F8688).

---

[1] Dykstra, M. (August 25, 2014). Alberta PC Leadership hopeful Thomas Lukaszuk dialed up $20,000 in data roaming charges on 2012 international trip. *Edmonton Sun*. Retrieved from http://www.edmontonsun.com/2014/08/25/alberta-pc-leadership-hopeful-thomas-lukaszuk-dialed-up-20000-in-data-roaming-charges-on-2012-international-trip.

[2] Retrieved from: http://www.cbc.ca/news/canada/edmonton/hancock-looking-into-leak-complaint-from-lukaszuk-1.2747313 and http://www.edmontonsun.com/2014/08/25/alberta-premier-concerned-about-leak-of-lukaszuks-20k-roaming-bill.

[3] Retrieved from: http://www.edmontonsun.com/2014/08/26/calgary-police-investigating-impersonation-following-leaked-pc-documents.

[4] Province of Alberta. (November 20, 2014). *Alberta Hansard, 28th Legislature, Third Session, Issue 4*. page 78. Retrieved from http://www.assembly.ab.ca/ISYS/LADDAR_files\docs\hansards\han\legislature_28\session_3\20141120_1330_01_han.pdf.

[7] The investigation was initiated on the Commissioner's own motion under section 53(1)(a) of the *Freedom of Information and Protection of Privacy Act* (FOIP Act), which reads:

> **General powers of Commissioner**
>
> 53(1) In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> (a) conduct investigations to ensure compliance with any provision of this Act…

[8] In deciding to investigate, the Commissioner considered the additional billing information, the Opposition's call for an investigation, and continued media and public interest. The Commissioner also considered the purposes of the FOIP Act, as stated under section 2, which include:

> 2 The purposes of this Act are
>
> …
>
> (b) to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information

[9] On April 29, 2015, the Commissioner extended the investigation to include the Executive Council Office (file 000712).

[10] The investigation's objectives included determining whether personal information was used or disclosed in contravention of the FOIP Act, and, if so, whether the public bodies that had custody or control of the personal information implemented reasonable safeguards to protect it. Determining who might have leaked the information was outside the scope of the investigation. None of the individuals affected by the disclosure asked the Commissioner to review the matter under section 65(3) of the FOIP Act.

[11] I was assigned to investigate this matter. This report outlines my findings and recommendations.

Application of the FOIP Act

[12] The FOIP Act applies to personal information in the custody or control of a public body. Both Service Alberta and Executive Council are "public bodies" within the meaning of section 1(p) of the FOIP Act.

[13] Section 1(n) of the FOIP Act defines personal information as follows:

> (n) "personal information" means recorded information about an identifiable individual, including
>
> (i) the individual's name, home or business address or home or business telephone number,

(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,

(iii) the individual's age, sex, marital status or family status,

(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

(vi) information about the individual's health and health care history, including information about a physical or mental disability,

(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else

[14] The records disclosed to the newspaper consist of three pages, containing the following information:

- Record 1: "Payment Invoices Listing". This record was published in the newspaper article of August 25, 2014 and shows long distance, data plan and other charges for five different invoice numbers. This record contains no personal information.

- Record 2: "Telus Wireless Charges", November 21, 2012. This record lists five cellphone numbers, plus the individual user names and charges associated with each number. Four individuals' names are listed in this record.[5] This record is signed by former Deputy Premier Lukaszuk, with the signature dated December 19, 2012.

- Record 3: "Data Services", dated December 14, 2012. This record shows a breakdown of the costs associated with one of the data services charges listed in Record 1. This record contains no personal information.

Records 1 and 3 appear to contain no personal information. Record 2, however, includes names and cellphone (i.e. telephone) numbers, which are "personal information" as defined in section 1(n) of the FOIP Act. It is a simple matter to link the data charges listed in Records 1 in 3 with the charges in Record 2, making the information in Records 1 and 3 identifiable. Therefore, I view the entire package of Records 1-3 as "personal information".

[15] The information at issue in Records 1-3 was in the custody or control of both Service Alberta and/or Executive Council and is personal information. Therefore, the FOIP Act applies to this matter.

