Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

# INVESTIGATION REPORT F15-03

# ACCESS DENIED: RECORD RETENTION AND DISPOSAL PRACTICES OF THE GOVERNMENT OF BRITISH COLUMBIA

**ELIZABETH DENHAM**
**INFORMATION AND PRIVACY COMMISSIONER FOR BC**

**October 22, 2015**

CanLII Cite: 2015 BCIPC No. 63
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 63

# TABLE OF CONTENTS

# COMMISSIONER'S MESSAGE

Access to information rights can only exist when public bodies create the conditions for those rights to be exercised. Government must promote a culture of access, from executive leadership to front-line employees. If they fail to meet this obligation, the access to information process is rendered ineffective.

This investigation deals with three access to information requests where political staff in two government ministries and the Office of the Premier failed to fulfill their duties as set out in s. 6(1) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

The cases we examined largely concern the existence, or destruction, of electronic records. Investigating these matters was highly technical and resource-intensive. My investigators requested backups of employee email accounts, seized and inspected computers, reviewed mailbox metadata and message tracking logs. This is the first time the office has requested email backups in the course of an investigation.

I am deeply disappointed by the practices our investigation uncovered. I would have expected that staff in ministers' offices and in the Office of the Premier would have a better understanding of records management and their obligation to file, retain and provide relevant records when an access request is received.

In conducting this investigation, it has become clear that many employees falsely assume that emails are impermanent and transitory, and therefore of little value. What this investigation makes clear is that it is a record's content and context that determines whether a record is transitory, rather than its form.

This investigation uncovered major issues that require immediate action. In order to address the very serious issues uncovered in this report, I have recommended that government make a technical fix to stop employees from permanently deleting emails. I have also called for mandatory training in records management, including training on what is a transitory record and what is not, to ensure that employees follow correct processes when responding to access to information requests.

Government is well advised to introduce a legislated duty to document its key actions and decisions as well as oversight of information management and destruction of records, with sanctions for non-compliance.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

# Executive Summary

This investigation report examines three access to information requests that raise significant questions about whether government is responding openly, accurately and completely to access requests made by citizens as required by s. 6(1) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

The investigation began when a former employee in the Office of the Minister of Transportation and Infrastructure filed a complaint with this office alleging that an employee of that office wilfully deleted email records that were potentially responsive to an access to information request received in November 2014.

Subsequently, the Office of the Information and Privacy Commissioner ("OIPC") received information about possible irregularities in relation to two other access requests. The first concerned the Ministry of Advanced Education ("AVED") and the second the Office of the Premier. The Commissioner expanded the investigation to encompass these additional matters.

In examining these three cases, the OIPC engaged the Investigations and Forensics Unit from the Ministry of Technology, Innovation and Citizens' Services ("MTICS"). The OIPC also retained its own forensic expert in order to preserve, restore and examine computer devices and email account backups.

### *MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE ACCESS REQUEST*

OIPC Investigators examined two aspects of an access request made on November 19, 2014, concerning missing women along Highway 16 / the Highway of Tears and, in particular, records about the meetings held by the Ministry of Transportation and Infrastructure ("MOTI") on this issue in June and July of 2014.

With regard to the processing of the access request, the investigation found that MOTI contravened its duty to assist under s. 6(1) of FIPPA by interpreting the applicant's request too narrowly and failing to clarify the nature of the records the applicant was seeking.

The OIPC's review of this access request also examined former Executive Assistant Tim Duncan's allegation that Ministerial Assistant George Gretes wilfully deleted emails from Duncan's email account that were potentially responsive to the request. Gretes denied Duncan's allegations.

To assist the investigation, the OIPC requested that government restore Duncan's email account for October and November 2014. Government advised the OIPC that it could not recover those accounts because it did not back them up when its email infrastructure was migrated in 2014 – an oversight not discovered until February 2015. The lack of monthly email account backups was a significant limitation in this investigation.

After multiple interviews under oath and a careful review of all available forensic evidence, the Commissioner found Duncan's evidence and testimony to be credible, and found it is more likely than not that Gretes deleted emails on Duncan's computer that may have been responsive to the access request.

After initially testifying under oath that he did not engage in the practise of "triple deleting" emails, George Gretes ultimately admitted that he did in fact engage in this practice.

The Commissioner has referred this case to the RCMP for investigation, including Gretes' failure to tell the truth under oath.

### *Ministry of Advanced Education Access Request*

The second access request in this investigation was made to AVED on July 21, 2014 for emails between the Minister's Chief of Staff and the Minister. The Chief of Staff did not produce any responsive records in the processing of this request. However, the Minister produced a large number of records that AVED released.

Upon examination of the monthly backup of the Chief of Staff's email account, OIPC investigators found that the Chief of Staff had approximately 20 responsive emails in his account at the time of the request that he did not produce. The Chief of Staff's explanation for why he did not produce these emails demonstrated, at best, a negligent search for responsive records.

As a result, the Commissioner found AVED contravened its duty under s. 6(1) of FIPPA to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the July 21, 2014 access request.

### *Office of the Premier Access Request*

The third access request investigated in this report was made on November 20, 2014 to the Office of the Premier. The request was for all outgoing email from the Premier's Deputy Chief of Staff between November 3 to 6 and November 17 to 20, 2014.

The OIPC's review found that the verbal process for processing access to information requests used by the Executive Branch of the Office of the Premier resulted in a systemic delay and a loss of potentially responsive records. The Commissioner found that this process was a contravention of the Office of the Premier's duty under s. 6(1) of FIPPA.

The proper identification of records as transitory or not transitory is an important access to information issue. The Deputy Chief of Staff's broad interpretation of transitory records resulted in the permanent deletion of almost all emails she sent in the course of her work. As a result, the Commissioner found that the Office of the Premier contravened its duty under s. 6(1) of FIPPA regarding the November 20, 2014 access request.

The Commissioner has recommended that the Executive Branch of the Office of the Premier change its process for access to information requests, to ensure it handles requests in a timely manner and there is a written record of how each request is processed.

### *Restoring Public Confidence*

This report recommends technical updates to stop employees from permanently deleting emails and ensure government retains a lasting record of email accounts. It also recommends mandatory records management training to all employees, including how to properly determine whether a record is transitory, and training to ensure proper retention and destruction of records.

Government should also implement legislative changes, including a duty to document the key actions and decisions of government, and oversight over record destruction with penalties for non-compliance.

The Commissioner, in this investigation, came to five findings and made 11 recommendations.

# 1.0 BACKGROUND

## 1.1 INTRODUCTION

Democracy depends on accountable government. Citizens have the right to know how their government works and how decisions are made. The *Freedom of Information and Protection of Privacy Act* ("FIPPA") enshrines this right, promoting openness, transparency and above all accountability of government activities.

Citizens can only exercise access rights when proper record keeping and retention is followed and the law providing access to records is respected. This requires that government:

- appropriately create records;
- understand and respect the distinction between a transitory record and a non-transitory record;
- preserve all records that are potentially relevant to an access request once the request is received;
- respond in an open, accurate and complete manner to access requests; and
- dispose of records only where there is legal authority to do so.

In this investigation, my office examined three specific access to information requests where the allegations raised questions as to the integrity of access to information in British Columbia. Are records properly retained by government employees? Is government producing all records in its custody or under its control that are potentially responsive to access requests? Are some government employees being prevented from producing potentially relevent records?

This investigation began with an allegation, made on May 27, 2015, that an employee within the Office of the Minister of Transportation and Infrastructure ("MOTI") wilfully destroyed potentially responsive records to an access to information request received in November 2014.

The access request concerned meetings held by MOTI in June and July of 2014 relating to the issue of missing women on Highway 16 / the Highway of Tears. The Highway of Tears is a stretch of approximately 720 kilometres along Highway 16 between Prince George and Prince Rupert on which a significant number of women have tragically disappeared.

While this investigation began with an allegation concerning the Minister's Office, we were already examining a complaint from the applicant concerning how MOTI handled the request.

On May 29, 2015, I informed the Minister of Transportation and Infrastructure that my office would examine both the alleged destruction of records and MOTI's overall processing of the access request.

I expanded the scope of my investigation to include two additional access requests that were brought forward which raised issues about the retention and disposal of records under FIPPA. On June 26, 2015, I notified the Minister of Technology, Innovation and Citizens' Services ("MTICS") of the expanded scope of my investigation.

While this Investigation Report is a detailed examination of these three access requests, I did not intend it to be a full review of all government's access to information practices. Given the seriousness of the allegations under examination here, there was a need to answer the questions expeditiously. Nonetheless, the matters examined in this report, covering two ministerial offices and the Office of the Premier, allow me to draw a number of conclusions about government access to information processes.

## 1.2 APPLICATION OF FIPPA TO THE GOVERNMENT OF BRITISH COLUMBIA

As is stated in s. 3(1), FIPPA "applies to all records in the custody or under the control of a public body." This investigation specifically deals with government ministry records that are, or may be, the subject of access to information requests. The definition of "public body" in Schedule 1 of FIPPA includes a "ministry of the Government of British Columbia." Further, the Minister's Office is part of a ministry. As a result, FIPPA applies.

## 1.3 INVESTIGATION PROCESS

As the Information and Privacy Commissioner for British Columbia, I have a statutory mandate to monitor the compliance of public bodies with FIPPA to ensure the law's purposes are achieved. The purposes, as stated in s. 2(1) of FIPPA, include making public bodies more accountable by giving the public a

right of access to records. Under s. 42(1)(a) of FIPPA, I have the power to conduct investigations to ensure compliance with FIPPA. Under s. 42(1)(f), I have the authority to comment on the implications for access to information of programs or activities of public bodies.

I will outline how we investigated the matters that form the basis of this report, including the tools my investigators drew upon in this process.

### *INTERVIEWS*

The allegations against MOTI and other ministries that gave rise to this investigation are of a serious nature and necessitated conducting many of our interviews under oath with a court reporter present.

With respect to the processing of the MOTI access request, my investigators interviewed two representatives from Information Access Operations ("IAO"), the central government body within MTICS that processes access requests for government ministries, two representatives from MOTI that were involved in the processing of the access request from within the Ministry and a senior government official from MOTI who was involved in the decision-making regarding the release of records for the request.

My investigators also met with the applicant who made the original access request that gave rise to the alleged destruction of records so as to fully understand the nature of the request as well as how it was processed from the applicant's perspective.

With respect to the allegations of the deletion of records within the Minister's Office at MOTI, the individual who made the allegation of destruction of records as well as the individual who was alleged to have destroyed the records were twice interviewed. We also interviewed the three other individuals who worked in the Minister's Office at the time the alleged events occurred. In addition, we questioned two staff members of the Office of the Premier who spoke with the person who allegedly deleted the records on the day the allegation first became public.

As part of our investigation into the two other access requests, my investigators interviewed individuals under oath who we believed had key knowledge of the material matters.

### *Computer Hard Drives*

My investigators also seized computers of relevant individuals within MOTI so that those computers could be forensically examined as part of the investigation.

## UNDERSTANDING GOVERNMENT INFORMATION SYSTEMS

Most of the matters considered in this investigation report concern the destruction or existence of certain records. It was therefore necessary to determine if these records, or information about them, could be recovered. For this reason, I asked for and received the assistance of the Investigations and Forensics Unit of MTICS, whose mandate is responsibility for government's collection and interpretation of electronic evidence. I also retained my own computer forensics expert to assist in this matter.

To understand what tools were available to my office in this investigation, it is necessary to explain how certain aspects of the government information system works.

### *Employee Email Accounts*

The email accounts of every government employee reside on 24 exchange servers that are in two locations. HP Advanced Solutions ("HPAS") operate these on the province's behalf. An employee's email account includes his or her calendar, mailbox, folders, email messages as well as any attachments and deleted messages that have not been permanently deleted from the system. I will explain later in the report how emails can be permanently deleted.

HPAS backs up all of this account information according to directions given to it by Messaging Services, a division within the Office of the Chief Information Officer of MTICS. This means that HPAS is responsible for backing up exactly what is in the employee's account at defined intervals.

### *Daily Backup*

Messaging Services has directed HPAS to do two kinds of backups. The first is a daily backup, which involves copying the email accounts of all government employees to an HPAS server once a day and storing it for 31 days before it is deleted. The main purpose of this daily backup is to enable government to reconstruct its email system in the event that one or both of the government servers should suffer a failure. Some data created or received since the previous backup might be lost during a catastrophic server failure, but government would have at its disposal very current data to restore its system.

