

ADDENDUM
to
**Deleting Accountability:
Records Management Practices
of Political Staff**

A Special Investigation Report

August 20, 2013



**Information & Privacy Commissioner,
Ontario, Canada**

**Ann Cavoukian, Ph.D.
Commissioner**

ADDENDUM
to
Deleting Accountability:
Records Management Practices
of Political Staff

A Special Investigation Report



Table of Contents

Introduction	1
Background	1
Post-Report Activities	3
Further Investigation	8
Conclusion	17
Appendices	21

Introduction

On June 5, 2013, I released my Special Investigation Report, *Deleting Accountability: Records Management Practices of Political Staff*. In that Report, I made findings critical of the email management practices of political staff that were identified through hearings taking place before the Standing Committee on Justice Policy (Justice Policy Committee). I also commented on the failure of political staff to retrieve emails responsive to motions of the Justice Policy Committee and to a number of freedom of information requests. This included the conclusion that emails, once deleted from the government email system, were unlikely to be retrievable. These observations and conclusions were based on information provided to my office by senior government officials.

Subsequent to the release of my Report, I was provided with new information regarding the Ontario Public Service (OPS) Enterprise Email System – information that should have been given to me during my investigation. This information was material to the issues in my investigation and directly responsive to questions my staff had asked. I was also informed that the Ministry of Government Services (MGS) had found 39,000 emails either sent or received by the former Chief of Staff to the former Minister of Energy, Craig MacLennan. In light of this new information and the fact that I had previously been misled, I felt it was important to prepare this Addendum in order to set the record straight. It should be added that the Deputy Minister for MGS apologized to me on several occasions and assumed full responsibility for his staff failing to provide me with the necessary information.

This Addendum describes the circumstances surrounding the disclosure of new information provided by MGS staff and sets out the detailed information that was not provided to my staff during the initial investigation. It describes the OPS Enterprise Email System and explains why this new information was relevant to the discovery of responsive emails. In my concluding remarks, I explain that in light of the information I now have, I would have arrived at a different conclusion regarding the ability of MGS staff to retrieve the relevant emails from Mr. MacLennan's email account. However, as I explain below, the other findings in my Report were not affected and remain accurate. In addition, all of the recommendations contained in my Report continue to be valid and remain unchanged.

Background

Complaint

In April 2013, my office received a complaint from MPP Peter Tabuns alleging that Craig MacLennan, the former Chief of Staff to the former Minister of Energy, had improperly deleted all emails concerning the cancellation of the Oakville and Mississauga gas plants. This allegation arose as a result of Mr. MacLennan's testimony before the Justice Policy Committee. Upon receipt of this complaint, my office immediately launched an investigation.

Investigation

As part of the investigative process, I conducted interviews with senior government officials who were thought to have knowledge of the issues, including the Secretary of the Cabinet, the Chief Information Officer (CIO) of the province, both the former and current Chiefs of Staff to the Minister of Energy and the former and current Premier, as well as the Executive Lead of the Information Technology Services Division for MGS (Executive Lead IT).

In April 2013, during my initial interview with the Executive Lead IT, I made it clear that in addition to reviewing the practices of the former minister's staff, my office would be looking into the possibility of whether any of the emails that had been deleted could be retrieved or reconstructed from possible archiving or any back-up systems.

During my investigation, I was kindly offered the assistance of Chuck Rothman, a specialist in computer forensics and electronic discovery, who works with the law firm, Wortzman Nickle Professional Corporation. Mr. Rothman provided independent, expert advice to my staff throughout the investigation. I note that the information provided to Mr. Rothman during the initial investigation was the same information that was provided to my office, thus the validity of the findings in the Report are no reflection on Mr. Rothman's expertise.

Upon completion of my investigation, I released the Special Investigation Report in which I concluded that the indiscriminate deletion of emails was in violation of the province's *Archives and Recordkeeping Act* (the ARA), and that this practice undermined the public's right of access to government records and the principles of the *Freedom of Information and Protection of Privacy Act*.

Based on the information provided to me at that time, I also concluded that the deleted emails in Mr. MacLennan's email account were irretrievable, subject to any back-up tapes that may not have been overwritten. This view was confirmed by Mr. Rothman.

With respect to the back-up tapes, the Executive Lead IT stated that there were no back-up tapes containing emails created during the relevant time period – any tapes that may have existed would have been overwritten as part of the usual back-up process. On this basis, I also concluded that it was not possible to retrieve any of the emails from the back-up tapes. This view was also confirmed by Mr. Rothman.

In my Report, I made a number of recommendations to the Premier's office and MGS, calling for a review of the Archives of Ontario records retention policies and practices, as well as the development of policies and procedures to ensure that political staff were fully trained regarding their records management obligations. My recommendations also called for the designation of a senior individual in each minister's office and the Premier's office to be accountable for the implementation of records management policies, and for ensuring that all new staff received appropriate training. I further recommended that the Premier issue a Directive to all political staff setting out the Premier's expectation that all staff will comply with the relevant laws and policies.

Post-Report Activities

OPP Investigation

On June 7, 2013, two days after I released my Report, the Ontario Provincial Police (OPP) launched a criminal investigation into the destruction of emails relating to the relocation and cancellation of the gas plants. The OPP investigation is independent of my investigation, including the inquiries leading to the completion of this Addendum. However, my office is cooperating fully with the OPP.

Justice Policy Committee

On June 25, 2013, I appeared before the Justice Policy Committee to answer questions about my Special Investigation Report. During my appearance, I testified that I found it very difficult to accept that the routine deletion of all emails was not an attempt by the staff in the former Minister's office to avoid transparency and accountability. Further, it was my belief that the absence of responsive records from the Minister's office was a result of both a failure to comply with the retention requirements of the ARA and a culture of avoiding the creation of written or electronic records. I explained that one of the most important rights that citizens enjoy in a free and democratic society is access to information about the activities of their government. I also stressed what had been set out in my Report – that without written records of how government decisions are made, transparency is seriously undermined and the basis for the government's policy choices is shielded from public scrutiny.

At the end of the Justice Policy Committee's session on June 25, 2013, the Committee passed three motions. Of relevance to this Addendum is the motion that required MGS to produce all documents and electronic correspondence stored on the Ministry's servers, related to the cancellation and relocation of the Oakville and Mississauga gas plants, sent or received, from 13 named individuals, including Mr. MacLennan.

New Information Uncovered

On July 9, 2013, my staff was advised that responsive emails from Mr. MacLennan's email account had been discovered. Upon receipt of this information, I immediately notified one member from each of the three political parties with representation on the Justice Policy Committee. I felt that for purposes of transparency I had to advise them of the new information that had been relayed to me.

The next morning, on July 10, 2013, I met with the Deputy Minister at MGS, Kevin Costante, and the CIO for this province, David Nicholl, at their request. At that meeting, the Deputy Minister informed me that approximately 39,000 additional email records sent or received by Mr. MacLennan had been found during the search carried out in response to the Justice Policy Committee's motion. Of those, approximately 1,800 related to the cancellation and relocation of the gas plants.