[5] One of the individuals had a data plan as well as a cell phone plan. Therefore, there were five numbers, but four individuals affected.

Issues

[16] As noted earlier, one of the purposes of the FOIP Act is to control the manner in which a public body collects, uses and discloses personal information. This investigation's initial objectives included determining whether personal information was disclosed in contravention of the FOIP Act, and, if so, whether the public bodies that had custody or control of the personal information implemented reasonable safeguards to protect it.

[17] During the course of my investigation, I received information concerning Executive Council's use of the personal information at issue. An investigation opened on the Commissioner's own motion under section 53(1)(a) about compliance with any provision of the FOIP Act does not limit the Commissioner. Therefore, I considered the following issues in my investigation:

- Issue 1: Did the public bodies disclose personal information in compliance with Part 2 of the FOIP Act?
- Issue 2: Did Executive Council use personal information in compliance with the FOIP Act?
- Issue 3: Did the public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act?

Methodology

[18] In conducting this investigation I reviewed the records at issue, published media reports and Hansard from the relevant period. I exchanged written questions and answers with the FOIP Coordinators from Service Alberta and Executive Council. I spoke with Mr. Lukaszuk, former Premier Hancock, the Assistant Deputy Minister of Labour and Employment Practices for Corporate Human Resources, and a former Executive Assistant to the Premier's [Redford] Chief of Staff.

Analysis and Findings

Issue 1: Did the public bodies disclose personal information in compliance with Part 2 of the FOIP Act?

[19] Service Alberta confirmed that Records 1 and 3 were reports generated from the Electronic Payment System (EPS), which is an information system maintained and managed by Service Alberta and used throughout the Government of Alberta. Government departments can only access their own data in the system. Service Alberta also said that only Executive Council would have access to these reports in the particular format presented in Records 1 and 3. Service Alberta did not recognize Record 2 as one of its reports and said it does not create or maintain this type of report.

[20] Executive Council confirmed that it had loaded Record 2 into the EPS system, subsequently printed it and sent it to the Deputy Premier's Office (which is part of Executive Council) for

Mr. Lukaszuk's signature. Executive Council then filed the signed copy of Record 2 according to the applicable records management schedule.

[21] Both Service Alberta and Executive Council stated that they did not disclose the records at issue. In other words, neither public body decided to disclose these records to the newspaper and had no purpose for the disclosure. At the same time, these records containing personal information were, in fact, disclosed.

[22] Routine disclosures of government information may be authorized under section 88, Part 6, of the FOIP Act which states:

> 88(1) The head of a public body may specify categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act.
>
> (2) The head of a public body may require a person who asks for a copy of an available record to pay a fee to the public body, unless such a record can otherwise be accessed without a fee.
>
> (3) Subsection (1) does not limit the discretion of the Government of Alberta or a public body to release records that do not contain personal information.

[23] At the time the information was disclosed to the newspaper, the Government of Alberta had implemented its Expense Disclosure Policy and was routinely disclosing expenses from Ministers' Offices on its Public Disclosure of Travel and Expenses website, including those of the Deputy Premier. Executive Council provided evidence to show that it had paid the charges indicated in the records at issue in February 2013. The Deputy Premier's Office records are available for that month online[6] and show a "Goods, supplies and services and other expenses" entry of $22,621. The reason for this charge is not included and it is much higher than previous and subsequent monthly expenses under this entry. Anyone reviewing the Deputy Premier's Office records could have seen an unusually large entry for the month of February 2013, but would see no details and would not know who was responsible for the charges.

[24] As stated earlier, I concluded the information in Records 1-3 is "personal information" as defined under section 1(n) of the FOIP Act because it includes the names of the individuals who incurred the data plan expenses. Including individual names with the expenses, as was the case when the information was disclosed to the newspaper, made the information "personal information." This goes beyond what the Provincial Government had decided to routinely release through its Expense Disclosure Policy and needs to be considered in light of the legal authorities to disclose personal information listed under section 40 of the FOIP Act. In particular, section 40(1)(b) says:

> **Disclosure of personal information**
>
> 40(1) A public body may disclose personal information only
>
> …

[6] Retrieved from: http://www.servicealberta.gov.ab.ca/Minister_Expenses/depprem/February_2013.pdf.