### *Monthly Backup*

In addition to the daily backup, HPAS also copies every employee's email account once a month and stores that data on an HPAS server for a minimum of 13 months. The purpose of this backup is for investigative and legal purposes. The 13-month period can be extended, if necessary, for either investigative and/or legal purposes. No one is authorized to destroy daily or monthly backups before the regularly planned retention expiry date.

### *Restoring the Backup*

The critical matters investigated in this report occurred more than 31 days after they were drawn to my office's attention. As a result, daily backups no longer existed. Where it was necessary to locate and retrieve email account information, I had to rely on the monthly email account backups. This is the first time my office has taken the step of requesting monthly backup data.

My staff had numerous meetings with the Investigations and Forensics Unit to assist in our understanding of what we could expect to extract from the backup system. We also requested that the Deputy Minister for MTICS provide a written response to various questions we had regarding backup systems for reasons explained later in this report. In addition, we received a written response to further questions we had on this issue from HPAS who, as I have described earlier, delivers data management and storage services to government.

### *Message Tracking Logs*

Government has configured its information systems to capture another sliver of information relating to employee email accounts – a message tracking log. The tracking log keeps a limited amount of information related to every email sent or received by employees. The log records the sender, receiver and subject line of every email that flows through the exchange database system; however it does not retain the email itself or whether the email was deleted. We requested message tracking logs for certain aspects of this investigation.

### *Mailbox Metadata*

Government also keeps other information about the emails that flow through its system which I will refer to as mailbox metadata.

The mailbox metadata records the number of megabytes ("MB") of data found collectively in the employee's mailbox, including the Inbox, Sent Items folder and Deleted Items folders as well as a separate statistic of the MB of data in an

employee's Recover Deleted Items folder. This data is compiled in a report on a nightly basis.

The mailbox metadata proved important to this investigation. To understand its importance, it is necessary to explain the steps an individual can take to delete emails from government's system.

### *How Emails are Deleted*

When a government employee deletes an email from his or her Inbox, Sent Items folder or a custom created folder, it normally moves to the Deleted Items folder.

How long an email remains in the Deleted Items folder varies among employees. Some employees have their account configured so that emails remain in this folder until the employee takes further action to remove it. Others have settings whereby the Deleted Items folder is automatically expunged when the user shuts his or her device down, generally at the end of the workday. Still others have settings that allow for the retention of email in the Deleted Items folder for a set amount of time (14 days, for example).

Whatever the case, when an email is expunged from the Deleted Items folder, this is referred to as a "double delete". Every employee must ultimately double delete emails because system administrators restrict the capacity of an employee's mailbox. Emails within the Deleted Items folder (together with emails in their Inbox, Sent Items folder or custom created folder) count against such storage. Once an employee double deletes items, these items no longer count against that individual's storage.

When items are double deleted, they do not immediately disappear from the employee's email account. Double deleted items move to the Recover Deleted Items folder. Government has configured employee accounts to keep emails in the Recover Deleted Items folder for up to 14 days. During this period an employee can recover that email and return it to their Inbox if, for example, an email is accidentally deleted. If emails are not recovered within 14 days, the system is configured to automatically delete them. If those emails were not previously copied during a daily or monthly backup they will be permanently lost.

While government's current configuration provides for emails to remain in the Recover Deleted Items folder for up to 14 days, an employee can shorten that time by opening the folder and manually deleting an email or emails at any time. Some employees refer to this as a "triple delete". Triple deleting an email completely expunges it from the government system, unless it was captured by a daily or monthly backup.

# 2.0 ISSUES IDENTIFIED

The issues in this investigation are:

1. In the processing of the access request, did MOTI fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 19, 2014 access request about Highway 16 /the Highway of Tears? [s. 6(1) of FIPPA]

2. With respect to the allegations made about the destruction of potentially responsive records, did MOTI fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 19, 2014 access request about Highway 16/the Highway of Tears? [s. 6(1) of FIPPA]

3. Did AVED fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the July 21, 2014 access request for emails between the Minister's Chief of Staff and the Minister? [s. 6(1) of FIPPA]

4. With respect to the processing of access requests by the Executive Branch, does the Office of the Premier fulfill its duty to make every reasonable effort to respond without delay to applicants openly, accurately and completely? [s. 6(1) of FIPPA]

5. Did the Office of the Premier fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 20, 2014 access request for the outgoing emails of the Deputy Chief of Staff? [s. 6(1) of FIPPA]

# 3.0 Section 6(1) of FIPPA

Section 6(1) of FIPPA sets out the duty to assist applicants that applies to a public body's handling of access to information requests. Section 6(1) states:

> 6(1) The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

The wording of s. 6(1) is clear and instructive of what is required by public bodies. The public body "must make every reasonable effort to assist applicants" in order to establish that it has conducted an adequate search. This includes responding "without delay to each applicant openly, accurately and completely."

Numerous orders issued by this office have dealt with a public body's obligation to search for records.[1] What these orders establish is that s. 6(1) of FIPPA does not impose a standard of perfection or require a public body to establish with absolute certainty that records do not exist. However, a public body must be able to show that its search efforts have been thorough and comprehensive, and that it has explored all reasonable avenues to locate records and to assist applicants.

When considering the duty to assist, an important element in the context of this investigation is whether a public body has obtained sufficient clarification of the parameters of a request from the applicant. In interpreting s. 6(1), former Commissioner David Loukidelis stated:

> This does not mean I agree that, where there is some doubt about the precise parameters of an individual access request, a public body should, or is entitled to, interpret the request strictly and not seek any further clarification from the applicant. The duty to assist may well – in appropriate cases – require a public body to ensure it understands clearly what information an applicant seeks, including by contacting the applicant where practicable, in order to clarify the request.[2]

This is particularly the case where an overly narrow interpretation of a request will deprive applicants of records they would otherwise receive.

The requirement to perform an adequate search for records is part of the duty to assist. "Record" is defined broadly in FIPPA to include "books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other

[1] See, for example, Order F07-12, [2007] B.C.I.P.C.D. No 17, Order 00-32, [2000] B.C.I.P.C.D. No. 35 and Order 00-26, [2000] B.C.I.P.C.D. No. 29.
[2] See p. 5 of Order 00-33 at https://www.oipc.bc.ca/orders/605.

means, but does not include a computer program or any other mechanism that produces records".

Public bodies must produce all responsive records in existence at the time an access request is received. Deliberately refusing to produce responsive records or deleting responsive records in response to a request is a clear violation of s. 6(1).

The requirement to search for potentially responsive emails is an issue that arises in the three access requests examined in this investigation. The duty to assist involves searching for emails in a thorough manner, including in the Inbox, the Sent Items folder and any folders custom created by the user.

The extent to which this duty also includes retrieving emails that have already been deleted is very important to this investigation. As such, we must consider how this duty applies to emails in the Deleted Items folder, emails in the Recover Deleted Items folder and emails that exist in government backup systems.

This issue has been considered, at least in part, by previous orders of this office.[3] The obligation these orders place on public bodies is to search for deleted emails that are retrievable without excessive efforts.

Emails in an employee's Deleted Items folder must be searched as part of any access request because emails in this folder are readily retrievable by performing an automated search.

Emails that an employee has deleted from his or her Deleted Items folder and moved to the Recover Deleted Items folder are records that may be responsive to an access request. However, it will only be necessary to do such a search of the Recover Deleted Items folder in instances where there is a reasonable belief that this folder may contain responsive records. The reason for this is that unlike the mailbox folders, there is no capacity within Microsoft Outlook to do an automated search of the Recover Deleted Items folder.

With respect to a public body's obligation to restore and search email accounts or records backed up by HPAS for government, the position of my office is that, under ordinary circumstances, the duty to assist does not require such a search. For a typical access request, retrieving backed up data is too costly and time-consuming an exercise to be considered reasonable.

[3] See Order No. 73-1995, [1995] B.C.I.P.C.D. No. 46; Order No. 121-1996, 1996 CanLII 755 (BC IPC); Order No. 198-1997, [1997] B.C.I.P.C.D. No. 59; and Order 02-25, [2002] B.C.I.P.C.D. No. 25.

In exceptional circumstances, however, an applicant may be able to overcome the presumption that a public body need not search the backup system where he or she can provide substantive evidence to demonstrate that responsive records likely exist there. Such evidence must be more than mere speculation.

# 4.0 GOVERNMENT'S PROCESS FOR ACCESS TO INFORMATION REQUESTS

To fully understand the context for this investigation, it is necessary to explain how core government processes access to information requests. Fundamental to this understanding is the role IAO plays in processing such requests.

IAO is a branch of MTICS that is primarily responsible for processing all access to information requests received by government. IAO was formed in 2009, under the then Ministry of Labour and Citizens' Services, to centralize government's processing of access to information requests. Although the formation of IAO centralized the processing, the head of each ministry remains responsible for compliance with FIPPA. The purpose of centralization was to provide consistent, efficient access to government records.

Citizens who request government records must do so in writing, either on paper or through an online form. IAO's Intake Services receives these requests. IAO assigns each request to an analyst who ascertains the substance of the request and, where necessary, clarifies the response with the applicant. Where the ministry that is the subject of the access request does not have its own access coordinator, the IAO analyst identifies the appropriate program area that has, or would have, custody and control of the requested records within a ministry. The analyst requests the records from the program area and monitors legislated timelines and response requirements. Where the ministry has its own access coordinator, the only change is that the IAO analyst communicates with this person, who subsequently communicates with the relevant program areas. According to IAO, just over half of the ministries have their own access coordinator.

If the government program area finds records relevant to the access request, the IAO analyst reviews the records to ensure that they are responsive to the substance of the request, and that disclosure is compliant with FIPPA. The analyst works with program area staff within the ministry to recommend the severing of information they believe is subject to exceptions to disclosure under FIPPA prior to releasing the records to the requesting party. It is the delegated head of each ministry who ultimately decides whether to approve the recommended severing.

The IAO analyst then communicates the results of the ministry's search to the applicant and closes the file.

It is important to note that once a public body receives an access to information request, it must keep all records, including both transitory and non-transitory records,[4] in its custody or under its control. If these records are responsive, the public body must produce them unless specific exemptions to disclosure under FIPPA apply.

# 5.0 SPECIFIC ACCESS REQUESTS EXAMINED

This investigation considers two distinct matters related to the Highway 16/ Highway of Tears access request. The first is an assessment of the overall processing of the request from the time MOTI received it until the time that it ultimately disclosed some records. The second is a specific assessment of the allegation that an employee in the Minister's Office destroyed potentially responsive emails to the November 20, 2014 access request. In both cases the central issue is whether there was compliance with s. 6(1) of FIPPA.

Through interviews of various government employees and my office's review of documents, we established the following chronology of key events relating to the November 2014 access request to MOTI regarding Highway 16 / the Highway of Tears. This chronology is the basis for my analysis of MOTI's compliance with s. 6(1) of FIPPA.

### *CHRONOLOGY*

**June – July 2014:** Representatives from MOTI engaged in face-to-face meetings with over 80 community and First Nation leaders. Their goal was to garner a first-hand understanding of existing transportation services and challenges along the Highway 16 corridor from Prince George to Prince Rupert and to provide practical and affordable solutions to these challenges.

The "Highway of Tears" is approximately 720 kilometres along Highway 16 between Prince George and Prince Rupert. Over past decades, a significant number of women have tragically disappeared along this stretch of highway. Many of these women were presumed to be hitchhiking at the time of their disappearance, due to a perceived lack of transportation options.

[4] The distinction between transitory and non-transitory records is set out at p. 46 of this report.

Two senior officials from MOTI, including an Assistant Deputy Minister ("ADM"), conducted the meetings, accompanied by four other MOTI employees. On one day, meetings also included one employee of the Office of the Premier.

**November 17, 2014:** Parliamentary Secretary Darryl Plecas stated the following in the Legislative Assembly**:**

> "… I'm therefore certain the member will welcome the news that in June and July of this year, staff at the Transportation Ministry travelled along Highway 16 corridor and held face-to-face discussions with over 80 communities. They met with 12 First Nations. They spoke with 13 different municipalities and regional districts."[5]

**November 19, 2014:** An applicant submitted an access to information request to IAO on behalf of MOTI stating:

> "Pursuant to the *Freedom of Information and Protection of Privacy Act,* I request all government records that make reference to the issue of missing women along Highway 16/the Highway of Tears and specifically including records related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."