The Deputy Minister explained that in order to respond to the June 25, 2013 motion requiring that MGS produce email records relating to the cancellation of the gas plants, MGS staff had asked its Corporate Security Branch (CSB) to assist in the search. The Deputy Minister stated that CSB was called in because “they are routinely used to conduct electronic searches for documents. This left me with an obvious question, why had CSB not been brought in to assist during the course of my investigation?

It became apparent during this meeting that in response to the Justice Policy Committee’s motion, significantly greater effort was put into searching for emails than had been put into doing so during my investigation. It also became apparent that important details about the configuration of the OPS Enterprise Email System had not been provided to my staff. In particular, my office was not provided with accurate information about the archiving and/or storage tools in use by MGS, nor were we told about any possible back-up tapes existing from the relevant time period. This information should have been conveyed to my staff during my investigation. This failure to provide my staff with a complete and accurate picture materially affected the accuracy of my Report.

As an Officer of the Legislature, I expect the highest degree of cooperation and diligence from all institutions during my investigations. I was baffled as to how MGS staff could have failed to provide relevant, accurate information about the IT systems under its control. More baffling was the fact that the resources that were brought to bear on the search for records in response to the Justice Policy Committee’s motion were not brought to bear in the context of my investigation. There is simply no valid reason why the CSB search team had not been asked to conduct the same review in response to my investigation as it had conducted in response to the Justice Policy Committee’s motion.

In our July 10th meeting, the Deputy Minister explained that Mr. MacLennan’s emails had been found in an “orphaned Enterprise Vault” associated with his email account. The “Enterprise Vault” is used to provide low cost secondary storage for emails that are over 30 days old, of many government ministries, including the Ministry of Energy. The Deputy Minister also informed me that MGS staff discovered at least one back-up tape for the relevant period of time that had not been overwritten. This back-up tape was in the possession of Iron Mountain – an off-site storage service provider to MGS.

It is important to note that MGS staff had not informed my investigators nor made any mention of an Enterprise Vault having been applied to Mr. MacLennan’s email account. In fact, in response to my staff’s questions about whether MGS has any archiving solutions in place, MGS staff responded that it did not, failing to mention that the Enterprise Vault existed, and that it was a key component of the government’s email infrastructure. In addition, when my staff had specifically asked MGS to confirm that all relevant back-up tapes had indeed been overwritten, MGS answered affirmatively, confirming this fact – even though this was not the case.

The Deputy Minister apologized profusely and acknowledged that my office had been provided with inaccurate and incomplete information regarding the OPS Enterprise Email System and the existence of possible back-up tapes from the relevant period. When I asked how this could possibly have occurred, he promised to provide my office with a full accounting to explain this failure.

On July 12, 2013, I wrote to the Deputy Minister (Appendix 1) reiterating my dissatisfaction with the recent revelations about the MGS IT systems and the inaccurate information provided during my investigation. I noted that the failure of MGS to work with my office directly affected my ability to report back to the people of Ontario about the possibility of retrieving the deleted emails. I also advised the Deputy Minister that I was expecting a full accounting of what had transpired.

On July 22, 2013, I received a letter from Deputy Minister Costante (Appendix 2), in which he again accepted full responsibility for the inaccurate information provided to my office. Specifically, the Deputy Minister stated:

I wish to communicate my regret that we did not provide your office with all the information necessary to assist your investigation.

...

Our work on the Justice Policy Committee motion has subsequently shown that we had exceptions to our normal protocols regarding deletion of email accounts and the retention of back-up tapes that should have been identified and reported to you as part of your investigation.

The Deputy Minister explained how these emails, contained in the “orphaned Enterprise Vault,” had been uncovered as part of the search for records responsive to the Justice Policy Committee’s motion:

ITS staff were also asked to check whether any decommissioned email accounts assigned to the individuals [named in the motion] had both primary and secondary storage components deleted, given that email accounts are maintained on two separate systems. ITS staff undertook a search of the Enterprise Vault server and a portion of the email account of Mr. Craig MacLennan, which was decommissioned in September of 2012, was identified.

In this regard, the MS Exchange portion of his account had been deleted, the secondary storage had not.

With regard to the discovery of back-up tapes that may contain relevant information, the Deputy Minister stated:

As part of our assessment of the availability of back-up tapes to respond to the Justice Policy Committee motion, staff also reviewed our existing inventory of back-up tapes in relation to the named individuals from the time of the motion backwards. This included a review of tapes held at our storage service provider Iron Mountain. Iron Mountain has been our service provider for the last ten years.

I responded to the Deputy Minister's letter on July 23, 2013 (Appendix 3) and reiterated my dissatisfaction with the response of MGS to my investigation. The Deputy Minister replied by letter dated July 24, 2013 (Appendix 4) acknowledging that steps were taken in response to the Justice Policy Committee's motion that also should have been taken in responding to my investigation.

It is important to note that at no time during the course of my initial investigation did MGS staff mention to my staff that MGS used the services of Iron Mountain. While I gather that MGS staff was of the opinion that this information was not relevant to my investigation, the back-up tapes in the possession of Iron Mountain potentially contained responsive emails and were thus directly relevant. For that reason, I am dismayed that the use of Iron Mountain was not disclosed to me, as it would have led my investigators to pursue additional lines of questioning.

In response to my question regarding how MGS could have "uncovered" relevant back-up tapes after assuring my office that none existed, the Deputy Minister stated:

The existence of additional back-up tapes in our inventory is attributable to some exceptional circumstances. In July of 2012 we started a refresh of our email system; we moved from Microsoft Exchange 2003 to Microsoft Exchange 2010. As part of the change process in November 2012, IT staff maintained the previous year's monthly back-up tapes on our old email system. This has resulted in the retention of more back-up tapes than we had first realized when we responded to your question about whether back-up tapes exist during the relevant period.

When I specifically asked the Executive Lead IT why the description of the Enterprise Vault and its relationship with the OPS email accounts had not been provided at the first meeting with my office, he indicated:

The nature of the first meeting was high level. I provided a general summary of the primary email environment, back-up tape process and the records deletion process. I made a mistake and should have described the Enterprise Vault during those discussions. I apologize for this oversight.

When I asked further why the Executive Lead IT had confirmed that all back-up tapes were overwritten when they had not been, he answered:

I referenced the general practice of the OPS tape back-up retention policy that the Minister of Energy was part of. The Ministry of Energy period between September 1, 2010 to December 31, 2011 identified in the original question was outside of the OPS Tape back-up retention period of one year. I based my response on the general practice of the OPS Tape retention policy. Since then I have learned of some exceptional cases where back-up tapes were retained beyond the general practice due to major projects and software upgrades.

I note that in the Deputy Minister's testimony before the Justice Policy Committee on August 6, 2013, he provided finality and clarity on these issues. A number of questions were asked by the members of the Committee regarding the information provided to my office during my initial investigation and the circumstances surrounding the discovery of Mr. MacLennan's emails.

When asked about the discovery of relevant back-up tapes, Deputy Costante stated:

[W]e didn't look under the hood. When we looked under the hood, we found a back-up tape for December 2011 for Mr. Craig MacLennan.

During his testimony, Deputy Costante acknowledged that MGS staff should have verified the information provided to my office regarding the back-up tapes as they were asked to. For example, he stated:

I'm not denying – we should have went and verified. I fully acknowledge that we should have went and verified and we didn't. We responded on what our policy was, and we didn't verify. That was our mistake.