(b) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17

[25] Section 17 of the FOIP Act prohibits disclosure of personal information unless the disclosure is not an unreasonable invasion of privacy. Specifically, the relevant parts of section 17 say:

> **Disclosure harmful to personal privacy**
>
> 17(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.
>
> (2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if
>
> …
>
> (e) the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body or as a member of the staff of a member of the Executive Council,
>
> (f) the disclosure reveals financial and other details of a contract to supply goods or services to a public body,
>
> …
>
> (4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
>
> …
>
> (d) the personal information relates to employment or educational history,
>
> …
>
> (g) the personal information consists of the third party's name when
>
> (i) it appears with other personal information about the third party, or
>
> (ii) the disclosure of the name itself would reveal personal information about the third party, or
>
> …
>
> (5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether
>
> (a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,
>
> (b) the disclosure is likely to promote public health and safety or the protection of the environment,
>
> (c) the personal information is relevant to a fair determination of the applicant's rights,

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

(e) the third party will be exposed unfairly to financial or other harm,

(f) the personal information has been supplied in confidence,

(g) the personal information is likely to be inaccurate or unreliable,

(h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and

(i) the personal information was originally provided by the applicant.

[26] Essentially, section 40(1)(b) of the FOIP Act authorizes the disclosure of personal information if it would not be an unreasonable invasion of personal privacy under section 17. Although there is a presumption against disclosure of personal information that relates to employment history, the Act is explicit that it is not an unreasonable invasion of privacy to disclose information about an individual's employment responsibilities as an employee of a public body or as a member of the Executive Council, or if the disclosure reveals financial and other details of a contract to supply goods or services to a public body. **Importantly, in determining whether a disclosure of personal information is an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all relevant circumstances, including those specifically set out in section 17(5).**

[27] In the case at hand, the personal information in Records 1-3 includes names and the fact that the individuals were employees of Executive Council. The information also includes financial details related to the individuals' cellphone and data plan charges, which were supplied on contract to Executive Council by a telecommunications company. A public body considering releasing this information might choose to redact the individuals' cellphone numbers, if these numbers were not otherwise available through a public directory. Alternatively, a public body might conclude that disclosing publicly paid cellphone numbers of public officials is not an unreasonable invasion of privacy. In either case, in deciding whether or not to disclose personal information, a public body is required to consider all relevant circumstances.

[28] This is consistent with the purposes of the FOIP act, as set out in section 2, which include "to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information".

[29] This controlled disclosure contemplated in the FOIP Act is reflected in section 17(1), where it says, "The head of the public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy." This means that the head of the public body (or their delegate) must consider a third party's privacy rights before making the disclosure. The head of a public body must consider the third party's privacy rights in responding to a formal access request, for example, or by setting policies relating to routine disclosures of information and the safeguarding of personal information. In this case, however, the information was disclosed without this consideration. Clearly, because there was no official intent or purpose behind

the disclosure, no head (or delegate) of either public body considered the release of the information in light of the four affected individuals' privacy rights.

[30] As there is no evidence that the disclosure of the personal information at issue was done in a controlled manner with due consideration of all relevant circumstances, the disclosure was not compliant with section 17 of the FOIP Act, and was not authorized by section 40(1)(b). I therefore conclude the personal information was disclosed in contravention of Part 2 of the FOIP Act.

[31] I next considered responsibility for the disclosure. The anonymous disclosure to the newspaper included Records 1, 2 and 3. As noted earlier, Record 2 was signed by former Deputy Premier Lukaszuk and filed at Executive Council. Service Alberta did not have access to Record 2. Executive Council stated, "Although some of the records at issue may have originated from EPS [a Service Alberta managed system, described earlier], the final version of the records at issue were strictly in a paper format created solely in Executive Council…". Therefore, in my view, it is more likely than not that the disclosure originated from within Executive Council. On a balance of probabilities, I find that Executive Council disclosed personal information in contravention of Part 2 of the FOIP Act. While this disclosure was not authorized by any Executive Council official, Executive Council is nonetheless responsible.