The applicant also included the above-noted quote from Parliamentary Secretary Darryl Plecas in the Legislative Assembly on November 17, 2014.

Later that same day, IAO sent the access request to MOTI's access to information coordinator.

**November 20, 2014:** MOTI's access to information coordinator sent the request, including the quote from Darryl Plecas, to all program area contacts within MOTI requesting that they search for responsive records. These program area contacts were tasked with sending the request to individuals within their group. They sent the request to the Minister's Office, including to the Executive Assistant and the Ministerial Assistant.

The Executive Assistant alleged that on this date the Ministerial Assistant deleted potentially responsive emails to the access request from the Executive Assistant's email account. The Ministerial Assistant denied the allegations.

[5] See p. 5313 of http://www.leg.bc.ca/hansard/40th3rd/20141117am-Hansard-v17n8.htm#5313.

**November 25, 2014:** MOTI's access to information coordinator followed up by email with the Ministry's program area contacts regarding the access to information request. In this email the following distinction was drawn:

> Note that this applicant is specifically requesting records that "make reference to the issue of missing women along Highway 16". If your records don't reference the issue of missing women along this highway and are about transportation planning and options etc. then your records may not be responsive. If you have questions, please contact me.

The assistant to the ADM who led the meetings in June – July 2014 along Highway 16 responded that the ADM advised that "… we do not have any records that make reference directly to the issue of missing women along Highway 16."

**November – December 2014:** MOTI located 36 pages of documents that were potentially responsive to the access request. Among these records were briefing notes, various handwritten pages and a document created by the Ministry of Justice.

MOTI worked with IAO to sever the documents by applying exceptions to access as is allowed under ss. 12 – 22.1 of FIPPA.

**December 16, 2014:** IAO sent a letter to the applicant informing her that MOTI was taking a time extension to consult with the Ministry of Justice as to whether a particular record created by the Ministry of Justice was, in fact, responsive.

**February 3, 2015:** After reviewing the document, the Ministry of Justice decided that it was not responsive and recommended that it be removed. MOTI agreed and these pages were removed from the package of potentially responsive records.

**February 12 – 16, 2015:** IAO asked for, and ultimately received, a second time extension from the applicant after letting the applicant know that there were "some notes that require transcribing" and the "file needs additional time to undergo the sign-off process".

**February 19, 2015:** MOTI communicated to IAO that the records originally considered potentially responsive were, in fact, not responsive. MOTI subsequently changed their response to "no responsive records". MOTI informed IAO that "Those involved directly with the meetings have advised that the topic of

the meetings with [MOTI] were on the topic of transportation options and community needs."

The ADM for MOTI, who was also the government lead in the June – July 2014 meetings along Highway 16, ultimately decided that the 36 pages of records were not responsive to the access request. The Deputy Minister for MOTI signed a form approving the no responsive records reply.

**February 20, 2015:** IAO sent a letter to the applicant stating that "no records were located in response to your request." The applicant responded by email to IAO asking how the request did not produce any records after MOTI took two time extensions.

**February 25, 2015:** The Official Opposition raised questions in the Legislative Assembly about MOTI producing no documents in response to this access request. On the same date, emails were sent within MOTI about re-processing the access request.

**March 3, 2015:** The applicant made a complaint to my office that MOTI had not fulfilled its duty to "openly, accurately and completely respond" under s. 6(1) of FIPPA. Later that day, IAO released three severed briefing notes to the applicant, most of which were not part of the 36 pages originally identified as responsive.

**May 27, 2015:** My office received a letter from the former Executive Assistant dated May 18, 2015 setting out his allegations.

**May 28, 2015:** The Official Opposition raised the former Executive Assistant's allegations in the Legislative Assembly during Question Period.

**May 29, 2015:** My office wrote the Minister of Transportation and Infrastructure announcing that we were investigating the allegations regarding the November 19, 2014 access request to MOTI regarding Highway 16/the Highway of Tears.

## 5.1 THE PROCESSING OF THE NOVEMBER 2014 HIGHWAY 16 /THE HIGHWAY OF TEARS ACCESS TO INFORMATION REQUEST TO MOTI

**Issue:** **In the processing of the access request, did MOTI fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 19, 2014 access request about Highway 16/the Highway of Tears? [s. 6(1) of FIPPA]**

### *EVIDENCE RE PROCESSING OF REQUEST BY IAO AND MOTI*

In assessing government's overall handling of the November 19, 2014 access request, a key question is why IAO told the applicant that responsive records existed when a "no responsive records" response would be issued less than a week later. The IAO and MOTI employees involved in processing this request said that they were not aware of any other instance where records were deemed non-responsive at this late stage of processing a file.

Interviews with MOTI employees disclosed that this change was the result of a difference of opinion among those Ministry employees as to what the access request was about.

Some of the individuals we interviewed acknowledged that the distinction drawn by MOTI executive between meetings about "missing women" and meetings about "transportation options and community needs" was not clear, while others felt there was a justification for a change to a "no responsive records" reply.

The ADM for MOTI was primarily responsible for the June and July 2014 meetings along the Highway 16 corridor and the person who ultimately decided on February 19, 2015 that the 36 pages of identified records were not responsive. Her evidence to my investigators was that she was "shocked" to find out after the February 20, 2015 "no responsive records" letter was issued that two time extensions had been taken on the request and that the applicant had already been informed of the existence of responsive records.

In response to questions raised in the Legislative Assembly by the Official Opposition on February 25, 2015, the Deputy Minister and the ADM for MOTI directed staff to release records to the applicant. The ADM stated to my investigators that given how the request had been handled, the applicant deserved a response and MOTI felt compelled to provide briefing notes that it

had created. The ADM stated that there was no discussion of providing the 36 records that had originally been identified as potentially responsive to the access request.

My investigators asked the ADM to clarify whether there were different meetings than those quoted by the applicant in the access request that took place between June and July of 2014 along the Highway 16 corridor. The ADM stated that there were not different meetings, but the meetings were not about the issue of "missing women", but instead were about "transportation options". The ADM stated that while "missing women" may have been infrequently mentioned at these meetings, it was not the main theme. MOTI's access to information coordinator also made this distinction in a November 25, 2014 email to the Ministry program areas.

My investigators' review of the 36 pages of potentially responsive records indicated that the records noted by the IAO analyst as requiring "transcribing" were actually handwritten notes that required further review and severing. The IAO analyst acknowledged that he had inappropriately used the word "transcribing".

### *ANALYSIS OF DUTY TO ASSIST RE PROCESSING OF REQUEST*

In considering MOTI and IAO's processing of the November 2014 access request regarding Highway 16 / the Highway of Tears, I will first restate the wording of the request. The applicant's November 19, 2014 request states:

> Pursuant to the *Freedom of Information and Protection of Privacy Act,* I request all government records that make reference to the issue of missing women along Highway 16/the Highway of Tears and specifically including records related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014.
>
> For reference, this was the statement made by Parliamentary Secretary Darryl Plecas on November 17, 2014 in the House:
>
> > *I'm therefore certain the member will welcome the news that in June and July of this year, staff at the Transportation Ministry travelled along Highway 16 corridor and held face-to-face discussions with over 80 communities. They met with 12 First Nations. They spoke with 13 different municipalities and regional districts.* (Hansard)

The “no responsive records” response stems from a distinction made by MOTI that the June and July 2014 meetings the applicant referenced were not about “missing women”, but were instead about “transportation options”. This distinction was drawn both by MOTI’s access to information coordinator in an email to the Ministry program areas, and by the ADM who led the meetings and ultimately decided that the 36 pages initially identified by MOTI were not responsive to the applicant’s request.

I believe MOTI took an unreasonably narrow view of the applicant’s request. The applicant requested records related to a series of meetings that took place in June and July 2014 along Highway 16. While noting that the meetings were about “missing women”, the applicant provides a great deal of context to enable MOTI to identify the meetings referred to by the applicant.

In processing the request, it appears that MOTI fully understood what meetings the applicant was referring to. Despite the narrow interpretation applied by the ADM and MOTI’s access to information coordinator, 36 pages of records were produced. Some of those records referenced “missing women”. In addition, government’s own internal discussions make the connection between “missing women” and the lack of “transportation options” regarding the highway. In the circumstances, the wording of the applicant’s access request should have been sufficient to consider these 36 pages as responsive.

It is difficult to understand how MOTI could have doubted that the applicant would be interested in any records relating to these meetings. Nonetheless, before MOTI made any distinction between the meetings being about “transportation options” or “missing women”, IAO should have contacted the applicant to clarify the request. The duty to assist an applicant under s. 6(1) of FIPPA requires such clarification where appropriate.

Further, prior to MOTI’s ADM making a determination that the 36 pages of records were not responsive, IAO had informed the applicant that responsive records existed. MOTI had taken two time extensions in the processing of this request, including one where IAO told the applicant that handwritten notes existed.

The ADM’s evidence to my investigators that she was unaware of key facts about this access request prior to making the decision to not release records demonstrates an unacceptable breakdown in communication regarding MOTI’s

handling of this access request. The response was not open, accurate or complete.

**I find that the Ministry of Transportation and Infrastructure contravened its duty to assist under s. 6(1) of FIPPA by interpreting the applicant's request narrowly and failing to clarify the nature of the records being sought in the November 2014 access to information request regarding Highway 16 /the Highway of Tears.**

**RECOMMENDATION 1:**

The Ministry of Transportation and Infrastructure should release the 36 pages of records initially identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on November 19, 2014 for:

> "… all government records that make reference to the issue of missing women along Highway 16 / the Highway of Tears and specifically including records related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."

## 5.2 THE ALLEGATION OF DESTRUCTION OF RECORDS BY THE MINISTER'S OFFICE IN MOTI REGARDING THE HIGHWAY 16/HIGHWAY OF TEARS ACCESS REQUEST

**Issue:** **With respect to the allegation made about the destruction of potentially responsive records, did MOTI fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 19, 2014 access request about Highway 16/ the Highway of Tears? [s. 6(1) of FIPPA]**

I have explained that when IAO received the applicant's Highway 16/the Highway of Tears access request on November 19, 2014, they emailed it the same day to,

among others, the MOTI's access to information coordinator. The following day, November 20, 2014, that coordinator relayed the request by email to four individuals in the Minister's Office – the Minister's Chief of Staff, his Administrative Coordinator, Ministerial Assistant George Gretes and Executive Assistant Tim Duncan. What occurred next is in dispute.

### *TIM DUNCAN'S EVIDENCE*

When the Highway 16/Highway of Tears request was received in the Minister's Office, Tim Duncan had been the Minister's Executive Assistant for about one month. Prior to this time he had worked for a number of years as a political aide in Alberta and in Ottawa.

Duncan believed he did a search of his mailbox in response to the request about midday or 1:00 p.m. on November 20, 2014. He said he searched his Inbox for the term "Highway of Tears", but was not sure whether he searched his Sent Items or Deleted Items folders. He is certain he didn't search other files on his computer for responsive records. Duncan said his search query generated 12-20 responses. He did not open any of them.

Duncan said he quickly alerted Ministerial Assistant George Gretes to his search results. Gretes worked in an adjoining office a few metres away and, as a new employee, Duncan understood he was to make Gretes aware when he had potentially responsive records. This was the first time he had received a request where a search revealed potentially responsive records.

Duncan said that Gretes came over to his desk and took a quick look at what the search had yielded. He described Gretes as "not being too happy" Duncan had records. Without opening any of the displayed email summaries, Duncan said that Gretes told him, "You got to get rid of these."

Duncan said he hesitated, at which point he said Gretes took his keyboard away and moved it near the corner of Duncan's desk. Duncan said he watched Gretes use Duncan's keyboard and mouse to move the searched items to the Deleted Items folder, delete the items from the Deleted Items folder, locate them in the Recover Deleted Items folder and delete them there; i.e. performing a "triple deletion". He recalled Gretes then saying "Hey, you don't need to worry about this anymore, it's done." Duncan said he was not happy about this, but did not say anything to Gretes.

Duncan told my investigators that staff commonly "triple deleted" emails in the Minister's Office and that Gretes had previously shown him how.

Duncan did not know if anyone witnessed the incident. He believed the only possible person would have been the Administrative Coordinator who sat nearby, but he was not sure she was at her desk.