With respect to the Enterprise Vault and its application in the OPS Email System, and the discovery of the “orphaned” Enterprise Vault associated with Mr. MacLennan's email account, Deputy Costante testified:

[W]e have taken responsibility for the mistakes. We should have told the Privacy Commissioner and given her a broader explanation of how our email system works and that there's a primary and secondary account.

He also described the approach that MGS staff took to my investigation as follows:

[W]hen we responded to questions, we responded from a policy perspective, and we should have gone in and *verified that the reality was the same as the policy*.
[Italics added]

While I accept the Deputy Minister's explanation for these oversights, I remain saddened that I was only provided with the **policy** relating to these practices, not the reality. Critical information, which was available at the time of my investigation, was only disclosed to me several weeks after the issuance of my Report, in response to the Justice Policy Committee's motion. It is interesting to note that, last year I had issued a white paper entitled: *A Policy is Not Enough: It Must be Reflected in Concrete Practices*,¹ precisely because a policy has little value if it is not mirrored in the actions taken by staff. This investigation would appear to be a case in point.

1. <http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1210>

In summary, following the release of my Report, I learned that senior staff in MGS's IT department had failed to provide me with a complete description of the OPS Enterprise Email System and the existence of relevant back-up tapes. In addition, relevant portions of the information they provided were not accurate. Further, greater resources and diligence were brought to bear by MGS to respond to the Justice Policy Committee's motion than were devoted to my investigation. This resulted in inaccurate information appearing in my Report, which unfortunately, had the consequence of misleading the public on this very important issue.

Further Investigation

For all of these reasons, I decided to reopen my investigation and prepare this Addendum to set the record straight. In order to provide my staff with independent expertise and advice, I retained the services of a highly recommended IT expert, Christopher Henry.

Mr. Henry provides independent advice on enterprise information technology strategy, selection, implementation, efficiency and effectiveness. In his more than 20 years in information technology in various roles as a Corporate Director of IT Operations and as a Chief Information Officer, Mr. Henry has overseen the selection, implementation and operation of mission critical regional, national and global enterprise systems including email and back-up systems. Mr. Henry has also given expert testimony in U.S. Federal District Court, and is a member of the CIO Association of Canada, speaking at numerous CIO summits and tech conferences.

My staff and Mr. Henry arranged for a site visit to the Primary MGS Data Centre on July 31, 2013. Prior to this visit, we provided MGS IT staff with a number of written questions regarding the OPS Enterprise Email System, back-up systems and the Enterprise Vault. After reviewing the operations of the Primary MGS Data Centre, answers to our specific questions were provided and we were briefed on the systems and Enterprise Vault. We then had an in-depth meeting with a number of individuals, including:

Dave Nicholl – Chief Information Officer

Marty Gallas – Corporate Chief Infrastructure Technology Services

Rocco Passero – Executive Lead IT

Kent Schramm – Head Corporate Security

Zelko Holjevac – Director Desktop Services/Field Services

Heather Clarke – Director Policy and Planning

Don Fawcett – Senior Legal Counsel

David Cullen – Manager Forensics and PEN Tests

David Chadbourne – Manager Enterprise Email Service Operations

Pat Mattson – Manager Server Management, Data Centre Operations.

Primary Data Centre

The Primary MGS Data Centre is Tier 4 (certified by Uptime Institute as Tier 4 Gold certification for Operational Sustainability) “Fault Tolerant” certified as it is physically designed, furnished and operated with heating, ventilation, air conditioning, fire and security systems to meet a 99.995 per cent availability standard for the systems hosted there. The Data Centre is also LEED accredited Tier 4 Gold having met the Leadership in Energy and Environmental Design green building design requirements. It functions, in part, as the operating and storage facility for OPS Enterprise Email Systems servers and the OPS Email Back-up System.

OPS Enterprise Email System

The OPS Enterprise Email System is a Microsoft Exchange 2010 Environment that was designed using industry best practices from Microsoft and has over 94,000 email accounts. To support the ongoing email storage needs of the large number of accounts, two tiers of storage were implemented in relation to the majority of email accounts.

The first tier is the Microsoft Exchange Primary Storage (Primary Storage) where emails up to 30 days old are stored. The second tier is the Enterprise Vault Secondary Storage where emails greater than 30 days old are stored. The second tier stores the majority of emails and is more cost effective storage because the hardware is less expensive and slower than the Primary Storage. Remarkably, during our initial investigation, my staff was only told about the Primary Storage.

Subsequent to the release of my Report, my staff was told that the default email setup of the majority of Ontario government ministries, including the Ministry of Energy, email accounts, uses both the Primary Storage and the Enterprise Vault Secondary Storage. The default email setup for staff in the Premier’s office, as well as a small number of other government ministries, **only** uses the Primary Storage. In both scenarios, if a user never deletes emails from his or her **Deleted Items** folder, the emails will be maintained.

As of January 2013, the MGS process for deleting or decommissioning entire email accounts of departing staff, and their associated Enterprise Vault, was a manual one i.e. staff at MGS had to delete the Primary Storage account and Secondary Storage account separately. In January of 2013, MGS staff discovered that while the Primary Storage of the email accounts for some departing employees had been deleted, in the case of approximately 30,000 users who had left the employment of the OPS, the Enterprise Vault had not been deleted and this data was still being stored in the Enterprise Vault Secondary Storage. In other words, MGS IT staff failed to manually delete the associated Enterprise Vaults of some users. As a result, there were approximately 30,000 “orphaned Enterprise Vault Files” on the Secondary Storage. MGS has changed its protocols and the removal of “orphaned Enterprise Vault Files” is planned following the migration to a newer version of the Enterprise Vault software. However, “orphaned Enterprise Vaults” that may be relevant to the gas plants are not being removed.

OPS Email Back-up System

The OPS Email Back-up System is a Symantec NetBackup Environment that has the primary purpose of backing up a copy of 800 Terabytes of OPS Enterprise Email System configuration² and data to tape so it can be restored in case of a disaster or major system crash. All daily, weekly and monthly back-up jobs are full back-ups of retained emails, run across multiple tapes and are listed and tracked in the NetBackup Tape Catalogue.

Currently there are 15,000 tapes in circulation, with an average lifespan of four years due to tape rotation and retention. Tapes taken off-site go to Iron Mountain for safekeeping. My staff was told that the Ministry of Energy and Premier's office had different back-up retention cycles prior to June 2013. Further, my staff was told that there are exceptions to the back-up tape retention cycle. For example, back-up tapes may be retained longer than scheduled when system upgrades are taking place and back-up tapes may be needed to restore the system.

This information, as well as additional details, are summarized in the tables below, along with other characteristics of the two environments.

2. Email configuration refers to the OPS Enterprise Email System settings as set-up by the MGS Email System administrator(s). The retention of this information enables the restoration of the Email System setup.