Issue 2: Did Executive Council use personal information in compliance with the FOIP Act?

Administrative Safeguards

[32] Section 39 of the FOIP Act sets out the purposes for which a public body may use personal information. Section 39 states:

> 39(1) A public body may use personal information only
>
> (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
>
> (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
>
> (c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.

[33] In the course of my inquiries concerning the disclosure of the Records, it occurred to me that Executive Council may have made efforts to reduce the roaming charges incurred, which could have required sending the records to other parties outside the expected circle of recipients involved with routine records storage. As such, I asked Executive Council to provide any related correspondence or records of discussions related to reducing the data roaming charges. Executive Council reported that it had no related records, but provided a statement outlining a sequence of events from October 2012 to March 2014. The statement says that Executive Council officials attempted to reduce the charges with the cellphone service provider until January 2013, but were unsuccessful. The statement indicates that the records at issue were then forwarded via then-Premier Redford's Chief of

Staff's Office to the Deputy Minister of Executive Council to obtain approval for payment in February 2013.

[34] According to Executive Council's statement, nothing further occurred with the records at issue until March 2014. At this time, the Executive Assistant to the then-Premier's Chief of Staff asked by phone for a copy of former Deputy Premier Lukaszuk's cellphone records from EPS from his time at Executive Council. An Executive Council Financial Coordinator retrieved the records, which were stored in paper format with the Executive Council's Financial Administrator on March 11, 2014. She then made copies and delivered them by hand to the Executive Assistant for the Premier's Chief of Staff.

[35] The circulation of the information in late 2012 and early 2013 as Executive Council attempted to reduce the roaming charges is understandable and for a recognized business purpose, consistent with the purpose for which the information was collected or compiled. Executive Council also provided documentation that supports the theory that the information was circulated for this purpose. However, the circulation of the information in March 2014 is curious. The information was requested by the former Premier's Chief of Staff's Office a year after the bill had been paid. In contrast to the earlier circulation of the information, Executive Council provided no explanation for the use of the information in March 2014. I contacted the former Executive Assistant to the Premier's Chief of Staff to ask about this use of the information. She remembered having requested the information but advised me she did not know the purpose, she was simply told to retrieve the information. I attempted to contact the former Chief of Staff to Premier Redford to clarify the purpose for which the records were requested, but was unsuccessful in reaching him.

[36] A public body may use personal information only as authorized by section 39 of the FOIP Act. In this case, Executive Council confirmed that paper copies of the records at issue were circulated within Executive Council in March 2014, a year after the invoice had already been paid. Executive Council did not explain the purpose for which the records were retrieved at this time, and there is no documentary evidence to support an authorized business purpose.

[37] As Executive Council did not explain its use of the personal information in March 2014, I find it was not authorized and in contravention of section 39 of the FOIP Act.

Issue 3: Did the public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as required under section 38 of the FOIP Act?

[38] Section 38 of the FOIP Act says:

> **Protection of personal information**
>
> 38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

[39] Section 38 requires that public bodies make reasonable security arrangements to protect personal information against a number of risks, including unauthorized use and disclosure. Section 38 includes the concept of reasonableness. This means that the security

arrangements do not need to be perfect. Unauthorized use and disclosure of personal information may still occur even when reasonable security arrangements have been implemented.

[40] Security arrangements should also be commensurate with the sensitivity of the personal information at issue and with the risk to individuals of inappropriate use and disclosure. In my view, the information at issue is of relatively low sensitivity. I considered the public bodies' security arrangements in this light.

[41] While I found that Executive Council is responsible for the unauthorized use and disclosure of the personal information at issue, both Executive Council and Service Alberta had a role to play in protecting the information. I will therefore consider the security arrangements in place at both public bodies.

Electronic Payment System

[42] Service Alberta maintains EPS on behalf of the Provincial Government. Records 1 and 3 originated from EPS. While Service Alberta did not recognize Record 2 as one of its reports, according to Executive Council, this record was uploaded into EPS before being printed and signed. Therefore, I considered the security arrangements in place to protect personal information stored in EPS.