Duncan said that on other occasions when he did a search in response to an access request he would report the results by email to the Administrative Coordinator. In this case, he did not report the result saying that he believed Gretes would have done so on his behalf given what had happened.

Duncan did not talk to anyone about the incident during the time he worked as an Executive Assistant.

In early January 2015, Duncan resigned his position as Executive Assistant to take a job as a researcher with the Liberal Caucus. He said the move followed discussions with the Chief of Staff from MOTI and the Premier's Deputy Chief of Staff about whether the role of Executive Assistant was appropriate for him. On January 7, 2015, he wrote the following letter to the Premier's Deputy Chief of Staff:

> I would like to inform you that I am resigning from my position as Executive Assistant for the Ministry of Transportation and Infrastructure, effective today.
>
> Thank you for the opportunity to learn about the Ministry that I have had during the past few months. I appreciate the support you provided me during my time there.
>
> If I can be of any help during the transition, please let me know.

Duncan said he did not discuss the alleged November 20, 2014 incident with anyone during his tenure as a Caucus researcher. He did recall one occasion where he said he voiced a general concern about how access to information requests were being handled by Ministers' Offices.

Duncan described a staff meeting where two people including the Chief of Staff of MOTI – his former supervisor – made a presentation about access to information responsibilities. After the meeting, Duncan said that four or five people gathered to discuss the session, including the Caucus Research Director.

Duncan said the Caucus Research Director asked what people thought of the presentation. At some point during the conversation, Duncan said he told the group that the presentation was hypocritical because the rules about how to respond to an access to information request as described in the presentation

were not being followed in Ministers' offices. Duncan says he stopped short of disclosing the allegation concerning Gretes because it likely would have resulted in his termination.

In the middle of March 2015, Duncan said he was "let go" from his employment with Liberal Caucus. He spent the better part of a month in Victoria before returning to Alberta in April 2015. Duncan said it was on his return to Alberta that he finally had time to consider and reflect on his employment experiences in B.C., including the incident he described concerning Gretes. He said he struggled with whether he should say something publicly about the incident.

Duncan said he determined that the role of the Information and Privacy Commissioner was to consider matters like his, and then he began in "bits and pieces" to draft a letter to my office in mid-April. He said he consulted no one on the matter and drafted it without assistance.

When Duncan determined in May 2015 that he would ask my office to investigate, he tried unsuccessfully to contact the Official Opposition in Victoria through a friend in Alberta who knew an Opposition Caucus member. Duncan then called an Official Opposition Member of the Legislative Assembly, who had publicly expressed concerns about the Highway of Tears matter. He talked with that Member the same day he sent a letter to my office. Duncan said he did not completely understand how my office functioned and what the Commissioner's powers were, and was worried his allegations would not be publicized if sent to this office alone.

Duncan said the Opposition did not make any suggestions or changes to his letter to my office and promised only to be a conduit for media inquiries.

I received the letter on May 27, 2015, though it was dated May 18, 2015. Duncan said that May 18 was probably the day the letter was originally formatted. The letter was made public in the Legislative Assembly on May 28, 2015, the last day of the spring legislative session.

Duncan said that he wanted to bring his allegations forward sooner, but stated that doing so while working for government would have been "career suicide", especially given that he was a new employee.

Duncan also said that although he was unhappy with how he came to leave his employment in British Columbia, he was not motivated by these circumstances when he decided to make the allegations public.

Duncan said he was motivated to bring attention to what he believed was a culture in government of evading access to information – an accusation that he focussed on politically-appointed staff. He was concerned about the Highway 16/ Highway of Tears access request and, in particular, with statements he heard

from government that everything in the case had been reported publicly. Duncan did not believe this to be the case. He said he sympathized with the families of the murdered and missing victims on the highway because his own father had been murdered in a domestic incident in 2010.

Duncan said that even after he was moved into the Liberal Caucus in January 2015 and subsequently terminated in March 2015, he realized that bringing these allegations forward would potentially have a negative impact on his ability to secure future work in certain positions, but nonetheless believed the issue important enough to make public.

### *GEORGE GRETES' EVIDENCE*

George Gretes was hired as MOTI's Ministerial Assistant in July 2014. He had served prior to that time in the same capacity to the Minister of Finance for a year.

George Gretes' evidence can be stated succinctly. He completely denied Duncan's allegations with respect to events on November 20, 2014. To be clear, his position is not that a different version of events took place. Instead, his position is that no version of the events alleged by the Executive Assistant took place at all.

Gretes said that, based on his general practice, he may have given Duncan a "heads-up in passing" to make sure Duncan looked at the access request, but he said that Duncan did not ask him for any assistance in respect of this request.

Gretes was unequivocal in his first interview that not only did he not triple delete Duncan's emails, he had never triple deleted his own emails. He would not have done so, he said, because he never found it appropriate in that it would not have served any purpose.

Gretes explained that each employee is allotted a limited amount of computer space to store emails. Emails that are located in the Inbox, Sent Items, and Deleted Items folders all count against an employee's allotment of storage; data that resides in the Recover Deleted Items folder does not.

Gretes said he has respect for other people's space and would never put himself in a position of taking control of a colleague's keyboard in an uninvited manner. He said he would definitely remember taking a colleague's keyboard and he did not in this instance.

Gretes said that the first he ever heard the allegation of his triple deleting Duncan's emails was when the issue was raised in the Legislative Assembly by the Official Opposition during Question Period on May 28, 2015.

At the time the allegation was raised in the Legislature, Gretes said he was in a room with fellow government staff members watching Question Period. Shortly after the allegations were raised, Gretes said he had a conversation with the Premier's Communications Director, who was a short distance from him in the room.

He said he told the Communications Director that the allegations were untrue, at which point Gretes was sent back to his office.

Later that afternoon Gretes was called to a meeting with the Premier's Deputy Chief of Staff, the Premier's Director of Executive Operations, and a member of the Human Resources team. Gretes was informed that he was suspended with pay until the matter was resolved. He is still on leave with pay as of the date of the issuance of this report.

Gretes said he did not know why Duncan would allege what he did. He said he considered Duncan a friend and was shocked by statements he made.

## Evaluating the Evidence

Given the conflicting testimony of the witnesses in this matter it was necessary to subject their evidence to further scrutiny.

### *TESTING TIM DUNCAN'S ALLEGATIONS*

My investigators first sought to evaluate Tim Duncan's allegations by both seeking out potential witnesses and looking to forensic evidence that would prove or disprove his allegations.

#### *EYEWITNESSES*

My investigators first asked whether anyone in the Minister's Office witnessed the events Duncan had alleged. It was apparent from a visit to the Minister's Office that only one staff member, the Administrative Coordinator, was likely in a position to see anything because her desk was the only one with a clear sightline

to Duncan's desk and was approximately 5 metres away. All of the other staff members were in adjoining offices with separate doors or were seated around a corner.

The Administrative Coordinator says that Gretes often visited at Duncan's desk and sat alongside him facing the computer and providing assistance. She does not remember whether or not Gretes was at Duncan's desk on November 20, 2014, and did not see Gretes take Duncan's keyboard or his mouse and use it at any point.

The Administrative Coordinator also said she normally takes her lunch around 1:00 p.m. It is therefore possible she was out of the office at the time of the alleged event. My investigators interviewed all other members of the Minister's staff; none had witnessed what Duncan alleged, nor had they heard of the allegations prior to them being made public on May 28, 2015.

### *EMAIL BACKUP*

We next turned to a review of government's monthly backup systems. My investigators asked that Duncan's email accounts for October and November 2014 be restored from monthly backups.[6] The intention was to search both accounts for the term "Highway of Tears", or other similar search terms, as Duncan described and compare the results. The monthly November 2014 backup, in particular, would have been revealing because if it contained any emails concerning Highway 16/the Highway of Tears predating Duncan's search of November 20, 2014, it would have cast doubt on Duncan's claim that Gretes had triple deleted them. On the other hand, if the November backup contained no emails relating to the Highway of Tears, especially ones that existed in the October backup, it would have lent some credence to Duncan's allegations.

When my investigators requested the monthly email backups from the Investigations and Forensics Unit of MTICS, we were advised that monthly backups did not exist for Duncan's account.

As I earlier outlined, HPAS is the service provider government contracts to back up its digital information, including employee email accounts. While HPAS stores the data, the Messaging Services branch of MTICS is responsible for telling HPAS how often it must backup this information.

In June 2014, government initiated a migration of employee email boxes from the 2007 version of the Microsoft Exchange email service to the 2013 version. This migration required a modified backup configuration. Messaging Services instructed HPAS to do an hourly and daily backup throughout the migration

[6] The daily backup system, with a retention period of 31 days, had long been deleted.

process. They did not instruct HPAS to do a monthly backup. This is because they believed the migration process would take less than a month and that hourly and daily backup would be sufficient.

As it turned out, the entire migration process would take eight months. When the process extended beyond June 2014, MTICS forgot to instruct HPAS to do backups on a monthly basis. This meant that every government mailbox that migrated onto the new system went without a monthly backup until all mailboxes were migrated. Any daily backup that existed was expunged after 31 days. At its peak, some 48,000 government mailboxes were without monthly email backups.

When the migration process was complete in January 2015, Messaging Services directed HPAS to reapply the standard backup configuration that included monthly backups. The net result was that, depending on when an email account was migrated, computers would have been without email backup anywhere from one to seven months.

Duncan's email account was already migrated to the new server when he began work for the Minister's Office on October 14, 2014. As a result, Duncan's account was not backed up during the months of October and November, the very months we sought to restore for this investigation.

No one in government or at HPAS realized the monthly backup error I have described until February 5, 2015, when the Investigations and Forensics Unit, in the course of an unrelated investigation, attempted to restore certain email accounts from 2014 that had been migrated and were not backed up.

MTICS officials acknowledge that the failure to do monthly backups of email accounts during the migration process was a serious oversight. Data has been permanently lost that may be needed for a myriad of investigative purposes, ranging from financial management matters to employee investigations. It would have assisted this investigation.

**RECOMMENDATION 2:**

Government should develop a policy for all future data migrations that requires at a minimum:

1. Hourly, daily and monthly backup of data;
2. Written directions to government's service provider with respect to these backups; and
3. Government monitoring of the directions to ensure their compliance.

MTICS has advised me they are taking steps to carry out these recommendations to ensure that proper backup will happen during the course of any future migration of data.

### *USE OF MESSAGE TRACKING LOGS*

Duncan said his search for Highway of Tears emails resulted in 12-20 responses. My investigators asked the Investigations and Forensics Unit to provide government's message tracking logs for all of Duncan's emails prior to November 21, 2014. My investigators then looked for terms in the subject lines of the emails such as "Highway of Tears" or "Highway 16".

This inquiry would not necessarily replicate Duncan's search of November 20, 2014, because his search for records would have also captured emails where the search terms appeared in the body of the email and not just the subject line, which is what the tracking log provides. In other words, Duncan's search might have yielded more responsive emails than our search did. Nonetheless, we conducted a search to see what results would emerge.

The query revealed six emails in his account predating his November 20, 2014 search. As explained earlier in this report, the tracking log does not note if the email was deleted. While this does not confirm Duncan's evidence that there were 12–20 emails in his mailbox responsive to his search, it is not inconsistent with the evidence.

### *DUNCAN'S COMPUTER*

My investigators also forensically examined Duncan's computer. Although it was long after his termination and others had been assigned to use the device, we were able to review aspects of Duncan's user activity. This search did not reveal any evidence relating to Duncan's allegations. This was not especially surprising because most activity undertaken involving email is on the government's Exchange Server and would not be stored on the user's device.

### *MAILBOX METADATA*

Duncan alleged that Gretes triple deleted 12-20 emails from his mailbox on November 20, 2014. He testified that the three stages of the deletion happened in quick succession in front of him on that day. We looked for any evidence that this occurred.

One method of determining whether the triple deletion occurred in the way Duncan described is to first review the size of an employee's mailbox (composed of their Inbox, Sent Items, custom created folders and Deleted Items folders) on consecutive days. If the total size of the mailbox diminishes from one day to the next, it means that emails have been moved to the Recover Deleted Items folder, in other words double deleted. If, on the same day, the volume of data found in the Recover Deleted Items folder is less than the amount of data moved into the folder from the employee mailbox, then we know at least some of the data has been triple deleted.

With this in mind, we examined Duncan's mailbox metadata between November 19 and November 20, 2014. We discovered that Duncan's mailbox decreased in size from approximately 281MB to 220MB over the two-day period, a deletion of about 61MB of data. The 61MB of deleted data should have been found in his Recover Deleted Items folder on November 20, 2014, unless it was expunged from the folder on the same day.

A review of Duncan's Recover Deleted Items folder revealed 0.79MB on November 19 and only 0.76MB on November 20, 2014. The only conclusion we can draw is that most, if not all, of Duncan's mailbox data that moved to his Deleted Items folder and then to his Recover Deleted Items folder was entirely expunged. In other words, the three stages of the triple deletion occurred on the same day as Duncan alleged.

This leaves open the question of who triple deleted these emails given that Duncan said that he also triple deleted emails on occasion. He said Gretes had shown him how to do this. A review of Duncan's mailbox metadata from when he started in mid-October through November 2014, confirmed he triple deleted sporadically over the course of 47 days.

This evidence of triple deletion and the time period in which it occurred is generally consistent with Duncan's allegation, and is not inconsistent with Duncan's evidence.

## *Testing George Gretes' Evidence*

My investigators next set about the task of testing aspects of Gretes' evidence. As stated earlier, no one witnessed the alleged incident. We interviewed a number of Gretes' work colleagues as to whether Gretes had spoken with them about events described in Duncan's allegations prior to them being made public on May 28, 2015. They said they had not. All expressed surprise at the allegation and said this did not sound like something Gretes would do.

### *MAILBOX METADATA*

One assertion Gretes gave under oath we could test with information provided us by the Investigations and Forensics Unit was that he had never triple deleted emails. We therefore examined Gretes' mailbox with a focus on his Recover Deleted Items folder.

During Gretes' second interview, my investigators presented statistics obtained from his Recover Deleted Items folder for the months of October and November 2014. Specifically, we drew to his attention that from:

i. October 20 to October 21, 2014, Gretes' Recover Deleted Items folder grew from over 22MB to over 85MB, meaning those additional 63MB should have remained for 14 days under the default system. Instead, on October 22, 2014, his Recover Deleted Items folder shrunk to just over 26MB.

ii. October 29 to October 30, 2014, Gretes' Recover Deleted Items folder grew from over 33MB to over 274MB, meaning those 241MB should have stayed in his Recover Deleted Items folder for 14 days. However, on October 31, 2014, his Recover Deleted Items folder dropped to approximately 32MB.

iii. November 9 to November 12, 2014, the Recover Deleted Items folder grew on two occasions from over 39MB to over 114MB. With natural attrition, at least the increased 75MB of data should have remained in his Recover Deleted Items folder for 14 days. Instead, it shrank to just under 3.9MB on November 13, 2014.

iv. November 16 to November 19, 2014, the Recover Deleted Items folder grew on three consecutive days from over 3MB to over 31MB. If the Recover Deleted Items folder was operating only according to its 14-day default, there should have been at least approximately 28MB of information in it. However, just one day later, on November 20, 2014, it dropped to about 2.7MB.

We conveyed to Gretes what the Investigations and Forensics Unit had told us – that there were only three possible explanations for the activity in his Recover Deleted Items folder. The first was that he changed the default deletion period on his Recover Deleted Items folder. Gretes confirmed he did not do this and the Investigations and Forensics Unit confirmed that Gretes' folder was set to a 14-day delete default.

The second possibility was that his account was moved from one exchange database or server to another. The Investigations and Forensics Unit confirmed Gretes' mailbox account had not been moved during this time period.

This left only one other possible explanation -- that Gretes did in fact triple delete his emails. My investigators asked Gretes whether, in light of this evidence, he wished to reconsider his earlier testimony.

Gretes admitted that he did not tell the truth in his original testimony and that he did triple delete his emails. He explained that his failure to tell the truth was based on a desire to protect the person who had shown him how to triple delete. He identified that person as the Administrative Coordinator in the Minister's Office. He said he didn't want to drag her into this investigation.

Gretes was at first vague about who approached whom to discuss triple deleting, describing it as a "conversation". He said the conversation involved the Administrative Coordinator talking about her past experience in the Alberta government and the fact that she triple deleted there. He thought others were part of the conversation – at one point indicating Duncan might have been present.

Gretes said the Administrative Coordinator asked those present during the conversation if they ever triple deleted and, when everyone answered that they did not, she proceeded to show them. He said that the Administrative Coordinator never explained why triple deleting would be a useful exercise. Gretes said he was not interested to know why, but assumed it had to do with managing his emails, although he said he didn't "mean necessarily concealment" of records.

Gretes then said his focus was on saving space on his computer and inferred triple deleting would assist in this task. When my investigators reminded him he had earlier given evidence that triple deleting did not assist with saving space he said he didn't know whether it would or not.

My investigators asked Gretes why he would be afraid to admit the Administrative Coordinator told him how to triple delete. He repeated his assertion that doing so would have dragged her into a "political battle".

The Administrative Coordinator, who was earlier interviewed about whether she witnessed the alleged triple deletion on November 20, 2014, was re-interviewed in light of statements and actions Gretes attributed to her.

The Administrative Coordinator told my investigators that she had worked in the Minister's Office at MOTI for the past two years and before that she had worked in Ministers' Offices in Alberta for 13 years. She testified that she did not know what triple deleting was or how to do it until she came to British Columbia. She said she thought the previous Ministerial Assistant at MOTI had taught her how to triple delete, but she was not sure.

The Administrative Coordinator recalled that the reason she was given for triple deleting was because there was a lot of confidential and sensitive information "and we need to make sure…it's not out there." She said she might have explained to Gretes how to triple delete, but was not sure. She was clear that she would not have explained triple deleting to Gretes without him asking her to do so. She described a clear separation between administrative staff such as herself and political staff like Gretes. "It wasn't my place to train political staff," she said.

The Administrative Coordinator was also clear that, in her view, there was nothing wrong with triple deleting and she would have no reason to hide it.

### *ANALYSIS OF THE DUTY TO ASSIST RE ALLEGED DESTRUCTION OF RECORDS*

Duncan's allegations speak directly to whether MOTI has complied with its obligations under s. 6(1) of FIPPA to meet its duty to respond to applicants "openly, accurately and completely". Deliberately destroying records in response to an access request would be a violation of s. 6(1) and an offence under s. 74 of FIPPA.

George Gretes and Tim Duncan provided diametrically contradictory evidence on the question of alleged destruction of records potentially responsive to an access request.

The question I must answer is whether, on a civil standard of proof, the incident Duncan alleged happened. The Supreme Court of Canada describes that standard as follows:

> …in civil cases there is only one standard of proof and that is proof on a balance of probabilities. In all civil cases, the trial judge must scrutinize the relevant evidence with care to determine whether it is more likely than not that an alleged event occurred. [7]

Therefore, in the context of this investigation, I must determine whether it is more likely than not that on November 20, 2014, George Gretes took control of Tim

[7] *F. H. v. McDougall* 2008 SCC 43 at para. 49.

Duncan's computer and deleted emails believed to be responsive to an access to information request with respect to Highway 16/ the Highway of Tears.

Duncan's evidence remained consistent through two interviews.

There were no witnesses to the alleged events of November 20, 2014. In the version of events set out by Duncan, there is a reasonable chance this would be the case. There might not have been anything that would have drawn anyone's particular attention to the incident as alleged. It is also possible the Administrative Coordinator was away at the time. In short, I do not find anything determinative about the fact there were no witnesses to the alleged incident.

My investigators questioned Duncan in detail about the fact that he talked with no one about the incident while he worked at MOTI or the Liberal Caucus Research Office. As a new person to Victoria and a very junior employee, unsure of the work culture, this explanation seems entirely plausible and I do not draw any adverse inference from his failure to share the information with colleagues or report it to his superiors at work.

My investigators also put to Duncan the suggestion that he was a disgruntled employee seeking retribution against those that fired him and his means of doing this was through the Official Opposition in the Legislature. After considerable questioning, my investigators did not perceive any extraordinary degree of animus towards his employer other than what any reasonable person might experience in the circumstances. If he was truly disgruntled after being let go from Liberal Caucus, one might have expected him to have made the allegations closer to his termination. Instead, he spent the next month in Victoria before returning to Alberta to think about his future.

In considering the totality of the circumstances, including Tim Duncan's sworn testimony, his demeanour during interviews with my investigators, the evidence of his work history, as well as the available forensic evidence, my investigators found him to be a credible witness. He did not strike them as a person seeking the public limelight or retribution against his previous employer. It is difficult to see what, besides disclosing what he believed was a wrongful action, he had to gain from making the allegations. As Duncan himself acknowledges, it may well be a challenge for him to ever again work again in the political realm.

By contrast, George Gretes' evidence presents challenges.

Key to his denial of triple deleting Duncan's email on November 20, 2014 was Gretes' sworn evidence that he did not triple delete Duncan's email, nor had he ever triple deleted.

In his initial interview with my investigators, Gretes denied on six separate occasions that he had ever triple deleted his own emails. Early in his first interview, Gretes suggested he "really had no idea" where the Recover Deleted Items folder was, though later in the same interview said he could find it.

After initially confirming his evidence from the first interview, George Gretes told my investigators in his second interview that he had failed to tell the truth. He admitted that he did, in fact, triple delete emails. It is reasonable to conclude that the only reason he admitted to this was that he had been confronted by indisputable forensic evidence.

When given the opportunity to explain why he did not tell the truth, Gretes said he wanted to protect the Administrative Coordinator. However, the Administrative Coordinator contradicted key aspects of Gretes' version of events. Her evidence was that she triple deleted records she no longer needed to keep and had no reason to hide that fact. She learned of triple deleting only when she came to work in British Columbia with MOTI two years ago. She did not learn of triple deleting in Alberta as Gretes had said. I also accept the Administrative Coordinator's evidence that she would never have proactively sought out a political staff member like Gretes to teach him how to triple delete. She would only have demonstrated how to triple delete if asked.

The Administrative Coordinator presented herself to my investigators as a credible and candid witness.

The Administrative Coordinator said she had nothing to hide with respect to triple deleting, which raised the question of what Gretes would be protecting her from by not disclosing her actions. We asked him that question in his second interview. His response was that it was a false assumption on his part that reporting that the Administrative Coordinator told him how to triple delete would have gotten her into trouble and he wanted to remain loyal to a fellow employee.

The preponderance of the evidence is that George Gretes failed again to tell the truth, this time about allegedly protecting a fellow employee. It is reasonable to believe that the reason he did not tell the truth about his own triple deletion is because he thought that admitting it would undermine his denial of Duncan's allegations.

Following Gretes' admission that he did not tell the truth under oath in the first interview, my investigators asked him again whether he deleted Duncan's records on November 20, 2014. Many of his responses were in the form of an argument rather than an answer. For example he said that even if he admitted to doing what Duncan said he had done, that "hypothetically speaking, what was deleted?…that's the question".

At other points, after denying the triple deleting of Duncan's emails, he said "It's just ridiculous that it would come to this point. Not based on the fact that he's accusing me of deleting emails from his email and grabbing his keyboard, it's just that – like I told you in the first interview, I really thought he was my friend…." Gretes said that he just couldn't have imagined Duncan making the allegation. In my view, this does not speak to a denial of triple deleting Duncan's email, but rather it appears to be an expression of betrayal by a person Gretes thought to be a friend.

Near the conclusion of the second interview Gretes, when my investigators asked if Gretes triple deleted Duncan's email on November 20, 2014, Gretes replied, "I don't know for sure," before stating finally that he did not do it.

Where does this lead in terms of the credibility of Gretes' evidence? As already indicated, it is reasonable to conclude, as I do, that he would not have admitted his failure to tell the truth about triple deleting but for the forensic evidence that conclusively demonstrated he had done so. The subject of that failure was not an unimportant matter. His claim about never triple deleting went to the core of his denial that he did not triple delete Duncan's email.

I also conclude that, having failed to tell the truth about triple deleting, Gretes was not truthful in his statement that he was trying to protect a fellow employee.

The allegation of records destruction in this case is a very serious one.

The forensic evidence conclusively demonstrates that emails were deleted from Duncan's computer on November 20, 2014. That evidence also proves that there was a triple deletion of emails on Duncan's computer that day.

I find Duncan's evidence about the triple deletion to be credible for the reasons already described. Conversely, Gretes was not a credible witness. His denials of the allegation during the second interview – that he triple deleted emails on Duncan's computer – were unconvincing, up to and including his statement that he didn't know for sure if he did it. He admits to falsifying his testimony in this investigation. The justification he gave for his failure to tell the truth also proved to be false. The only reasonable explanation for his failure to tell the truth was to hide the triple deleting of emails as alleged.

**I therefore find it is more likely than not that George Gretes deleted emails on Tim Duncan's computer on November 20, 2014, that may have been responsive to the Highway 16/ the Highway of Tears access request. It follows that the Ministry did not comply with s. 6(1) of FIPPA because it failed to openly, accurately and completely respond to that request.**

Finally, I cannot overstate the gravity with which I view the false testimony given during this investigation by George Gretes. To that end, I have referred the matter for investigation to the RCMP and have advised them of the contents of this report, including the failure of George Gretes to tell the truth under oath. I am deeply saddened that the evidence in this case has required me to take this course of action.

## 5.3 JULY 2014 ACCESS REQUEST TO THE MINISTRY OF ADVANCED EDUCATION

**Issue:** **Did the Ministry of Advanced Education fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the July 21, 2014 access request for emails between the Minister's Chief of Staff and the Minister? [s. 6(1) of FIPPA]**

Our examination of this access request is again best introduced by a chronology of the key events.

### *CHRONOLOGY*

**July 21, 2014:** IAO received an access request to AVED for:

> "Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014."

**July 23, 2014:** The Ministry's FOI coordinator emailed the Chief of Staff to see if he had any responsive records.

**July 30, 2014:** The Chief of Staff emailed the Ministry's FOI coordinator to say that he had no responsive records.

**August 29, 2014:** Responsive records were provided to IAO on behalf of Minister Virk.

**December 29, 2014**: IAO wrote the applicant and released approximately 435 pages of severed records, including many emails sent by the Chief of Staff to Minister Virk.

**June 3, 2015**: My office received a letter from the applicant setting out concerns about the Ministry of Advanced Education's handling of this access to information request.

### *DOCUMENTARY EVIDENCE*

The records produced by the Minister, but not by the Chief of Staff, raised questions about the Chief of Staff's practices regarding the retention of records. As a result, my investigators requested that the Investigations and Forensics Unit provide my office the monthly backup of the Chief of Staff's email account that was preserved as of August 1, 2014. On review, we found the Chief of Staff's Sent Items folder contained approximately 20 emails that he sent to Minister Virk that fell within the date range of the access request. However, the Chief of Staff stated by email on July 30, 2014, that he had no responsive records.

### *EVIDENCE OF THE CHIEF OF STAFF*

The Chief of Staff started working in government in June 2013 and had received training on access to information on multiple occasions. He started as Chief of Staff with the Ministry of Health, moving to the Ministry of Advanced Education after about four months.

The Chief of Staff felt he understood how to properly search for potentially responsive records. He explained the way he did his searches was to do such things as search files on his desk and the files in his cabinet and also to search his emails. He searched emails by, where appropriate, looking at particular date ranges and printing potentially responsive emails. If a request was on a particular topic, he would make a list of keywords and then search the Inbox, Sent Items and Deleted Items folders.

The Chief of Staff also stated that he sent numerous emails on a regular basis to Minister Virk.

We provided the Chief of Staff with the information that his mailbox contained approximately 20 responsive emails to the July 21, 2014 access request. We further explained that these emails were in his Sent Items folder at the time he said he had no responsive records to the access request. He responded that he did not recall specifically how he searched for records for that access request. He said that although he typically did searches from his desktop, it was possible he had searched from his phone or his iPad. His evidence was that he had not realized that these devices might only load the last 100 sent emails and this could possibly explain his search not turning anything up. But, to be clear, the Chief of Staff did not recall what kind of search he undertook or what happened in this particular instance and said he typically did searches from his desktop.

### *ANALYSIS OF THE DUTY TO ASSIST*

Once a public body receives an access to information request, all records in its custody or under its control, whether transitory or non-transitory, must be searched in order to locate potentially responsive records. It is therefore the wording of the access request that directs the public body as to what records must be searched. In this case, the applicant's request was easy to interpret; it asked for all emails sent by the Chief of Staff to the Minister over certain dates. With access to the Chief of Staff's email account, my investigators were able to locate responsive records within minutes. I observe that the emails in question are not of a particularly sensitive nature.

There are three logical possibilities that could explain why the Chief of Staff said on July 30, 2014, that he had no responsive emails related to the July 21, 2014 access request when the evidence conclusively demonstrates he did. The first is that he did not perform a search for the records at all. The second is that he performed an inadequate search. The third is that he located the responsive emails, but decided not to produce them.

The Chief of Staff's sworn evidence is that he would have searched for the records, but he had no specific recollection of doing so in this case. He said it is possible he could have done the search on his phone or iPad. He said he subsequently learned that such a search might have yielded only the last 100 emails he sent and this might explain why he did not produce them. In any event, he acknowledges that this would not be his normal method of searching for records and that he likely would not have used this method alone. Additionally, the evidence of the Chief of Staff when he was asked how to search for records demonstrated a thorough understanding of the proper steps to take to locate responsive records.

Searching for records on a phone or iPad or similar device is not a reasonable means of conducting a search. The ability to readily identify and convey the results of a search on a hand-held or smaller device is challenging. My own investigators have determined that the search limitation the Chief of Staff referred to associated with his iPad or phone may possibly have been the case at the time of his search. This further speaks to why searching on such a device would not comply with s. 6(1) of FIPPA. A reasonable search will be one that is performed from a desktop or laptop.

Apart from not doing any search at all, it is difficult to understand how the Chief of Staff would have thought he had no responsive records in these circumstances. The request covered all emails he would have sent to his Minister during a period

ending just one week before he received the request. The Chief of Staff acknowledged that he sends a large number of emails to the Minister. Based on these facts alone, it is difficult to understand how the Chief of Staff thought his reply of no responsive records on July 30, 2014, could be accurate given that our review of his account as of August 1, 2014, showed a large number of emails from various dates, including the approximately 20 responsive records.

Whether the Chief of Staff intended to wilfully disregard this access request is not clear. What is clear is that this is an instance where the Ministry of Advanced Education is in contravention of s. 6(1) of FIPPA because, at best, the Chief of Staff conducted a negligent search for responsive records.

**I find that the Ministry of Advanced Education contravened its duty under s. 6(1) of FIPPA to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the July 21, 2014 access request for emails between the Chief of Staff and the Minister.**

**RECOMMENDATION 3:**

The Ministry of Advanced Education should release the approximately 20 email records identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on July 21, 2014 for:

> "Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014."

The Investigations and Forensics Unit will retrieve the emails and provide them to the Ministry.

## 5.4 NOVEMBER 2014 ACCESS REQUEST TO THE OFFICE OF THE PREMIER

This access request raises two distinct issues under s. 6(1) of FIPPA. The first is the Executive Branch of the Office of the Premier's process for tracking access to information requests and the second is the Deputy Chief of Staff's records management practices. I will first set out the chronology that is relevant to both these issues.

### *CHRONOLOGY*

**November 20, 2014:** IAO received an access request to the Office of the Premier for:

> "Any and all records of outgoing email correspondence to any recipient including attachments from Deputy Chief of Staff Michele Cadario. Timeframe November 3 to 6 and November 17 to 20, 2014."

On this same day, IAO received another access request for all emails sent by the Premier's Chief of Staff, Dan Doyle for the same date range.

**November 24, 2014:** IAO sent the access request to the FOI coordinators for the Office of the Premier's Deputy Minister and the Executive Branch. The Deputy Chief of Staff is part of the Executive Branch. IAO also sent the request to the Office of the Premier's central coordinator of access requests, who coordinates responses for the Office of the Premier as a whole.

**November 25, 2014:** The email request was forwarded to each of the employees in the Deputy Minister's Office. Kim Henderson, the former Deputy Minister, Corporate Initiatives, produced one email chain responsive to the request.

**December 1, 2014**: The FOI coordinator for the Executive Branch communicated by email to the Office of the Premier's central coordinator of access requests that neither the Deputy Chief of Staff nor anyone else in the Executive Branch had responsive records.

**February 18, 2015:** IAO released a severed version of the one email chain produced by Kim Henderson to the applicant.

**April 28, 2015:** IAO released an additional 123 pages of records to the applicant in response to the access request sent to the Chief of Staff Dan Doyle. The release included numerous emails sent from the Deputy Chief of Staff to the Chief of Staff.

**June 3, 2015**: My office received a letter from the applicant setting out concerns about the Office of the Premier's handling of this access to information request.

**Issue:** **With respect to the processing of access requests by the Executive Branch, does the Office of the Premier fulfill its duty to make every reasonable effort to respond without delay to applicants openly, accurately and completely? [s. 6(1) of FIPPA]**

This issue relates to how the Executive Branch of the Office of the Premier processes access requests once it receives them. While the chronology of the November 20, 2014 access request regarding the Deputy Chief of Staff is useful in illustrating the process for the Executive Branch, our examination is not strictly limited to this access request for this portion of our review.

### *EVIDENCE OF THE FOI COORDINATOR FOR THE EXECUTIVE BRANCH*

The FOI coordinator for Executive Branch of the Office of the Premier's official title is Director of Issues Management. He has responsibility both for access to information in the Executive Branch as well as for issues management, such as managing media issues. He says that when he is dealing with access requests, he acts entirely in that role and is not looking at requests from an issues management perspective.

The evidence of the FOI coordinator is that he began working for the Executive Branch in July 2014, but had previously worked in government since about 2009. He received access to information training in 2013 for approximately one hour. He works primarily in Victoria, but also works in Vancouver. When the Legislature is sitting, he typically spends one day per week in Vancouver. At other times, he can spend two or more days in Vancouver for work.

Once the FOI coordinator receives notice of an access request by email from IAO, he said he personally speaks with each individual within the Executive Branch to ask whether or not they have responsive records. The FOI coordinator stated that it takes him anywhere from a day to as much as three or four days upon receipt of a request to speak with all members of the Executive Branch about the request.

The FOI Coordinator said that each individual would respond to him in person and, where necessary, print potentially responsive records. The FOI coordinator stated that he does not correspond by email or by telephone with members of the Executive Branch regarding access requests.

The FOI coordinator stated he records on a sticky note the people he has told about an access request and that he would get rid of the note after dealing with the request. He said he does not keep any other record of processing access requests.

The FOI coordinator stated he designed the process for responding to access requests in the Executive Branch. He was not sure of the process prior to his being hired and he had not received instruction from any supervisors about the matter when he joined the Executive Branch. He was aware the Premier's Deputy Minister's Office and other offices in government send emails to employees about access requests and also receive emails in response.

The FOI coordinator stated that he would never question an individual's response that they had no records responsive to an access request.

The FOI coordinator did not recall, and had no record to confirm, when he would have asked the Deputy Chief of Staff about the access request at issue here. He would have followed the same process as for other requests.

The Deputy Chief of Staff also stated that that the FOI coordinator's practice was to ask her in person whether or not she had records to access requests and that she responded in person, printing potentially responsive records when she found them. The Deputy Chief of Staff did not recall exactly when the FOI coordinator asked her about this specific access request, but did recall that she had no records.

### *ANALYSIS OF THE DUTY TO ASSIST RE EXECUTIVE BRANCH'S PROCESSING*

In determining whether the processing of access requests by the Executive Branch of the Office of the Premier complies with s. 6(1) of FIPPA, it is important to closely look at the wording of this section which requires that public bodies "respond without delay to each applicant, openly, accurately and completely."

With the wording of s. 6(1) in mind, I am troubled by the manner in which the Executive Branch of the Office of the Premier processes access requests.

There should be an electronic record of each person's response to an FOI coordinator for each access request. It is the process used by the Deputy Minister's Office of the Office of the Premier and the process my investigators observed in all other instances associated with this investigation. The current process for the Executive Branch results in no lasting record of the person who receives notice of the request or how individuals respond.

Personally asking individuals whether they have responsive records, rather than sending an email, also creates the potential for systemic delay in access requests reaching relevant employees. This is especially the case given that employees within the Executive Branch commonly split their time between

Vancouver and Victoria. The FOI coordinator was not able to definitively say when he made the Deputy Chief of Staff aware of the access request relating to her outgoing emails or when she responded that she had no records.

The FOI coordinator verbally asks each employee for records and verbally receives the answer. The only element of a written record tracing a request is a sticky note penned by the FOI coordinator each time a request comes in denoting which employees he has talked to about it. The note is disposed of when the FOI coordinator believes the processing is complete.

The FOI coordinator says that he put this process in place himself. He has received one hour of training on access to information. The Office of the Premier has put the FOI coordinator in a difficult situation. I believe he is not adequately positioned to determine the Executive Branch's access to information process. It is surprising that the Executive Branch of the Office of the Premier would conclude that not writing anything down about the processing of an access request, apart from a temporarily retained sticky note, is appropriate.

Moreover, the Executive Branch's process creates the potential for delay in the request reaching the employees most likely to have records. This systemic delay can, and almost certainly does, in some instances, result in the loss of potentially responsive records and a frustration of the access rights for citizens. This is because even though the public body has received the request, an employee may have deleted records responsive to it not knowing the request had been received.

**I find that the Executive Branch's systemic delay in its processing of access requests and the resulting loss of potentially responsive records is a contravention of the Office of the Premier's duty under s. 6(1) of FIPPA "to respond without delay to each applicant openly, accurately and completely."**

**RECOMMENDATION 4:**

The Executive Branch of the Office of the Premier should change its access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.

**Issue:** **Did the Office of the Premier fulfill its duty to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 20, 2014 access request for the outgoing emails of the Deputy Chief of Staff? [s. 6(1) of FIPPA]**

### *TRANSITORY RECORDS*

The issue of what constitutes a transitory and non-transitory record figures prominently in this part of our Investigation Report. It is therefore necessary at this point to briefly explain what these terms mean.

The transitory record schedule, approved by the Legislative Assembly, precisely and narrowly defines what a transitory record is. Transitory records are: convenience copies, unnecessary duplicates and working materials and drafts once the finished record has been produced.[8] Unless records fall within these prescribed categories, they must be retained in accordance with an approved schedule. The proper identification of records as transitory or not transitory is an important access to information issue because when records are prematurely destroyed it negatively impacts citizens' access to information rights.

Transitory records are routinely destroyed when they are no longer required for a business purpose. The authority to identify and destroy transitory records is delegated to government employees under the transitory records schedule.

The routine destruction of transitory records is necessary to reduce the volume of government records and the cost of managing records.

Non-transitory records, on the other hand, need to be filed and saved in accordance with the appropriate government records schedule. The classification and scheduling of records should make them readily identifiable and retrievable when subject to an access request.

Non-transitory records include such things as decision records, instructions, and advice as well as documentation of a policy matter or how a case was managed. It is important to note that it is a record's content and context that determines whether a record is transitory, rather than its form.

[8] See BC Government's Transitory Records (schedule 102901) at http://www.gov.bc.ca/citz/iao/records_mgmt/special_schedules/transitory_records.html.

### *DOCUMENTARY EVIDENCE*

As is set out in the chronology, the applicant in the access to information request regarding the Deputy Chief of Staff received 123 pages of severed records from a similar request to Chief of Staff, Dan Doyle. Those records included various emails sent from the Deputy Chief of Staff to the Chief of Staff that were not produced by the Deputy Chief of Staff with respect to the access request regarding her sent emails.

The released emails sent by the Deputy Chief of Staff to the Chief of Staff appeared to my investigators, on first reading, to include potentially substantive actions taken by the Deputy Chief of Staff – in other words, they were non-transitory records. This raised questions about the Deputy Chief of Staff's practices regarding the retention of records and necessitated further inquiry. Given the original access request concerned emails sent in November 2014, we asked the Investigations and Forensics Unit to restore the monthly backup of the Deputy Chief of Staff's account as of November 27, 2014. We found no emails in the Deputy Chief of Staff's Sent Items folder on any subject.

We did identify 163 sent emails that resided in either her Deleted Items folder or in her Recover Deleted Items folder (the Investigations and Forensics Unit told us it was not possible to delineate which folder). What is of importance is the content of those emails in light of the issue of transitory and non-transitory records.

### *EVIDENCE OF THE DEPUTY CHIEF OF STAFF*

The Deputy Chief of Staff stated that "very few" of the emails she sends are not transitory and believes that none of the emails she sends to the Chief of Staff should be kept as they do not document a decision of government or create policy. She stated that it was not part of her responsibility to create government policy or to give policy advice, which she stated was the responsibility of public servants who worked within the various government ministries. Instead, the Deputy Chief of Staff agreed that her role was to assist with government making informed decisions about the political aspects of an issue.

The Deputy Chief of Staff stated that her practice was to delete emails from her Sent Items folder on a daily basis and if all emails in that folder were of a transitory nature, she would delete all of them. Her evidence was that her Deleted Items folder was set to purge at the end of each day when she exited Microsoft Outlook.

The Deputy Chief of Staff added she had not heard of the Recover Deleted Items folder until two days prior to our interview with her. The topic had come up in a conversation with a work colleague that was unrelated to our investigation. But since she had learned of the existence of the Recover Deleted Items folder, she had begun to triple delete items as part of her management of records.

Where non-transitory emails were the responsibility of someone else to keep, the Deputy Chief of Staff would forward those emails to the appropriate individuals. For example, where she may have sent emails related to human resource matters, she would forward those to another member of the Office of the Premier for keeping.

My investigators put before the Deputy Chief of Staff certain emails from her that the Office of the Premier released in the access request to the Chief of Staff and asked why she had not retained these records. Her evidence was that she considered all of the relevant emails from her to be transitory in nature and nothing that she needed to keep.

The Deputy Chief of Staff's evidence as to why she believed her emails were transitory included that, in one instance, the advice she appeared to provide was based on incorrect facts. In another instance, when we suggested to her certain records appeared to disclose advice, she said that the record of such advice would not have to be retained if it had not resulted in any course of action. In other words, she believed such a record would be transitory.

### *ANALYSIS RE DUTY TO ASSIST*

In looking at whether the Office of the Premier has complied with s. 6(1) of FIPPA on this specific access request, I note that my office has no evidence that potentially responsive emails existed anywhere but in the Deputy Chief of Staff's Recover Deleted Items folder. This is because I accept that the Deputy Chief of Staff's Deleted Items folder was set to purge emails at the end of every day and thus emails do not exist in that folder for more than one day. I also accept that the Deputy Chief of Staff was not aware of the existence of the Recover Deleted Items folder at the time of the November 20, 2014 access request. Nonetheless, I cannot ignore the evidence of the Deputy Chief of Staff that she believes "very few" of the emails she sends are not transitory and believes that none of the emails she sends to the Chief of Staff should be kept.

While her evidence is that she does not create policy, the job description for the Deputy Chief of Staff was released in a 2013 access to information request and it included providing "strategic advice to the Chief of Staff, Premier and Executive Council to advance government's policy and legislative objectives". It seems

reasonable to expect that some of this advice to advance government's policy and legislative objectives is communicated through email and requires retention. In fact, my investigators viewed emails in her November 27, 2014 account that we believed demonstrated exchanges with the Chief of Staff that she should have retained to document the decision-making process.

Other staff may well capture and retain some of the Deputy Chief of Staff's emails on particular matters. In such instances, the Deputy Chief of Staff may not be required to retain those records if she is aware that those responsibilities have been clearly assigned to someone else. I accept that in some instances, such as with human resource matters, this appears to be the case for the Deputy Chief of Staff.

Apart from rare emails that she forwards to others to file for her, it is the Deputy Chief of Staff's practice to delete every email she sends every day and these emails are purged from her Deleted Items folder every time she shuts down her computer. This practice creates a scenario where she will almost never have a sent email that is responsive to an access request.

This is because the Deputy Chief of Staff applies a broad interpretation of transitory records and a daily practice of deleting all transitory records from her account. From my investigators' review of her November 27, 2014 account, we can confirm that she has not personally retained a single email she has ever sent from her government email address.

Given the importance of the role of the Deputy Chief of Staff within government, it is difficult to accept that she almost never sends an email that would be considered non-transitory and therefore requires retention. It must be kept in mind that the medium of communication does not determine whether a record needs to be saved. This determination is solely based on content. Some emails may be transitory, but an informed and reasoned approached should be used to make this determination on a case-by-case basis.

I believe that the broad interpretation given to transitory records by the Deputy Chief of Staff, which results in her retaining almost no sent emails, effectively frustrates the Office of the Premier's ability to comply with s. 6(1) of FIPPA.

In addition, when looking at the specific November 20, 2014 access request, the Deputy Chief of Staff's broad interpretation of transitory records has resulted in emails that she should have properly retained not being available once she completed her search for responsive records.

**I find that the Office of the Premier contravened its duty under s. 6(1) of FIPPA to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 20, 2014 access request to the Office of the Premier for the outgoing emails of the Deputy Chief of Staff.**

# 6.0 RESTORING PUBLIC CONFIDENCE

It is difficult to overstate the seriousness of the problems that my office discovered in the course of this investigation and the resulting effect on the integrity of the access to information process in our province. These problems include:

- deleting emails responsive to access to information requests and preventing others from producing these records;
- either wilfully or negligently failing to produce records that are potentially responsive to an access request;
- failing to keep any sent emails, irrespective of the topic;
- failing to tell the truth to my office under oath;
- failing to clarify a request with an applicant or to communicate effectively internally regarding the processing of a request, which results in the applicant feeling a file has not been processed in good faith;
- implementing a verbal process for responding to access to information requests that avoids personal accountability; and
- flaws in the configuration of government's email system and its backup of email accounts that compromised my office's ability to perform elements of this investigation and create the potential to impact future investigations by my office as well as by government itself.

In light of the serious nature of these problems, it is important that government take immediate action to restore public confidence in the access to information process. Where major problems exist, only major change will suffice. Below I set out a path that I believe government should follow in order to demonstrate it takes these issues seriously and accepts that it is time for a change in culture.

## 6.1 MEETING THE DUTY TO ASSIST

The obligation under s. 6(1) of FIPPA on public bodies "to respond without delay to each applicant openly, accurately and completely" is at the heart of this investigation and has arisen in numerous contexts. If public bodies do not meet their obligations under this section, the access to information process is rendered ineffective.

My office has clearly stated that when public bodies interpret the wording of access requests, they are not complying with s. 6(1) if they apply a narrow interpretation.[9] Further, if there is any confusion about a request, the public body has an obligation to clarify the nature of the request with the applicant. This obligation can be simply discharged by a phone call or an email from the public body to ensure that it fully understands the applicant's request.

Had this been done at any step along the way by MOTI in the processing of the November 2014 access request regarding Highway 16/the Highway of Tears, the applicant could have received the appropriate records in a timely manner and MOTI would have avoided considerable public scrutiny as to why records had not been produced on this access request.

Program areas within public bodies can play a key role in determining the process that works for them in getting access requests into the necessary hands in an efficient and timely manner. There is room, within this general framework, for program areas to mould the process in a manner that works best for them.

But, as was the case with the Executive Branch of the Office of the Premier, there is no room to create the potential for a systemic delay in communicating the existence of access requests to individuals who might have responsive records. Such a delay will inevitably lead to the loss of potentially responsive records to some access requests.

With this in mind, it is essential that all program areas have a system in place that results in access requests being emailed to all employees with potentially responsive records as soon as possible. If follow-up in person is desirable in some instances, this should be an additional measure that is taken and not the only means of notifying employees. Further, employees within program areas who have responsibility for the coordination of responses should keep reliable electronic records of the responses of all individuals who they correspond with for a reasonable amount of time after the resolution of an access request in case follow-up is needed.

[9] See, for example, https://www.oipc.bc.ca/investigation-reports/1510.

IAO should provide government employees with substantive guidance on how to search for potentially responsive records. While I appreciate that for some employees this might seem rather basic, the results of this investigation show that this is not the case for all individuals. Of course, even the best guidance is only useful if it is followed.

Ultimately, each government employee must take the time to conduct a proper search for each and every access request that they receive. The amount of time it takes to do a thorough search for each request is minimal compared to the amount of time it takes to deal with adequate search complaints that result from poor initial searches.

There is nothing complicated or particularly onerous that is required for public bodies to meet their duty to assist applicants under s. 6(1) of FIPPA. It simply requires public bodies making this duty a priority and putting in place appropriate processes to enable this to occur on a consistent basis.

**RECOMMENDATION 5:**

Government should clarify access requests with applicants where necessary to ensure it does not interpret the request too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request.

**RECOMMENDATION 6:**

Government should create clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request. This guidance should be incorporated into government's access to information training and should specifically include that employees should conduct searches from their desktop or laptop and not from mobile devices.

## 6.2 TRANSITORY RECORDS

Proper management of government records is another critical component of access to information rights and goes to the heart of government being able to meet its duty to assist under s. 6(1) of FIPPA. Without the proper retention of records and a fulsome understanding of transitory records, government cannot effectively preserve these rights.

In previous reports, I expressed concerns about overly liberal interpretations as to what constitutes a transitory record.[10] While those we interviewed had a general understanding of transitory records, over the course of this investigation my investigators heard evidence to support my concern.

Throughout this investigation, we consistently heard individuals claim that government records retained elsewhere could be destroyed as transitory. While it may be the case that there is a designated office for retaining particular records, employees need to know who is responsible for record keeping in order to make informed decisions about whether or not a record is transitory. Employees should know that records are being retained before they destroy non-transitory records as unnecessary copies. For this to happen, employees need to understand their office's record keeping system as well as their individual responsibility for managing records.

During our interviews we also heard conflicting opinions about whether or not drafts of decision or issues notes for ministers are transitory records, and whether or not cursory advice needs to be retained. Draft documents or email advice that shows how decisions were reached should be retained. These records provide evidence regarding high-level decision-making and approvals.

All government employees have a responsibility to ensure that they are properly managing records. Despite this responsibility, government does not currently offer mandatory training dedicated to records management. The current government training on access to information delivered to all employees and to those located in Minster's offices included insufficient information about transitory records or the broader topic of records management. This is an important and nuanced subject that is foundational to citizens' ability to meaningfully exercise their access rights.

[10] See pp. 18-19 of https://www.oipc.bc.ca/investigation-reports/1510 and p. 31 of https://www.oipc.bc.ca/special-reports/1696.

I note that government has created effective guidance material for its employees on this topic, but lacks the training component for delivery of this guidance.[11] Training is important in order to ensure that employees understand proper records management, including the filing, retention and disposition of records.

Government should also be encouraging employees to contact those within the Office of the Chief Information Officer, which has expertise in this area, when questions arise. This message should be reinforced in the dedicated training sessions on the topic of transitory records.

There also needs to be independent oversight of the destruction of government records. It is unacceptable that no independent body watches over this important step in the lifecycle of government records. Adding independent oversight would be a major step towards restoring public confidence that government properly destroys its documents and is accountable for its practices.

**RECOMMENDATION 7:**

Government should provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records. This training should describe employees' responsibilities for records management and provide the basis for understanding an office's record keeping system.

**RECOMMENDATION 8:**

Government should legislate independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met.

[11] See http://www.gov.bc.ca/citz/iao/records_mgmt/guides/transitoryug.pdf and http://www.gov.bc.ca/citz/iao/records_mgmt/guides/email_decision.pdf.

## 6.3 MANAGING GOVERNMENT'S EMAIL SYSTEM

At numerous points in this investigation, my office encountered problems with government's email system that impacted our ability to acquire evidence that would have been useful in this investigation.

The failure of government to ensure monthly backups were in place in the transition of servers from Microsoft Exchange 2007 to Microsoft Exchange 2013 denied my office the ability to see crucial evidence in our examination of the November 2014 access request to MOTI regarding Highway 16/the Highway of Tears. Government says that this problem has since been rectified in such a way that should ensure it does not happen again. Given the impact that the lack of backups can have on government investigations, litigation involving government records and investigations of my office, government should also have in place a plan to monitor its backups.

Our investigation also uncovered a practice of deletion of records in certain government offices that I had not previously been aware of, namely the emptying of the Recover Deleted Items folder or, as was described to us by several people interviewed for this Report, "triple deletion". The Recover Deleted Items folder is intended to allow individuals to recover emails that have been deleted by accident or that soon after deletion become relevant.

The practice we observed was the routine emptying of the Recover Deleted Items folder to ensure that emails were permanently deleted from an employee's system. This is not the intention of the Recover Deleted Items folder and for employees managing their mail account it serves no legitimate purpose. Only emails in an employee's Inbox, Sent Items, custom folders or Deleted Items folders counts towards their allotted mailbox space limit. Emails in the Recover Deleted Items folder do not. Therefore, deleting items from the Recover Deleted Items folder, i.e. triple deleting, is of no advantage in creating more space in an employee's account.

Government should configure the settings in Microsoft Outlook such that it does not allow individual employees to remove items from the Recover Deleted Items folder.

The Recover Deleted Items folder is also relevant with respect to monthly backups. As explained earlier in this report, monthly backups currently capture what is in the Recover Deleted Items folder. But the Recover Deleted Items folder is set so that it retains items for only 14 days. This means, for example,

that if an item arrives in an employee's mailbox early in the month and is moved to the Recover Deleted Items folder shortly thereafter, it will have purged from the mailbox before the monthly backup takes place at the end of the month.

In other words, there will be no permanent record of the substance of the email itself. This limitation impacted my office's investigation as well in that some emails can come and go from an employee's account without ever being captured in a monthly backup, so it is currently not possible to determine the existence of certain emails. The metadata that government does capture, including the subject line of emails, is not enough to discern the substance of emails.

This problem can be easily rectified by ensuring that items in the Recover Deleted Items folder are retained for just over a month to ensure they are caught by the monthly backup system. I appreciate this requires additional storage space for government emails, but this incremental cost is justified given the value such emails can play in investigations or litigation by ensuring a lasting record of all government emails. As discussed earlier in this report, a public body's reasonable efforts to assist applicants under s. 6(1) of FIPPA include having to search this folder when there is a reasonable belief that this folder may contain responsive records.

**RECOMMENDATION 9:**

Government should configure the settings in Microsoft Outlook to prevent employees from removing items from the Recover Deleted Items folder.

**RECOMMENDATION 10:**

Government should configure the settings in Microsoft Outlook so that it preserves items in the Recover Deleted Items folder for just over one month. This would ensure all government emails are captured in monthly backups.

## 6.4 DUTY TO DOCUMENT

Government must adopt a legislated duty to document in order to regain public confidence in the access to information process. The public has a right of access to records for the purpose of making public bodies accountable. But this right can only be exercised if a record exists. It is predicated on the creation of records that document the affairs of government.

My office investigates numerous complaints each year where applicants question how it is that records about key government decisions do not exist. Government's response in these investigations is often that it never created records. This is partly the result of an entrenched oral culture of decision-making in government. This culture undermines public sector accountability as public bodies can effectively avoid public scrutiny as to the basis and reasons for their actions.

I am cognizant that removing an employee's ability to triple delete emails might create a further temptation towards the culture of oral government. This concern further underlines the importance of a duty to document.

A legislated duty to document would help address public concerns about the accountability of their government by creating a positive duty for public servants and officials to create records of their business activities. This duty does not need to be onerous and criteria could be prescribed to define its application. FIPPA, it should also be remembered, already creates a number of exceptions to disclosure of information, including an exception for providing advice and recommendations.

The retention and accessibility of records has been complicated by the adoption of new communications technologies, the volume and variability of records, and challenges posed by developments such as bring your own device arrangements. These challenges do not alleviate public bodies' responsibilities under access legislation. By deliberately creating and managing records, public bodies uphold access rights and ensure that records exist for evidence-based decision-making, legal obligations, and a comprehensive historical record.

**RECOMMENDATION 11:**

Government should create a legislative duty to document within FIPPA as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its key decisions and actions.

# 7.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

## 7.1 SUMMARY OF FINDINGS

I have made the following findings in this investigation:

1. I find that the Ministry of Transportation and Infrastructure contravened its duty to assist under s. 6(1) of FIPPA by interpreting the applicant's request narrowly and failing to clarify the nature of the records being sought in the November 2014 access to information request regarding Highway 16/the Highway of Tears.

2. I find it is more likely than not that George Gretes deleted emails on Tim Duncan's computer on November 20, 2014, that may have been responsive to the Highway 16/Highway of Tears access request. It follows that Ministry did not comply with s. 6(1) of FIPPA because it failed to openly, accurately and completely respond to that request.

3. I find that the Ministry of Advanced Education contravened its duty under s. 6(1) of FIPPA to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the July 21, 2014 access request for emails between the Chief of Staff and the Minister.

4. I find that the Executive Branch's systemic delay in its processing of access requests and the resulting loss of potentially responsive records is a contravention of the Office of the Premier's duty under s. 6(1) of FIPPA "to respond without delay to each applicant openly, accurately and completely."

5. I find that the Office of the Premier contravened its duty under s. 6(1) of FIPPA to make every reasonable effort to respond without delay to the applicant openly, accurately and completely regarding the November 20, 2014 access request to the Office of the Premier for the outgoing emails of the Deputy Chief of Staff.

## 7.2 SUMMARY OF RECOMMENDATIONS

### RECOMMENDATION 1

The Ministry of Transportation and Infrastructure should release the 36 pages of records initially identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on November 19, 2014 for:

> "… all government records that make reference to the issue of missing women along Highway 16 / the Highway of Tears and specifically including records related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."

### RECOMMENDATION 2

Government should develop a policy for all future data migrations that requires at a minimum:

1. Hourly, daily and monthly backup of data;
2. Written directions to government's service provider with respect to these backups; and
3. Government monitoring of the directions to ensure their compliance.

### RECOMMENDATION 3

The Ministry of Advanced Education should release the approximately 20 email records identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on July 21, 2014 for:

> "Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014."

The Investigations and Forensics Unit will retrieve the emails and provide them to the Ministry.

### RECOMMENDATION 4

The Executive Branch of the Office of the Premier should change its access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.

## RECOMMENDATION 5

Government should clarify access requests with applicants where necessary to ensure it does not interpret the request too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request.

## RECOMMENDATION 6

Government should create clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request. This guidance should be incorporated into government's access to information training and should specifically include that employees should conduct searches from their desktop or laptop and not from mobile devices.

## RECOMMENDATION 7

Government should provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records. This training should describe employees' responsibilities for records management and provide the basis for understanding an office's record keeping system.

## RECOMMENDATION 8

Government should legislate independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met.

## RECOMMENDATION 9

Government should configure the settings in Microsoft Outlook to prevent employees from removing items from the Recover Deleted Items folder.

## RECOMMENDATION 10

Government should configure the settings in Microsoft Outlook so that it preserves items in the Recover Deleted Items folder for just over one month. This would ensure all government emails are captured in monthly backups.

**RECOMMENDATION 11**

Government should create a legislative duty to document within FIPPA as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its key decisions and actions.

# 8.0 CONCLUSION

FIPPA was brought into force in British Columbia in 1993 to serve as a foundation upon which government would be open and accountable to its citizens. Over the course of my tenure as Information and Privacy Commissioner, I have made many recommendations to enhance citizens' access to information rights. While government has adopted some of my recommendations, it has chosen not to implement certain key changes such as a legislative duty to document and independent oversight over the creation and destruction of records.

Legislative amendments are, however, only part of the required action. In order for change to be truly effective, leaders in government and within individual public bodies must embrace their responsibilities under FIPPA and create a culture that emphasises the importance of fulfilling their obligations to the public. The majority of problems witnessed in this investigation occurred in offices that are inherently political in nature. While this investigation is not broad enough to be truly systemic, it does raise concerns for me that Ministerial offices are more likely to suffer from some of the problems illustrated in this report than other offices within government.

Government leaders must fully embrace both the words and the spirit of our access to information legislation to ensure a true culture of public accountability. This requires, among other things, that employees benefit from more effective and mandatory training on key aspects of the access to information process, including how to properly determine whether a record is transitory in nature. Even more important, however, is creating a daily atmosphere in government offices that demonstrates the importance of access to information.

In the face of severe challenges lies an opportunity for government and for British Columbians. Government can make the necessary changes to legislation as well as to policies and processes that would help regain public confidence and establish our province as a national and international leader in access to

information. For this to take place government has to demonstrate, through immediate and meaningful action, its will to ensure a government-wide culture of respect for citizens' access to information rights.

# 9.0 ACKNOWLEDGEMENTS

The Government of British Columbia cooperated fully with my office's investigation. I would specifically like to acknowledge the cooperation of the Investigations and Forensic Unit.

I would also like to thank Michael McEvoy, Deputy Commissioner, Troy Taillefer, Senior Policy Analyst, and Nathan Elliot, Policy Analyst, who conducted this investigation and contributed to this report.

October 22, 2015

**ORIGINAL SIGNED BY**

_____
Elizabeth Denham
Information and Privacy Commissioner
for British Columbia