Ministry of Energy Microsoft Exchange 2010 Environment with Enterprise Vault		
	Microsoft Exchange Primary Storage	Enterprise Vault Secondary Storage
Purpose	Store emails up to 30 days old.	Store emails more than 30 days old.
What the user sees	Emails up to 30 days old appear and are stored in Outlook folders as managed by the user. Emails greater than 30 days old appear in Outlook folders as managed by the user, have an Enterprise Vault icon, are only a partial “stub” of the original email and point to the full email stored in the Enterprise Vault Secondary Storage.	The full contents of emails greater than 30 days old are stored in the Enterprise Vault.
How an email is deleted	Step 1 – Manual - The user deletes the email from a folder and it moves to the Deleted Items folder. Step 2 – Manual – The user goes to the Deleted Items folder and deletes the email or right-clicks the Deleted Items folder and selects Empty Folder. The email moves to the Recovered Deleted Items folder. Step 3 – Automatic – The email will be removed as soon as possible from the Recover Deleted Items folder during the automated Microsoft Exchange maintenance process.	1 Step – Manual – The user deletes an email with an Enterprise Vault Icon from an Outlook folder or the Enterprise Vault Plug-in in Outlook. After confirming deletion the email is deleted from both the Primary and Secondary storage.³

3. During the upgrade which began in July 2012 from Microsoft Exchange 2003 to Microsoft Exchange 2010, enhancements were made with a newer version of the Enterprise Vault software, to ensure that when a user uses the Microsoft Outlook “delete” for items older than 30 days, that the corresponding Enterprise Vault item is deleted.

Ministry of Energy
Microsoft Exchange 2010 Environment with Enterprise Vault

	Microsoft Exchange Primary Storage	Enterprise Vault Secondary Storage
Orphaned Enterprise Vault Files	Not applicable.	MGS acknowledged that the process of deleting an email account and its associated Enterprise Vault file when a person leaves employment was recently updated and communicated early in 2013. The manual removal of Enterprise Vault files was not being done and led to 30,000 “orphaned Enterprise Vault Files” on the Secondary Storage. The removal of orphaned Enterprise Vault accounts is planned following the migration to a newer version of the Enterprise Vault software.
Sync Conflicts⁴	Emails up to 30 days old that have had a sync conflict between Outlook and Exchange will be stored in the Sync Issues\Conflicts folder. Emails greater than 30 days old will have an Enterprise Vault icon, are only a partial “stub” of the original email and point to the full email stored in the Enterprise Vault Secondary Storage.	The full email of emails greater than 30 days old is stored in the Enterprise Vault.

4. Sync/Conflict folders are Outlook system folders which are generally are not visible in the standard Outlook folder structure. For further discussion, see page 14.

Ministry of Energy Microsoft Exchange 2010 Environment with Enterprise Vault		
	Microsoft Exchange Primary Storage	Enterprise Vault Secondary Storage
Back-up System		
Back-up Tape Contents	Email setup/settings and data	Email data
Back-up Tape Purpose	Restoring the environment in case of a disaster or major system crash.	Restoring the environment in case of a disaster or major system crash.
Back-up Tape Retention Cycle	Daily (7 nights) – 1 Month Weekly – 8 Weeks Monthly (Last Sun-Mon am) – 1 Year	Daily – 8 Weeks Every 12 Weeks – 1 Year
Back-up Tape Retention Cycle Exceptions	Jobs that didn't fully complete due to a failed tape or insufficient time (nightly window for back-ups) due to significant systems upgrades and migrations in case a "back-out" is needed.	Jobs that didn't fully complete due to a failed tape and the increased retention period of some back-up tapes due to significant systems upgrades and migrations in case a "back-out" is needed.

Office of the Premier
Microsoft Exchange 2010 Environment – No Enterprise Vault

	Microsoft Exchange Primary Storage	Enterprise Vault Secondary Storage
Purpose	Store emails regardless of age (no limits).	Not applicable unless the user has email records in Secondary Storage from a previous role/ministry where Secondary Storage was utilized. If so, see Ministry of Energy Table.
What the user sees	All emails appear and are stored in Outlook folders as managed by the user.	See above.
How an email is deleted	Step 1 – Manual – The user deletes the email from a folder and it moves to the Deleted Items folder. Step 2 – Manual – The user goes to the Deleted Items folder and deletes the email or right-clicks the Deleted Items folder and selects Empty Folder. The email moves to the Recovered Deleted Items folder. Step 3 – Automatic – The email will be removed as soon as possible from the Recover Deleted Items folder during the automated Microsoft Exchange maintenance process.	See above.
Sync Conflicts	Emails that have had a sync conflict between Outlook and Exchange will be stored in the Sync Issues\Conflicts folder.	See above.
Back-up System		
Back-up Tape Contents	Email set-up/settings and data	See above.
Back-up Tape Purpose	Restoring the environment in case of a disaster or major system crash.	See above.

Office of the Premier Microsoft Exchange 2010 Environment – No Enterprise Vault		
	Microsoft Exchange Primary Storage	Enterprise Vault Secondary Storage
Back-up Tape Retention Cycle prior to June 2013	Daily 10 days	See above.
Back-up Tape Retention Cycle as of June 2013	Daily (7 nights) – 1 Month Weekly – 8 Weeks Monthly (Last Sun-Mon am) – 1 Year	See above.
Back-up Tape Retention Cycle Exceptions	Jobs that didn't fully complete due to a failed tape or insufficient time (nightly window for back-ups) due to significant systems upgrades and migrations in case a "back-out" is needed.	See above.

Where Responsive Emails Were Later Found by MGS

As noted above, I was informed at my July 10th meeting with the Deputy Minister of Government Services that emails responsive to the motion passed by the Justice Policy Committee had been discovered after the issuance of my initial Report. Since then, MGS staff have located additional potentially responsive emails. Based on information provided by MGS, particularly at the July 31st meeting at the Data Centre, five areas have been identified where responsive emails exist, or may exist, that were not originally disclosed to my office.⁵

1. Responsive emails were found on the Enterprise Vault Secondary Storage within the Enterprise Vault File, particularly related to the former Chief of Staff of the former Minister of Energy. When users started working at the Ministry of Energy, their email accounts had been set up for the vaulting of any retained emails older than 30 days on the Enterprise Vault Secondary Storage. As confirmed by MGS, when the users departed from the Ministry of Energy, only their Microsoft Exchange Primary Storage File was deleted as part of the decommissioning process, not their Enterprise Vault File. This Enterprise Vault File requires manual deletion and in the case of Mr. MacLennan, this had not been done by MGS - so the Vault File remained and responsive emails were found.

⁵ Responsive records may also exist in backed-up data on a user's desktop in the case where a user chooses to back-up their handheld data or Exchange email items locally on the desktop. Backed-up data was not found by MGS on Craig MacLennan's desktop computer during my initial investigation. A further search of Craig MacLennan's computer could not be conducted because the computer had been seized by the OPP.