[43] Service Alberta reported that information in EPS is protected through access controls. Only users in a specific department have access to that department's information. For example, only Executive Council can view or generate reports for Executive Council's purposes. Twenty seven Service Alberta staff members have administrator access to EPS for such purposes as setting up and decommissioning accounts, working with departments to resolve issues, providing training, and running reports. Service Alberta says that unless its staff members are investigating an invoicing issue, they would not view or print reports, such as the ones that are part of this investigation. Of note, the EPS does not generate audit logs that show whether information has been viewed or printed.

[44] Executive Council described the same access controls in place to protect information in EPS, also mentioning password protection, and a process to authorize users.

Paper Records

[45] Executive Council maintains that the records at issue must have been in a paper format at the time they were disclosed. Because of the expense sign-off process described by Executive Council [see paragraph 20] and the fact that former Deputy Premier Lukaszuk's signature appears on Record 2, I have accepted this assertion.

[46] While it establishes standards and policies for records management across government, Service Alberta is not directly responsible for maintaining Executive Council's paper records. I therefore concentrated on reviewing Executive Council's security arrangements to protect Records 1-3 while in paper format.

[47] Executive Council says these records were stored with its Corporate Services unit on the 6th floor of Park Plaza in Edmonton until July 2014, when they were moved to semi-active

storage space elsewhere in the building. Both locations are kept locked and protected with card readers, with limited access. Executive Council says six staff had access to Records 1-3 in paper format and the knowledge to locate them.

[48] The above describes the routine storage of the paper versions of the records at issue at Executive Council. However, I have previously noted that the records at issue were retrieved from records storage on March 11, 2014 and delivered by hand to the Executive Assistant to the Chief of Staff. Executive Council did not explain this use of the information, and I found it to be an unauthorized use.

Finding on Security Arrangements

[49] Overall, I observed a range of administrative, technical and physical arrangements in place to protect the information at issue stored in EPS and in paper records in Executive Council's custody. Considering the relatively low sensitivity of the specific personal information at issue (public officials' names, business phone numbers, data usage and related cellphone carrier charges), in my view, it would not be reasonable to expect the public bodies to have extraordinary measures in place. I find that reasonable safeguards were in place as required under section 38 of the FOIP Act.

[50] I make this finding despite the fact these safeguards did not prevent what appears to have been an unauthorized use of the information, and a deliberate, unauthorized disclosure. However, section 38 of the FOIP Act requires that safeguards be reasonable, not perfect, and reasonable safeguards may not be enough to protect against deliberate acts.

[51] In making this finding I note two important caveats. First, the security arrangements protecting the electronic versions of the records at issue in EPS are basic, not advanced. As observed above, many people had electronic access. Further, there is no audit capability to log who may have accessed or printed the information. As noted above, I considered the sensitivity of the personal information that was disclosed in this case and found that the basic security arrangements in place to protect that particular personal information were reasonable because that personal information is not inherently sensitive. However, Ministries and departments may store other, much more sensitive information in EPS. If this is the case, it may be that the safeguards in place are not reasonable to protect the information.

[52] Given this, I recommend that the two public bodies review the security arrangements to protect personal information in EPS in light of the sensitivity of all of the information stored in the system, and determine what, if any, additional safeguards should be implemented. In particular, the public bodies should consider whether the large number of authorized users and the lack of audit capability are commensurate with the sensitivity of the personal information in EPS and the potential risk of unauthorized use and disclosure.

[53] My second caveat relates to the security arrangements protecting the paper version of the information at issue. Paper records were retrieved and circulated within Executive Council in March 2014 and no notes were kept of why this was done, whether copies were made, or who the recipients were. There does not seem to be much protection in place to protect paper documents that are circulated within Executive Council. In this case, the personal information involved was not inherently sensitive from a privacy perspective. However, and

similar to the point in the above paragraph, there may be some risk that more sensitive personal information could be disclosed without authorization in future.

[54] I recommend that Executive Council review its handling of paper records to ensure that appropriate controls are in place to track and document the purposes for circulating sensitive personal information on paper to protect against the risk of unauthorised use and disclosure.