2. Responsive emails were found in the *Sync Issues\Conflicts* folder of certain users. These folders are Outlook system folders and generally are not visible in the standard Outlook folder structure. Emails end up in the *Sync Issues\Conflicts* folder for one of three reasons: 1) an email could not be uploaded from the Outlook email on the computer to the Exchange 2010 Server; 2) an email could not be downloaded from the Exchange 2010 Server to Outlook email on the computer; or 3) the email got edited in two separate locations at the same time. According to Mr. Henry, reasons one and two can be caused by various software factors including temporary Outlook or Exchange 2010 database corruption, or connectivity factors, including loss of connectivity or a poor connection between Outlook email and the Exchange 2010 server. Reason three typically occurs when multiple versions of the same email are being edited on the same computer in different software or on different devices at the same time. The existence of these emails is not apparent to the user, and a general search of Outlook folders will not identify them. The fact that responsive emails were discovered in the *Sync Issues\Conflicts* folder only came to light as a result of the electronic search performed by CSB.
3. Responsive emails were found in shared drives accessible to certain users. A shared drive is an electronic storage location on a network accessible to a defined group of users. Emails saved on the shared drives could be accessed by other users who have the necessary access rights.
4. Responsive emails may be found in the *Recovered Deleted Items* folder of certain users. The *Recovered Deleted Items* folder is meant to hold deleted emails for a short period of time in case a user has deleted an email by mistake and wants to retrieve it by undeleting it. The deletion of an email in Outlook and Primary Storage is a 3-step process: 1) The user deletes the email from a folder and it moves to the **Deleted Items** folder; 2) The user goes to the **Deleted Items** folder and deletes the email or right-clicks the **Deleted Items** folder and selects **Empty Folder**. The email moves to the **Recovered Deleted Items** folder; 3) The email stays in the **Recovered Deleted Items** folder for the number of days specified by the MGS administrator so the user can retrieve it if deleted by mistake. If the email is not undeleted before the deadline it is removed by Microsoft Exchange during the automated Microsoft Exchange maintenance process. In the case of the OPS Enterprise Email System, the number of days has been set to “0” by MGS so the deletion will typically happen within one day. However, responsive emails sitting in the *Recovered Deleted Items* folder might still be recoverable when back-up tapes are made in accordance with the applicable schedules.
5. Other responsive emails may have been found on approximately 3,000 back-up tapes, of which some had been kept beyond the standard retention cycle of one year. MGS explained that certain back-up tapes had been set aside when the Exchange Email System was upgraded to Exchange 2010 from Exchange 2003 to allow for a restore of the old system in case of a new system failure. This practice was confirmed by Mr. Henry as a reasonable and accepted IT industry best practice. MGS has reported back to the Justice Policy Committee regarding the existence of these back-up tapes and provided the Committee with an estimate of the time and cost of re-constituting the back-up tapes. That decision lies with the Committee.

Having reviewed the information provided by MGS, including the review conducted by Mr. Henry, it appears that MGS has now taken greater effort to locate emails that are responsive to the Justice Policy Committee's motion. While MGS acknowledges that there may yet be surprises, I am satisfied that they have considered the most logical location for responsive emails and have made "good faith" efforts to recover them. Having come to this conclusion, my only regret is that the same efforts had not been made to locate these emails during my investigation.

Conclusion

While I value the collaborative relationship my office has shared with MGS in the past, I remain saddened at the failure of MGS staff to dedicate adequate resources to provide accurate and complete information to my office during the course of my initial investigation. I am left with the inescapable conclusion that they did not take my investigation very seriously. For example, MGS staff did not inform my office about the following essential pieces of information: (1) the existence and the application of the Symantec Enterprise Vault as part of the OPS Enterprise Email System; (2) the existence of approximately 30,000 undeleted or "orphaned" vault accounts; (3) the existence of an inventory of approximately 3,000 back-up tapes; and (4) Iron Mountain's involvement with the back-up tapes.

The provision of inaccurate and incomplete information in my initial investigation is unprecedented during my tenure as Commissioner. As a direct consequence of MGS' incomplete response, the public has been misled as to the nature of the OPS Enterprise Email System and the ability of MGS staff to retrieve potentially relevant information. We now know that relevant email records were indeed retrievable through these systems.

I accept the apologies of senior government officials and the fact that they take full responsibility for their missteps during my investigation. I am hopeful that we will be able to move past these unfortunate events and that in future, investigations by my office will be treated with greater respect, with all possible resources being made available to respond to the inquiries of my investigators. As an independent, non-partisan Officer of the Legislature who reports directly to the Legislative Assembly through the Speaker, a key part of my role is to ensure transparency and accountability in all parts of government. It has been said that the role of an independent Officer of the Legislature is to "execute scrutiny and demand accountability of the executive"⁶ – this is a key component of our democratic process. It is my expectation, and I believe that of all Ontarians, that the public service and members of political staff will be forthright when participating in an investigation conducted by my office.

I have received assurances from senior staff and the Deputy Minister of MGS that the Ministry intends to work with my office in a fully cooperative manner in the future. I believe that Ministry staff regret the manner in which they responded to my investigation. I also believe that the interests of all Ontarians can only be served through the full cooperation of the OPS in my investigations.

6. Paul G. Thomas, "The Past, Present, and Future of Officers of Parliament" in *Canadian Public Administration*, Volume 46, No. 3 (Fall 2003), 292 at 203.

Moving Ahead – Information Management in the Modern Context

This investigation has shone a bright light on some serious concerns related to information management within the Ontario government. As my initial Report made clear, there is great uncertainty with regard to the records retention responsibilities of staff. Email management practices appear to be inconsistent and there is a lack of clarity as to how emails, as public records, are to be retained, stored and deleted in accordance with the ARA and the records retention schedules. Staff training and awareness continue to be ongoing issues, particularly in a fast-changing technological environment.

To its credit, there is clear recognition of these issues within government. Consistent with its desire to work cooperatively with me, the Ministry of Government Services has invited my office to participate in a working group to address these challenges. I am happy to work with MGS and have agreed to provide guidance around the following issues:

- In what way should the information management practices of the OPS be changed to reflect the prevalence and ubiquitous nature of email communications in daily business operations. How can MGS facilitate compliance with the requirements of the ARA for managing public records created or received through email communications.
- Recognizing the size of the workforce, the diverse nature of the work and services provided to the public, and the rapidly changing technological environment, how can MGS implement new information management practices and be satisfied that the workforce will put the policies into practice. How can MGS effect the cultural change necessary to move from policy to concrete practices?
- What are the expectations of the IPC and the government regarding freedom of information requests and the legislative requirement in the *Freedom of Information and Protection of Privacy Act* to conduct a reasonable search for email records responsive to a freedom of information request?

My office will be collaborating with MGS staff to provide advice on the best means to address these issues over the next few months. Regardless of the outcome, the recommendations made in my earlier Report stand on their own, unaffected by the most recent revelations. We present them again below, for your information:

Ministry of Government Services

I recommend that the Ministry of Government Services:

1. Conduct a complete review of the Archives of Ontario records retention policies and practices that apply to the records management processes in ministers' offices and the Premier's office, having regard to the issues raised in this Report. Staff responsibility for retaining business records must be clearly set out, in an effort to ensure proper execution of the retention schedules. Particular attention should be paid to staff responsibility for retaining records originating with, and kept by, offices and branches within the ministries.

Office of the Premier

I recommend that the Office of the Premier:

1. Develop policies and procedures to ensure that ministers' staff are fully trained regarding their records management obligations – immediately following a change in ministers' staff, a change in government, or upon the hiring of any new staff within the office.
2. Require that a senior individual be designated in each minister's office and the Premier's office as the person who is accountable for the implementation of the Archives of Ontario records management policies, and for ensuring that all new staff receive the appropriate training.
3. Issue a directive to all staff within the Premier's and ministers' offices regarding this Investigation Report. This directive should include a message that the Premier takes records retention requirements and the transparency purposes of *FIPPA* and the *ARA* very seriously, has an expectation that all staff will comply with relevant laws and policies, and requires that a senior individual be designated in each office to be accountable for the implementation of records management policies and procedures.

***FIPPA/MFIPPA* amendments**

I recommend that *FIPPA* and *MFIPPA* be amended to address institutions' responsibilities to ensure that all key decisions are documented, to secure retention of records, and to add an offence for the wilful and inappropriate destruction of records. In particular, the amendments should:

1. Create a legislative duty to document communications and business-related activities within *FIPPA* and *MFIPPA*, including a duty to accurately document key decisions;
2. Require that every institution subject to *FIPPA* and *MFIPPA* define, document and put into place reasonable measures to securely retain records that are subject to or may reasonably be subject to an access request under *FIPPA* and *MFIPPA*, taking into account the nature of the records to be retained;
3. Prohibit the wilful destruction of records that are subject to, or may reasonably be subject to, an access request under *FIPPA* and *MFIPPA*; and
4. Make it an offence under *FIPPA* and *MFIPPA* for any person to wilfully destroy records that are subject to, or may reasonably be subject to, an access request under *FIPPA* and *MFIPPA*.



Ann Cavoukian, Ph.D.
Commissioner

August 20, 2013

Date

Appendices

Appendix 1



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

VIA COURIER

July 12, 2013

Mr. Kevin Costante
Deputy Minister, Ministry of Government Services
Associate Secretary of Cabinet and
Secretary of Management Board of Cabinet
99 Wellesley Street West
Room 5320, Whitney Block
Toronto, ON M7A 1A1

Dear Deputy Minister Costante:

Re: Deleting Accountability: Records Management Practices of Political Staff

Thank you for taking the time to meet with my office and I on July 10th.

You indicated during our meeting that the Ministry of Government Services (MGS) would be providing my office and the Standing Committee on Justice Policy with a full accounting of the circumstances surrounding the recent discovery of Mr. MacLennan's emails in the "orphaned vault account" and a back-up tape from the relevant period at Iron Mountain.

I am writing to ask that your accounting specifically address the following issues:

1. Your accounting should explain why MGS failed to disclose the existence of the "Enterprise Vault" and its relationship to the Enterprise Email System, during the course of my investigation. The existence of the Enterprise Vault and its application to Mr. MacLennan's email account should have been disclosed when our offices first met in April, 2013. The existence of the Enterprise Vault was clearly material to the question of whether the emails were retrievable, and it was **directly** responsive to specific questions that my staff asked about the configuration of the Enterprise Email System, Outlook, and the archiving solutions and back-up systems in place.
2. Your accounting should explain why, when specifically asked to confirm that all relevant back-up tapes had been overwritten, MGS unequivocally stated that all back-up tapes for the relevant period had been overwritten – that was **not** in fact, the case. Also, please clarify whether Iron Mountain was contacted by MGS prior to responding to my office's request for confirmation.
3. I understand that, as part of the process of responding to the motion of the Standing Committee dated June 25, 2013, MGS computer forensic experts conducted an examination of the Enterprise Email System. I note that in your letter to the Chair of the Standing Committee on Justice Policy dated July 9, 2013, you stated that in order to

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

- 2 -

respond to the Committee motion, MGS “employed knowledgeable IT staff to conduct the necessary searches.” Please ensure that your accounting explains why MGS at no time advised my office during the course of our investigation of the fact that there was a computer forensic team within MGS whose services could have been used to search for Mr. MacLennan’s emails. Why were their services not offered to my office or utilized by MGS in the context of my investigation?

4. Please explain what was unique about the motion of the Standing Committee dated June 25, 2013, that prompted MGS to devote additional resources to locating the email records and the back-up tape – more so than the resources devoted to my investigation.

I am left with the impression that far less vigour was brought to bear in responding to the inquiries made during my investigation. In fact, it appears that assumptions were made by MGS, such that no one felt it necessary to delve deeply into this matter and look “under the hood” – even when asked to do so.

As an Officer of the Legislature, I have always received full cooperation in the context of my investigations, appeals and complaints. In light of all of these circumstances, you will understand why I am dismayed by the misinformation received during the course of my investigation, and by the failure of MGS to disclose all of the pertinent information. In failing to provide my office with accurate information and the necessary resources available to MGS, my investigation was directly impacted.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

c: Mr. Peter Wallace, Secretary of the Cabinet
Mr. Dave Nicholl, Corporate Chief Information & Information Technology Officer
Mr. Don Fawcett, Senior Counsel, Ministry of Government Services

Appendix 2

Ministry of Government Services

Deputy Minister, Government Services
and Associate Secretary of the Cabinet,
Secretary of Management Board
of Cabinet

99 Wellesley Street West
Room 5320, Whitney Block
Toronto ON M7A 1A1
Tel.: 416-325-1607
Fax: 416-325-1612

Ministère des Services gouvernementaux

Sous-ministre, Services gouvernementaux
et secrétaire associé du Conseil des ministres,
Secrétaire du Conseil de gestion
du gouvernement

99, rue Wellesley Ouest
Édifice Whitney, bureau 5320
Toronto (Ontario) M7A 1A1
Tél.: 416 325-1607
Télééc.: 416 325-1612



July 22, 2013

Ms. Ann Cavoukian, Ph.D.
Commissioner
Information and Privacy Commission of Ontario
2 Bloor Street East
Suite 1400
Toronto, ON
M4W 1A8

Dear Commissioner Cavoukian:

Further to our meeting of July 10, 2013 and your letter of July 12, 2013 I am writing to provide information about the Ministry of Government Services' recent discovery of Mr. MacLennan's email records and explain the process we undertook during your investigation and after the motion of the Standing Committee on Justice Policy (Justice Policy Committee) on June 25, 2013.

In the first instance, I wish to communicate my regret that we did not provide your office with all information necessary to assist your investigation. We cooperated with your investigation and my staff endeavoured to work collaboratively with your office during the investigation process. In April 2013 senior MGS staff, including the Executive Lead of the Information Technology Services Division (ITS) had a meeting with senior staff in your office to provide an overview of the OPS Enterprise email system, our back-up tape process and the records deletion process. Subsequent to this initial meeting, MGS staff worked collaboratively with your staff during the investigation. Our legal counsel liaised with your investigators to obtain answers to their follow-up questions directed to our IT staff.

Our work on the Justice Policy Committee motion has subsequently shown that we had exceptions to our normal protocols regarding deletion of email accounts and the retention of back-up tapes that should have been identified and reported to you as part of your investigation.

The Enterprise Vault

In your letter you have asked why MGS did not identify the existence of the "Enterprise Vault" and its application to Mr. MacLennan's email account, including in our initial meeting in April 2013.

The "Enterprise Vault" is employed on the email accounts of many public servants. The Vault provides low cost storage for emails thirty one days and older. An email account configured with the Enterprise Vault contains two parts: Microsoft Exchange (primary storage) and the Symantec Enterprise Vault (secondary storage).