Additional Comments

Internal Investigation by the Government of Alberta

[55] As previously noted, in August 2014, then-Premier Hancock publicly stated that his government would look into whether internal government documents (the records at issue in this matter) were leaked for political purposes. A spokesperson stated the government was "in the early stages of examining what options might be available to look into the matter."[7] I interviewed former Premier Hancock and confirmed it was his government's intent to investigate the matter.

[56] I asked whether Service Alberta or Executive Council had conducted an investigation to discover the cause of the unauthorized disclosure. This is common practice in an investigation by the OIPC, as often public bodies, custodians or organizations conduct parallel internal investigations in order to be able to answer questions put to them by an OIPC investigator.

[57] In this case, both Service Alberta and Executive Council reported that they had no knowledge of any investigation, but suggested another public body may have been assigned this task.

[58] Ultimately, I was directed to the Corporate Human Resources (CHR) office of the Public Service Commissioner's Office, which falls under Treasury Board and Finance. I spoke to CHR's Assistant Deputy Minister (ADM) of Labour and Employment Practices, who was not aware of any documentation or active investigation work. The ADM informed me that CHR had considered doing an investigation, but had decided to hold off pending the results of the Information and Privacy Commissioner's investigation. Our Office was not consulted on this point and we did not request that the Provincial Government delay any investigation.

[59] To recap, the newspaper article about the data roaming charges appeared in the *Edmonton Sun* on August 25, 2014. As noted earlier, then-Premier Hancock indicated the Provincial Government's intent to investigate the matter within days. However, Premier Hancock only remained in power until September 15, 2014. The Commissioner launched this investigation on December 10, 2014. It appears that the Provincial Government took no action to investigate this matter for almost four months until it decided to hold-off conducting an investigation, after the Information and Privacy Commissioner announced her investigation publicly.

[7] Retrieved from: http://www.cbc.ca/news/canada/edmonton/hancock-looking-into-leak-complaint-from-lukaszuk-1.2747313 and http://www.edmontonsun.com/2014/08/25/alberta-premier-concerned-about-leak-of-lukaszuks-20k-roaming-bill.

Summary of Findings and Recommendations

[60] This investigation was triggered by the disclosure to media of information about the Deputy Premier's data roaming expenses. The investigation considered whether personal information was used and disclosed in contravention of the FOIP Act, and whether the public bodies that had custody or control of that personal information implemented reasonable safeguards to protect it. Notably, none of the four individuals affected by this disclosure asked the Commissioner to review the matter under section 65(3) of the FOIP Act, which would have afforded them additional rights, such as the ability to request an inquiry. Determining who might have leaked the information was outside the scope of my investigation.

[61] One of the core purposes of the FOIP Act is to control the collection, use and disclosure of personal information. In this case, I found there was no evidence that the disclosure of the personal information at issue was done in a controlled manner with due consideration of all relevant circumstances. The disclosure was not compliant with section 17 of the FOIP Act, and was not authorized by section 40(1)(b). I therefore concluded the personal information was disclosed in contravention of Part 2 of the FOIP Act.

[62] While both Service Alberta and Executive Council had custody and control of the information at issue, I concluded that the most likely source of the unauthorized disclosure was Executive Council.

[63] A public body may use personal information only as authorized by section 39 of the FOIP Act. In this case, Executive Council confirmed that paper copies of the records at issue were circulated within Executive Council in March 2014, a year after the invoice had already been paid. No explanation was provided as to why the records were retrieved from storage at this time, and there is no documentary evidence to support an authorized business purpose. As Executive Council was not able to demonstrate that its use of the personal information in March 2014 was authorized, I found the use to be in contravention of section 39 of the FOIP Act.

[64] Given the relatively low sensitivity of the personal information that was disclosed, I found that the basic security arrangements that protect the EPS and paper records management are reasonable as required under section 38 of the FOIP Act. However, I recommended that the public bodies review the security arrangements that protect the EPS to determine whether its basic level of security is appropriate to protect other more sensitive information that it may contain. I also recommended that Executive Council review its paper records handing processes with the same objective.

[65] I would like to thank the responding public bodies for their cooperation with this investigation.

Brian Hamilton
Director, Compliance and Special Investigations