We treat the Vault as an integral part of our email account – emails stored in the Vault are shown on the screen and displayed to users when they open their account. Account holders can access and delete emails from both the primary and secondary storage parts of their email account. Emails stored in the secondary storage vault are maintained during the life of an email account. When an email account is decommissioned (deleted) our protocols require that both the primary and secondary storage portions of the account are deleted.

After our initial meeting in April 2013, your staff followed up with more specific questions relating to the version of Microsoft Exchange that is utilized by the OPS Enterprise Email System and any configuration to recover deleted emails. Your staff also inquired as to the ability of deleted data to be restored on our RAID servers, Mr. MacLennan's hard drive and our back-up system. I understand that detailed responses to your questions were provided by Ministry staff. We also advised, in answer to your staff member's question as to whether Mr. MacLennan's desktop computer was configured to auto-archive emails through Microsoft Exchange Outlook settings, that the Outlook auto-archive is not a standard feature enabled in the Windows 7/Outlook 2010 image/configuration that was installed on Mr. MacLennan's computer. In answering this question, which we understood to relate to whether emails might be saved outside of Mr. MacLennan's email account, we did not explain that the "Enterprise Vault" was configured with Microsoft Exchange, and that the Vault provided secondary storage for emails in connection with a user's email account.

The June 25th motion to MGS by the Standing Committee on Justice Policy

As you are aware, the Justice Policy Committee passed a motion requiring MGS to produce email records relating to the cancellation and relocation of the Oakville and Mississauga gas plants, sent or received by 13 named individuals, including records stored on OPS RAID servers. In order to respond to the motion, a Ministry team was established, including staff in the MGS corporate security branch, staff in our ITS Division who administer our networks, and ministry counsel.

The Corporate Security Branch (CSB) (staff who safeguard our network from threats) was asked to assist in this search because they are routinely used to conduct electronic searches for documents required for production in large litigation files and related matters for the government. When undertaking electronic searches, CSB staff work with ITS staff to obtain copies of relevant email accounts and folders stored on our network from ITS staff, and then run "search terms" to obtain documents that may be responsive to a request. We describe this search for records as a "forensic" search because it is undertaken centrally into an individual user's accounts.

After receiving the motion, the team met to coordinate and map out the search process. They planned out the search in three stages: email accounts would be searched first, then the network folders assigned to the individuals, and finally assessments were made about the potential to retrieve information from back-up tapes.

Staff discussed with counsel that the Microsoft Exchange (primary storage) and Enterprise Vault (secondary storage) portions of email accounts are maintained on separate server systems and back-up systems. The Microsoft Exchange portion of email accounts is recorded on back-up tapes that could be potentially accessed to respond to the Committee motion.

Counsel requested that the team first locate and search the email accounts of the individuals named in the motion. ITS staff were also asked to check whether any decommissioned email accounts assigned to the individuals had both the primary and secondary storage components deleted, given that email accounts are maintained on two separate systems. ITS staff undertook a search of the Enterprise Vault server and a portion of the email account of Mr. Craig MacLennan, which was decommissioned in September of 2012, was identified.

In this regard, the MS Exchange portion of his account had been deleted, the secondary storage Vault had not. Following an OPS-wide refresh of the email system, a review of operational practices was undertaken by OPS ITS staff from December 2012-January 2013. As a result of the review in February of 2013, ITS strengthened the email account management procedures including a new protocol to address the occurrence of undeleted Vaults.

Back-up Tapes

As part of our assessment of the availability of back-up tapes to respond to the Justice Policy Committee motion, staff also reviewed our existing inventory of back-up tapes in relation to the named individuals from the time of the motion backwards. This included a review of tapes held at our storage service provider Iron Mountain. Iron Mountain has been our service provider for the last ten years.

In the course of this review, we identified that we have back-up tapes in storage that extend beyond the normal one-year retention period. Our answer to your question about the existence of back-up tapes during the relevant time period was based on our existing retention protocol, in which monthly back-up tapes (for most ministries), are to be held for one year and then overwritten. In answering this question IT staff advised that email back-ups are written to tape on the last Friday of the month and held for one year. After that year, the tape would be put back into the OPS tape library pool and over-written many times.

The existence of additional back-up tapes in our inventory is attributable to some exceptional circumstances. In July of 2012 we started a refresh of our email system; we moved from Microsoft Exchange 2003 to Microsoft Exchange 2010. As part of the change process in November of 2012, IT staff maintained the previous year's monthly back-up tapes made on our old email system. This has resulted in the retention of more back-up tapes than we had first realized when we responded to your question about whether back-up tapes exist during the relevant time period.

Accordingly, in the case of Mr. MacLennan (employed in the Ministry of Energy during the relevant time period of your request --September 2010 to December 2011), we have identified one back-up tape kept as part of this change management process that was made in December, 2011. We also have monthly back-up tapes for the year 2012 for the Ministry of Energy.

In addition, because of the changeover in our email system, IT staff have identified that we may have an additional three months of back-up tapes for the Premier's office in 2012. While daily back-up tapes for the Premier's office were normally only maintained for ten days, as per that Office's retention protocol, at the time the email system was changed for the Premier's office, the new system kept back-up tapes on a monthly basis for a three month cycle. Subsequently, the existing ten-day daily back-up retention protocol was applied.

We have also discovered that we may have certain daily back-up tapes for Mr. Bentley, former Minister of Energy. His email account was transferred from the Ministry of the Attorney General (MAG) when he became the Minister of Energy in the Fall of 2011. MAG has a longer back-up tape retention protocol than do other ministries. The MAG retention protocol attached to Mr. Bentley's account continued while he was at the Ministry of Energy. We are currently assessing what may be available on back-up tape and will report back to the Justice Policy Committee as information becomes available.

In your letter you have asked us to explain why we did not disclose the Enterprise Vault and asked us to explain the approach we took to responding to the motion and why that differed from your investigation. In retrospect, we have discussed this matter and believe that we could have better supported your investigation by offering your staff further briefings of our electronic records management systems, led by subject matter experts, and walked your staff through our email and records management systems from end to end. In this manner we could also have better explained our systems, including the architecture and function of the primary and secondary storage components of our email accounts. In our first meeting in April, the Executive Lead mentioned to one of your staff that our MS Exchange was supported by a product called Symantec (name of software developer) to manage user email boxes, in response to his question about whether our MS Exchange was configured with auto-archiver. This is our Enterprise Vault program. However, the use of the term Symantec, and the very brief nature of this conversation would not have given your staff member sufficient information to understand how this program works to provide secondary storage on OPS email accounts.

In addition, our work on the motion demonstrated that we had a number of exceptions to our normal protocols and practices. In this regard, our initial approach to your investigation should have included walking through our processes and identifying these exceptions to your staff.

In closing I would like to remark that my staff undertook to provide helpful assistance to your office during your investigation. It is important to assure you that we did not intend to take your investigation less seriously than the Justice Policy Committee motion. We value the collaborative relationship we have with your office and I sincerely apologize for our mistake and its impact on your investigation. We would welcome the opportunity to meet with you again to discuss this matter further including a briefing on the records located as part of our search. In addition, we could discuss the attached technical briefing document we recently prepared to assist in our communications with your office and the Chair of the Justice Policy Committee.

Sincerely,



Kevin Costante
Deputy Minister, Ministry of Government Services
Associate Secretary of the Cabinet and
Secretary of Management Board of Cabinet

c: Mr. Peter Wallace, Secretary of the Cabinet
Mr. David Nicholl, Corporate Chief Information Officer, Ministry of Government Services
Mr. Don Fawcett, Crown Counsel, Ministry of Government Services

Attachment:
Technical briefing document

Appendix 3



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

VIA COURIER

July 23, 2013

Mr. Kevin Costante
Deputy Minister, Ministry of Government Services
Associate Secretary of Cabinet and
Secretary of Management Board of Cabinet
99 Wellesley Street West
Room 5320, Whitney Block
Toronto ON M7A 1A1

Dear Deputy Minister Costante:

RE: Deleting Accountability: Records Management Practices of Political Staff

Thank you for your letter of July 22, 2013. While I am pleased that MGS has taken marginal responsibility for the inaccurate and incomplete information provided to my office, I am disappointed with the number of inconsistencies in your letter and, MGS' overall failure to take full responsibility for the misinformation provided to my office.

You stated in your letter that in order to respond to the June 25, 2013 motion of the Justice Policy Committee, requiring that MGS produce all email records relating to the cancellation of the gas plants, MGS asked its Corporate Security Branch (CSB) to assist in the search. This was done because "they are routinely used to conduct electronic searches for documents." You also stated that after receiving the Justice Policy Committee motion, the MGS search team met to coordinate and map out the search process – the team was asked to "check whether any decommissioned email accounts assigned to the individuals had both the primary and secondary storage components deleted." What you have not stated is why this team did not conduct the exact same search during the course of my investigation? As an Officer of the Legislature, I would expect the highest degree of cooperation and diligence. After my office specifically asked how one would recover Mr. MacLennan's "deleted emails" from his email account, how is it possible that there would be no examination of his decommissioned email account? There is no valid reason why the CSB search team was not asked to verify that all relevant email accounts had indeed been decommissioned.

You stated in your letter that in response to the Justice Policy Committee motion, "staff also reviewed our existing inventory of back-up tapes in relation to the named individuals from the time of the motion backwards." As a result of this review, several back-up tapes were then found. What your letter fails to mention is why your staff did not review the existing inventory of back-up tapes in response to my office **specifically** having asked for confirmation that no back-up tapes existed from the relevant time period. How can this possibly be justified?

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7639
www.ipc.on.ca

- 2 -

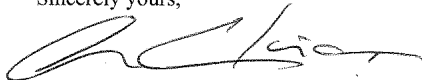
You stated that MGS staff could have better supported my investigation by offering my staff "further briefings of our electronic records management systems." On this, we agree. You also stated, in relation to our first meeting in April 2013, that the MGS Executive Lead had mentioned to one of my staff that MGS' "MS Exchange was supported by a product called Symantec (name of software developer) to manage user email boxes." This is fiction – it is simply not true – there was no mention of this to my staff.

Your letter also indicates that Symantec is the MGS "Enterprise Vault" program and that your Executive Lead's use of the term "Symantec" would not have given my staff member "sufficient information to understand how this program works to provide secondary storage on OPS email accounts." Again, the term "Symantec" was never used or conveyed to my staff. This is a detail that would have been clearly noted (and I assure you, comprehensive notes were taken throughout). Moreover, your letter fails to acknowledge that my staff **did** ask the MGS Executive Lead whether any archiving solutions existed for the MGS email system, and also what recovery options were available to users who had accidentally deleted an email. At no time did your Executive Lead mention the words "Symantec" or "Enterprise Vault" to my staff.

Finally, you stated that following a review of the OPS email system in February 2013, MGS ITS "strengthened the email account management procedures including a new protocol to address the occurrence of undeleted Vaults." I find this statement to be particularly surprising since your staff **repeatedly** stated that they had never heard of a vault not being deleted when the MS Exchange portion of the account had been deleted, in two meetings held between our offices in July 2013. How can this be? It appears from this statement that your staff did indeed have prior knowledge of vaults, on occasion, not being properly deleted.

While I value the collaborative relationship our offices have shared in the past, it is for this reason that I am dismayed at the lack of information provided to my office during the course of my investigation. MGS did not inform my office of the following essential pieces of information: (1) no one advised us of the existence of the Enterprise Vault; (2) no one verified the existence of undeleted vault accounts; and (3) no one reviewed the existing inventory of back-up tapes. Yet in response to the Justice Policy Committee motion, thousands of relevant emails and several back-up tapes somehow managed to be found. I find it very difficult to accept the fact that your office took my investigation seriously – certainly not as seriously as the Justice Policy Committee motion. Clearly, they did not.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

c: Mr. Dave Nicholl, Corporate Chief Information & Information Technology Officer
Mr. Don Fawcett, Senior Counsel, Ministry of Government Services
Mr. Peter Wallace, Secretary of the Cabinet

Appendix 4

Ministry of Government Services

Deputy Minister, Government Services
and Associate Secretary of the Cabinet,
Secretary of Management Board
of Cabinet

99 Wellesley Street West
Room 5320, Whitney Block
Toronto ON M7A 1A1
Tel.: 416-325-1607
Fax: 416-325-1612

Ministère des Services gouvernementaux

Sous-ministre, Services gouvernementaux
et secrétaire associé du Conseil des ministres,
Secrétaire du Conseil de gestion
du gouvernement

99, rue Wellesley Ouest
Édifice Whitney, bureau 5320
Toronto (Ontario) M7A 1A1
Tél. : 416 325-1607
Télééc.: 416 325-1612



July 24, 2013

Ms. Ann Cavoukian, Ph.D.
Commissioner
Information and Privacy Commission of Ontario
2 Bloor Street East
Suite 1400
Toronto, ON
M4W 1A8

Dear Commissioner Cavoukian:

I regret that my letter of July 22 left you with the impression that the Ministry of Government Services (MGS) took only marginal responsibility for the information provided to your office during your investigation.

My intention was to provide as much information as possible on the process followed by the ministry during your investigation and following passage of the Committee's motion.

I fully acknowledge that steps were taken in responding to the Committee's motion that also should have been taken in responding to the requests from your office.

I accept this is fully the responsibility of MGS and my staff and I sincerely apologize for the impact this had on your investigation and report.

As I have indicated, I would be pleased to meet with you and your staff to discuss what took place with a view to ensuring this does not occur in the future.

Sincerely,

Kevin Costante
Deputy Minister, Ministry of Government Services
Associate Secretary of the Cabinet and
Secretary of Management Board of Cabinet

c: Mr. Peter Wallace, Secretary of the Cabinet
Mr. David Nicholl, Corporate Chief Information Officer, Ministry of Government Services
Mr. Don Fawcett, Crown Counsel, Ministry of Government Services

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8

Canada

416-326-3333 1-800-387-0073

Fax: 416-325-9195

TTY (Teletypewriter): 416-325-7539

Web site: www.ipc.on.ca

Email: info@ipc.on.ca



**Information and Privacy Commissioner
Ontario, Canada**

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-326-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca