Information Commissioner of Canada
Commissaire à l'information du Canada

# ACCESS TO INFORMATION AT RISK FROM INSTANT MESSAGING

Special report to Parliament
by Suzanne Legault
Information Commissioner of Canada
November 2013

November 2013

The Honourable Noël A. Kinsella
Speaker of the Senate
Ottawa ON  K1A 0A4

Dear Mr. Speaker:

I have the honour to submit to Parliament, pursuant to section 39 of the *Access to Information Act,* a special report entitled, *Access to information at risk from instant messaging*.

Yours sincerely,

Suzanne Legault
Information Commissioner of Canada

November 2013

The Honourable Andrew Scheer, M.P.
Speaker of the House of Commons
Ottawa ON  K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament, pursuant to section 39 of the *Access to Information Act,* a special report entitled, *Access to information at risk from instant messaging*.

Yours sincerely,

Suzanne Legault
Information Commissioner of Canada

# Contents

## Message from the Commissioner

Technology and its use in government are evolving rapidly. Thousands of federal employees use wireless devices to send and receive instant messages every day. This includes communications to and from BlackBerrys using unique personal identification numbers (PINs). Government policies on the use and retention of such messages are unclear, and internal rules vary widely from institution to institution.

My investigation into the use of wireless devices and instant messaging in 11 federal institutions revealed that there is a real risk that information that should be accessible by requesters is being irremediably deleted or lost. No valid operational requirement was provided to me to justify this risk.

Complaints to my office about missing records have increased substantially in the past two years. However, unless instant messages are actively saved, they will be automatically deleted from wireless devices after a short period and no longer exist or be recoverable by the time my office receives a complaint. For all practical purposes, this negates my ability to investigate the very existence of these records.

Proposed Treasury Board Secretariat policies to address the use of new wireless technology and instant messaging will likely exacerbate the risk that government information, one of our national resources, will be lost.

In light of this, I called on the President of the Treasury Board to review the use of instant messaging, including PINs, across the federal government. His response did not address issues raised by my office, but focussed instead on training and employees' obligations under existing and proposed policy instruments.

I also repeat my call to Parliament to include in the *Access to Information Act* a comprehensive legal duty to document decisions made by government with appropriate sanctions for non-compliance.

Information is the lifeblood of democracy. Loss of information or an infringement on requesters' right of access should not be quietly accepted simply because the impact of new technologies has not been properly considered. While technology is a powerful tool for innovation, its use must not infringe on the right of requesters to know what government is doing and to hold it accountable for its decisions.

## Executive summary

In this investigation, the Office of the Information Commissioner reviewed the practices of 11 institutions and various ministerial offices with regard to the use of instant text-based messages on wireless devices, including communications to and from BlackBerrys using their unique personal identification numbers (PINs). We concluded that these practices, along with the training provided to wireless users, were widely divergent.

Our investigation revealed that instant messaging was enabled in all 11 institutions and the various ministerial offices. We also learned that, with few exceptions, these messages, unlike emails, were not automatically stored on a corporate email server. Even though it was possible to store instant messages sent via BlackBerry by actively enabling a function using the BlackBerry Enterprise Server software, only two of the institutions had taken that step and only one stored all types of instant messages. In the other nine institutions, the retrieval of such messages in the case of deletion or loss was practically impossible, since they were not stored on a central server. This has been particularly problematic for our investigations into missing record complaints, which have increased noticeably in the past two years.

The likelihood that instant messages could or would be retrieved in ministerial offices was almost non-existent as a result of guidance from the Treasury Board Secretariat (TBS), the administrator of the access to information system and the organization responsible for information management policy. This guidance instructs access officials within government institutions to only ask these offices for records when officials have reasonable grounds to believe, based on credible evidence, that records determined to be under the control of the institution would be found.

We have concerns that the absence of any TBS policy instrument that requires instant messages to be preserved for a reasonable period does not adequately safeguard the right of access under the *Access to Information Act*. Reliance on the goodwill of individual public servants and ministerial staff to identify, save and store records of business value is insufficient to address the risk that information that should be subject to the Act will be lost without a means of being recovered or retrieved.

When questioned about the operational need for enabling instant messaging, despite the security risks and the risks to access to information rights, institutions said that it is necessary because instant messaging is faster than email, reduces roaming charges when employees are outside of Canada and serves as an alternative method of communication during urgent situations when institutional servers are not working. In our view, these reasons do not outweigh the risks that information that should be subject to the right of access is being irretrievably destroyed or lost.

As a result of our investigation, we recommended that TBS develop and implement a government-wide policy that instructs institutions to disable instant messaging, including PIN-to-PIN communication, on all government-issued wireless devices, except for when five specific and operationally grounded conditions are met. The President of the Treasury Board has not agreed to follow this recommendation.

We also recommended that TBS revise its guidance on the tasking of ministerial offices to require that tasking occur without delay when records of potential relevance to an access request might exist in those offices or on a wireless device used by a member of a ministerial office's staff. Despite our recommendation, however, TBS continues to maintain that an institution must have reasonable grounds to believe, based on credible evidence, that responsive records exist in a ministerial office before that tasking is done.

We have reiterated all our recommendations to TBS in this report, since these have yet to be adequately addressed.

The report also recommends that Parliament amend the *Access to Information Act* to include a comprehensive legal duty to document decisions made by federal government officials with appropriate sanctions for non-compliance. This would ensure that records documenting public policy decisions and how they were made are created and preserved for access purposes and to promote accountability.

# Introduction

In August 2012, the Information Commissioner launched a systemic investigation into the use and preservation of non-email, text-based messages on government-issued wireless devices. The decision to launch this investigation was, in part, the result of a complaint against Indian and Northern Affairs Canada (now Aboriginal Affairs and Northern Development Canada). In that case, the complainant had received an email in which one government official asked another to use a "pin" instead of email to communicate.[1] When we investigated the complaint, we were informed that, prior to receiving the request for information, the relevant BlackBerrys had been replaced and subsequently destroyed. Thus, any information that might have existed and fallen within the scope of the access request was permanently lost.

Based on this complaint, as well as an increasing number of complaints related to missing records and "pins," the Commissioner determined that there were reasonable grounds to self-initiate a complaint in order to investigate the impact of instant messaging, including PINs, on the right of access to information in Canada. The investigation focused on 11 institutions:

- Aboriginal Affairs and Northern Development Canada (AANDC)
- Department of Justice Canada
- Foreign Affairs and International Trade Canada (now known as Foreign Affairs, Trade and Development Canada; DFATD)
- Health Canada
- Industry Canada
- Library and Archives Canada (LAC)
- National Defence
- Privy Council Office (PCO)
- Public Works and Government Services Canada (PWGSC)
- Transport Canada
- Treasury Board of Canada Secretariat (TBS).

We also sought information from the offices of the head of some of these institutions (ministerial offices).[2] This is because records held in those offices may be subject to the *Access to Information Act*.[3] Finally, we added Shared Services Canada to the investigation in March 2013, due to its role in providing wireless and information technology infrastructure services to institutions and ministerial offices.

---

[1] "Pin" stands for "personal identification number." PIN-to-PIN communications are non-email text-based messages sent and received using the unique eight-digit BlackBerry PIN. These and other similar types of message, such as those sent and received via BlackBerry Messenger and Short Messaging Service (SMS), are considered "instant messages" in this report. We also use that term and "PIN-to-PIN" or "PINs" interchangeably.

[2] Offices of the ministers of Aboriginal Affairs and Northern Development, Foreign Affairs, International Trade, Health, Industry, Defence, Public Works and Government Services and Transport, along with the offices of the Minister of Justice and Attorney General of Canada, and the President of the Treasury Board, and the Prime Minister's Office. We did not survey the Minister of Canadian Heritage and Official Languages, however. While Library and Archives Canada reports to Parliament through this Minister, staff in the Minister's office are not involved in the institution's daily operations.

[3] The Supreme Court of Canada ruled in May 2011 that agendas, notes and emails related to the activities of a former prime minister and two Cabinet ministers did not have to be disclosed in response to an access request. However, the Court specified that records held in ministerial offices are under a government institution's control when a) they relate to an institutional matter and b) a senior official in a government institution should reasonably be expected to be able to obtain a copy of them upon request. (*Canada (Information Commissioner) v Canada (Minister of National Defence) et al.,* 2011 SCC 25)

We gathered a significant amount of information through questionnaires given to the 12 institutions and the various ministerial offices. We then prepared preliminary observations and findings and shared these with TBS, which in turn provided written representations on our observations and findings. In September 2013, we provided the President of the Treasury Board with a report on the findings of our investigation and made specific recommendations. On October 9, 2013, we received a response from the President of the Treasury Board (see Appendix A). Since he did not agree to follow all of our recommendations, we consider the complaint in this systemic investigation to be unresolved.

## Context

The *Access to Information Act* provides a quasi-constitutional right of access to records that are under the control of a government institution at the time it receives an access to information request.[4] In certain instances, the right of access is also protected by section 2(b) of the *Canadian Charter of Rights and Freedoms*, which guarantees the right to freedom of expression.

The Supreme Court of Canada has described the underlying purpose of the Act as facilitating democracy by ensuring that citizens have the information they need to participate meaningfully in the democratic process, and that politicians and bureaucrats remain accountable to them.[5] The purpose of the Act has also been linked to that of the *Library and Archives of Canada Act*. Both laws recognize government information as a resource of national value.[6]

Information management at the federal level is governed by Treasury Board's suite of information policies, and associated TBS directives and guidelines. These tools refer to the principles of preserving and ensuring access to information and records for the benefit of current and future generations and require institutions to implement efficient and effective information management practices to support program and service delivery.[7] The policy instruments emphasize institutions' responsibility for creating, acquiring, capturing, managing and protecting the integrity of information resources of business value. Individual employees, in turn, are responsible for ensuring that decisions and decision-making processes are documented and that all information of business value is captured in an appropriate corporate repository for government information.

[4] On the quasi-constitutional nature of the right of access, see, for example, *Statham v Canadian Broadcasting Corporation*, 2010 FCA 315, and *Canada (Information Commissioner) v Canada (Minister of National Defence) et al*., 2011 SCC 25, para. 79.

[5] See *Dagg v Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, para. 61.

[6] See *Bronskill v Canada (Minister of Heritage)* 2011 FC 991, paras. 16–22.

[7] The Policy on Information Management (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12742) and the TBS Directive on Information Management Roles and Responsibilities (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12754) refer to the *Access to Information Act* under the heading "Relevant Legislation." The TBS Directive on Recordkeeping (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16552) provides in section 3.5 that recordkeeping is carried out in accordance with the *Access to Information Act*, the *Financial Administration Act* and *Library and Archives of Canada Act*.

The *Access to Information Act* defines records subject to the right of access as "any documentary material, regardless of medium or form." It is important to note that although records may be of business value or transitory in nature (see box, right), *any* record under the control of an institution at the time it receives a request must be retrieved, processed for access purposes and preserved.

Both Communications Security Establishment Canada and the Privacy Commissioner have previously reported on the security vulnerabilities associated with the use of instant messaging.[8] Despite these concerns, approximately 98,000 BlackBerrys have been issued to government institutions (as of August 2013, as per Shared Services Canada). Most are enabled to send instant messages, which, in turn, are not generally stored on corporate servers.

**Know your records**
"Records of business value" are those that record or communicate business decisions and support ongoing operations.

"Transitory records" include those created to complete a routine action.[1]

All records of business value must be saved in a repository such as a corporate email server. Transitory electronic records may normally be deleted immediately.[2] However, if they exist when an institution receives an access request then they must be reviewed to determine whether they fall within the scope of the request.

1. Transitory records are defined in Section 2.1.4 of LAC's Multi-Institutional Disposition Authorities (MIDA, 1990; http://www.collectionscanada.gc.ca/government/disposition/007007-1008-e.html).
2. MIDA, Section 2.5.

## Use of instant messaging

As part of our investigation, we sent each institution and ministerial office a questionnaire about the use of wireless devices and instant messaging. All of the institutions and ministerial offices responded to the questionnaire. Their responses illustrate widely divergent use of instant messaging. We also reviewed internal policies, procedures and practices on information management, and the use of wireless devices and instant messaging, including PINs, in both settings.

### Institutional practices

The following table summarizes whether instant messaging is enabled for all users, whether institutional policy allows users to send information of business value by instant message and whether instant messages are automatically stored on a corporate server for each of the institutions surveyed.

[8] Communications Security Establishment Canada 2011 bulletin, *Security of BlackBerry PIN to PIN Messaging*; Privacy Commissioner 2010 audit report, *The Protection of Personal Information in Wireless Environments: An Examination of Selected Federal Institutions*.

| | Is instant messaging enabled for all users? | Are wireless users permitted by policy or other measures to send information of business value via instant messaging? | Are instant messages automatically stored on a corporate server? |
|---|---|---|---|
| AANDC | Yes | No | No |
| Department of Justice Canada | Yes, but different functions for different users | Yes | No |
| DFATD | Yes | Yes | Yes* |
| Health Canada | Yes | No | No |
| Industry Canada | Yes | Yes | No |
| LAC | Yes | No | No |
| National Defence | Yes, but different functions for different users | Yes | SMS: Yes<br>PIN-to-PIN: No |
| PWGSC | Yes | Yes | No |
| PCO | Yes | Yes | No |
| Transport Canada | Yes, but different functions for different users | Yes | No |
| TBS | Yes, but different functions for different users | Yes | No |

* All messages sent via BlackBerry Messenger, PIN-to-PIN and Short Messaging Service (SMS) are stored for audits and forensic investigations but not for information management purposes.

We also learned the following:

- The BlackBerry is the primary wireless device used by federal institutions.
- All of the institutions surveyed use BlackBerry Enterprise Server software to connect their wireless devices to their corporate email servers. Only two of the institutions enabled this software to automatically store some or all PINs and other BlackBerry-generated instant messages.
- Instant messages are automatically deleted from wireless devices, usually after 30 days.
- In response to our questionnaire, only AANDC told us that it has a formal procedure for backing up and restoring instant messages when upgrading or troubleshooting wireless devices. Transport Canada said it has procedures employees must follow to preserve business-related messages when returning wireless devices.
- None of the institutions has employed a technical means to ensure instant messages are preserved when wireless devices are disposed of or deactivated. Instead individual users determine whether messages are of business value and then store them in a corporate repository. PCO explained that Shared Services Canada, as the provider of wireless devices, is responsible for reformatting, cleaning, deactivating and disposing of wireless devices.
- AANDC, Health Canada, LAC and National Defence require wireless users to sign an agreement under which they must abide by policies on device use. However, only National Defence's agreement makes explicit reference to instant messaging.[9]

[9] National Defence also has users sign an awareness form before instant messaging is activated to acknowledge that there is no daily backup of PIN-to-PIN messages and, as such, that they will not be retrievable once they are deleted.

### Ministerial offices

The questionnaire responses from ministerial offices were not as clear as those received from institutions.[10]

With one exception, ministerial offices enabled all instant messaging functions on all wireless users' government-issued devices. Different functions were enabled for different users in the office of the Minister of Justice and Attorney General of Canada.

Most offices did not state categorically that they allowed information of business value to be communicated via PINs. We did learn, however, that wireless users in the office of the Minister of Public Works and Government Services were expressly allowed to use instant messaging for these purposes, while their counterparts in the Minister of Aboriginal Affairs and Northern Development's office were not. We were told that ministerial staff working in the offices of the ministers of Foreign Affairs and of International Trade were expected to abide by institutional policy, which permits the use of instant messaging for non-transitory communications.

Instant messages sent and received by staff in the offices of the ministers of Justice and Attorney General of Canada, Health and Public Works and Government Services were not automatically stored on a corporate server. The office of the Minister of Defence stored SMS messages but not PIN-to-PIN communications. Otherwise, it was not clear whether the other institutions backed up instant messages on a central server.

We learned through the questionnaire responses that the majority of ministerial offices do not require staff, upon receiving a wireless device, to sign a written agreement acknowledging their information management responsibilities for the messages they send and receive.

## Findings

Our investigation sought to answer two main questions: Does the use of instant messaging, including PINs, pose a risk to the rights of requesters to receive information under the *Access to Information Act*? Is there any operational requirement that would justify taking such a risk?

We reached two main conclusions. First, the current use of instant messaging presents an unacceptable risk to the right of access to information in Canada. Second, the operational requirements identified by government institutions do not explain or justify the risk created by the use of instant messaging.

[10] The ministerial office questionnaire differed from the institutional questionnaire. The former asked whether the ministerial office shared the same wireless infrastructure as the institution and, if not, how the office's use of text-based messaging differed from the institution's. Many ministerial offices responded that they share the institution's infrastructure but did not explicitly state how their office's functions differed. Some answers were implied and others provided limited information.

## Instant messaging presents an unacceptable risk to the right of access to information

Based on the information obtained and reviewed during the investigation, we concluded that the absence of a technical safeguard, the gaps in existing policies, the proposed policies to address the use of instant messaging, and the impact of instant messaging on the ability of our office to investigate missing record complaints all pose unacceptable risks to the right of access to information.

### The absence of a technical safeguard leaves no margin for error or delay

Instant messages are not actively stored on institutional email servers. Although it is possible to store copies of instant messages, institutions must take active steps to enable this function using the Business Enterprise Server (BES) software that connects wireless devices with corporate email systems. Otherwise, wireless devices automatically delete instant messages after a set period of time, usually 30 days. Accordingly, unless an institution has enabled its BES to store instant messages, or an individual user has transferred instant messages into a corporate repository, these communications are not stored anywhere other than the wireless device and cannot generally be recovered once they have been deleted.

Reliance on individual employees to preserve and transfer information either of business value or that falls within the scope of an access request is an insufficient safeguard of the right of access. Human error or other circumstances such as a heavy workload or illness may prevent a wireless user from ensuring that instant messages of business value are identified and then saved in a corporate repository, prior to being auto-deleted.

Wireless users may not receive or act on requests for records from access officials before the automatic deletion occurs. Thus, instant messages that are not of business value, but are in existence at the time an access request is received by the institution, are at great risk of permanent deletion, unless access to information officials ask for records immediately upon receiving a request and employees act on that tasking without delay.

In the case of wireless devices of ministerial office staff, the risk that PINs will be deleted was heightened by the April 22, 2013, version of TBS' *Implementation Report No. 115: Access to Records in a Minister's Office—Prime Minister's Agenda case*.[11] This report expressly instructed access to information officials to *delay* asking ministerial offices for records that may be relevant to a request until after collecting all or most of the records from within the institution. Since instant messages are usually deleted from wireless devices after a month, this delay may well result in information that would fall within the scope of an access request being permanently deleted.

### Inconsistent policies and guidance do not sufficiently address the risk to access

The investigation demonstrated that there is considerable variation in institutions' internal policies, guidelines and procedures governing the use of wireless devices, including instant messaging.

[11] During the investigation, TBS proposed amendments to this document. See page 14.

| | Draft policies and guidelines in place | Provide some direction to wireless users about information management and preservation of instant messages | Rely on general policies that refer to information management |
|---|---|---|---|
| AANDC | ✓ | ✓ | |
| Department of Justice Canada | | ✓ | |
| DFATD | | ✓ | |
| Health Canada | ✓ | ✓ | |
| Industry Canada | ✓* | | ✓** |
| LAC | | ✓ | |
| National Defence | ✓ | ✓ | |
| PCO | | ✓ | |
| PWGSC | | ✓ | |
| Transport Canada | | ✓ | |
| TBS | | | ✓** |

* Industry Canada reported that it is waiting for guidance from TBS on the use, management and preservation of instant messages prior to formalizing its policies.
** However, in both these institutions, the policies speak to security-related issues not information management practices for text messages.

Ministerial offices are, in accordance with TBS's 2011 *Policies for Ministers' Offices*, bound by TBS policies and regulations. Ministerial offices are also bound by PCO's 2011 *Accountable Government: A Guide for Ministers and Ministers of State*. All ministerial offices indicated that they follow one or both of these policy instruments. Neither of these documents specifically addresses the records management challenges associated with the use of instant messaging.

Only some of the ministerial offices surveyed indicated that they abide by more specific policy instruments developed or implemented in their respective institutions. Some reported that they receive a copy of institutions' information management guidelines or rules (ministerial offices at AANDC, DFATD and Health Canada). Only the office of the Minister of International Trade indicated that it adheres to the institution's policies governing the records management and use of PINs, while the office of the Minister of Aboriginal Affairs and Northern Development reported that its ministerial staff use the institution's policies as a guide.

Institutions do give some information management training to wireless users. However, there is considerable variation in the quantity and quality of that training when it comes to the use of instant messaging. Some institutions reported that their access officials explain that instant messages are "records" within the meaning of the *Access to Information Act*. In other organizations, the institution's chief information officer or departmental security officer offers awareness sessions on information management. Employees also receive web content and paper handouts regarding their information management responsibilities.

With regards to training of ministerial office staff, many offices reported that staff are given copies of *Policies for Ministers' Offices* and *Accountable Government* without further training or information. Other offices referred to training on information management responsibilities given to ministerial office staff; however, these sessions appear to have focused on the classification of information and security awareness, rather than information management of records of business value for retention, accountability or access to information purposes. Two offices also mentioned that the chief of staff is available to provide guidance on information management and security matters.

**Monitoring compliance**
During the investigation, TBS highlighted the Recordkeeping Assessment Tool (RKAT) as a way for institutions to monitor their compliance with recordkeeping requirements, including the treatment of instant messages. However, this self-assessment tool (developed by TBS and LAC) is, in our view, of little effective assistance in ensuring instant messages are available for access purposes, since using it is largely a paper exercise. The RKAT does not offer a tangible means of capturing information that would enable an audit of an institution's compliance with information management policies or the requirements of the *Access to Information Act*.

In our view, the evidence set out above speaks clearly to a need for TBS to address the gaps in the existing information management and access to information policy instruments and training. While deputy heads may be best placed to understand the internal workings of their institutions and determine who requires access to instant messaging functions, TBS must ensure that access rights in Canada are not put at risk by gaps in the current policies that allow such a wide divergence in the treatment of PINs and the training given to wireless device users.

**Proposed TBS policies heighten the risk to access rights**
During the investigation, TBS reported that it intends to implement new policy instruments on the information management of text-based messages, including instant messages.

Having examined draft versions of these documents, it is our view that they would increase, not lessen, the likelihood that instant messages responsive to access requests will be permanently deleted.

TBS's draft standard on email management, which would apply to both email and instant messaging, instructs wireless users to transfer "as soon as possible" any emails or instant messages that contain information of business value to a corporate repository. However, the draft standard then proposes very different treatment of emails and PINs.

Emails that users have proactively identified for deletion would be removed from corporate servers after 30 days. By contrast, the draft standard instructs institutions to ensure that instant messages are stored on wireless devices "for a maximum" of three days and that messages are not to be automatically backed up on a central server within that short period of time. Therefore, all instant messages would be automatically and permanently destroyed within three days, unless users took steps on their own to preserve them elsewhere than their wireless device.

TBS's draft protocol *Instant Messaging using a Mobile Device* reminds access to information officials that they should ask institutional employees to search "all records under the control of

the institution, regardless of medium or format, including instant messages sent or received over mobile devices." However, no existing or proposed policy or procedure requires access officials to initiate searches for responsive records or requires that institutional subject-matter experts respond within less than three days.

Thus, even if employees were to achieve perfect compliance with the draft standard and preserve all instant messages containing information of business value within three days, transitory instant messages in existence at the time an access request was received (and that therefore might fall within the scope of an access request) would likely be unavailable for review and possible disclosure.

Moreover, the draft protocol contains misinformation in that it states, "Any instant message that does not have business value is deemed to be transitory and can be deleted at any time." This guidance is contrary to the right of access under the *Access to Information Act*. This right is not confined to information of business value. Rather, it applies to a*ll* records in existence at the time an institution receives a request, including transitory instant messages.

The likelihood that instant messages sent or received by ministerial office staff and that might fall within the scope of an access request would be permanently destroyed is virtually assured. The draft protocol specifies that searches for records should be directed to "employees of the government institution." The fact that records located in ministerial offices could be determined to be under the institution's control, within the meaning of the *Access to Information Act*, is not mentioned.

This risk to access rights is compounded by the direction to delay asking for records from ministerial offices set out in TBS's April 2013 Implementation Report, as noted above (see page 11). In light of the proposed three-day retention of instant messages, this means that instant messages would have long been destroyed before ministerial offices were asked for them in response to an access request, much less by the time a requester might complain to our office.

We note that although the Implementation Report is said to "reflect the Supreme Court of Canada's decision" in the Prime Minister's agenda case nowhere in that decision does the Court suggest that institutions ought to delay asking ministerial offices for records until after collecting all or most records from institutional subject-matter experts. Nor does the decision support the Implementation Report's direction that access officials should only ask ministerial offices for records when they are of the view that there are "reasonable grounds," "based on credible evidence," that they will find relevant records that will be determined to be under the control of the institution. Indeed, the Supreme Court expressly stated that the phrase "under the control" is not to be interpreted in a manner that turns "a Minister's office into a 'black hole' to shelter sensitive records that should otherwise be produced to the requester in accordance with the law."[12]

In response to our report of the findings of our investigation, the President of the Treasury Board indicated that he agreed "that [access to information and privacy] coordinators may consider tasking their Ministers' office when the request is received" and provided us with an

[12] *Canada (Information Commissioner) v Canada (Minister of National Defence) et al.,* 2011 SCC 25, at para. 51.

amended Implementation Report, to be published shortly. However, it is our view that this amended guidance does not, in fact, respond to our concerns.

The Implementation Report continues to impose criteria not reflected in the Supreme Court of Canada decision. Access to information coordinators are still informed that they are to have reasonable grounds, based on credible evidence, of the existence of relevant records that would be determined to be under the institution's control before asking a ministerial office for records responsive to an access request. The report suggests that "such evidence may come from … records already obtained from the institution."

Whether a record is "under the control" of an institution hinges, in part, on the content of the record itself—that is, whether it relates to an institutional matter. It is difficult to envision how an access official could possibly determine that a record is under an institution's control without seeing the record's content. However, the Implementation Report proposes that coordinators make such a determination, supported by credible evidence, before tasking the ministerial office. The suggestion that such evidence may come from records already obtained from the institution indicates, in our view, that ministerial offices would not be immediately asked for records, thus increasing the likelihood that records that might fall within the scope of an access request would be irremediably deleted or lost.

**Current treatment of instant messaging renders independent oversight ineffective**

One final but important impact of the current treatment of instant messaging is that it limits the ability of our office to investigate complaints about missing records or no record responses.

The *Access to Information Act* creates two levels of independent review of government decisions on the disclosure of information. The Commissioner is the first. One of the frequent complaints our office receives is that institutions have not provided all the relevant records, including instances in which the institution has told the requester that "no records" exist.

Complaints about missing records totalled 45 percent of the complaints we received in 2012–2013 concerning refusals to grant access, up from 29 percent the year before.

Instant messages, including PINs, in existence at the time a request is received are records responsive to the request even if they would otherwise be considered transitory. However, unless employees considered instant messages to be of business value and stored them in a corporate repository, any messages not retrieved at the time of an access request's receipt would be unlikely to still exist by the time our office received a complaint.

**Missing records complaints registered[1]**

**2010–2011**: 398 (45% of refusal complaints)
**2011–2012**: 284 (29%)
**2012–2013**: 428 (45%)

In the first six months of 2013–2014, we registered 241 missing records complaints. This puts us on track to receive roughly 480 for the year. This would equal a 12-percent increase in missing records complaints over 2012–2013, and a 69-percent increase in just two years.

1. Prior to April 1, 2013, we only registered one complaint when asked to review the use of exemptions and determine whether additional records existed, with regard to a single access request. We now register the missing records complaint separately. This means, to be consistent across all years and more accurately reflect the number of missing record complaints we registered, the numbers cited in this box and elsewhere in this report are higher than those that appeared in our annual reports for 2010–2011, 2011–2012 and 2012–2013. (See our advisory notice here: http://www.oic-ci.gc.ca/eng/missing-records-documents-manquants.aspx.)

This negates the ability of our office to effectively investigate complaints concerning missing records. In the absence of a technical safeguard, such as storing instant messages on a server, there is no way for us to retrieve the records to confirm whether they would be subject to the request.

Accordingly, we concluded that the current use of instant messaging has and will continue to have a negative impact on requesters' right to complain to our office.

### No clear operational requirement for enabling instant messaging

Our second main conclusion is that government institutions have not identified a clear operational requirement for enabling PINs and other types of instant messaging for all wireless device users.

During our investigation, TBS expressed concern about the amount of additional information that would have to be retained and possibly searched and retrieved for access purposes if all instant messages were backed up on corporate servers. This position, however, presupposes the extensive use of instant messaging that we are of the view is unjustified, puts requesters' rights at risk and is troubling in light of the security and privacy concerns previously identified by Communications Security Establishment Canada and the Privacy Commissioner.

Institutions told us that they enable instant messaging for three reasons:

- Instant messages are transmitted more rapidly than emails.
- Using instant messaging in remote locations or overseas avoids roaming charges.
- Instant messages can be sent and received when institutional servers are unavailable. This provides officials with an additional means of communication and reporting during emergencies.

In our opinion, the first two reasons are clearly insufficient for institutions to justify an activity that puts the quasi-constitutional right of access at risk. We are not convinced that marginally quicker transmission times and avoiding roaming charges generally constitute operational requirements.

Allowing instant messaging for emergency purposes may be of sufficient operational importance to warrant careful consideration. Nonetheless, these functions should, in our view, be enabled for officials in only a small number of key positions. The resulting messages could then be automatically stored without imposing an undue information management burden.

## Conclusions

If instant messages, including PINs, were treated in the Government of Canada in the same manner as emails, many of the concerns about the impact of instant messaging on access would be addressed.[13] Instead, instant messages, for the most part, are not backed up on servers, are automatically deleted after a set period of time and are, as a result, not recoverable.

To comply with TBS policy instruments, the retention and preservation of instant messages of business value would hinge on individuals' proactively and correctly identifying these communications and forwarding them to a server. However, relying on this approach presents an unacceptable risk that government information in an institution or ministerial office will be permanently destroyed. As a result, records that might have fallen within the scope of an access to information request might not be available to be retrieved and disclosed.

In addition, no government-wide technical safeguard has been envisioned to account for human error or device malfunction, much less for the fact that the right of access under the *Access to Information Act* is not limited to records determined to have lasting business value but rather encompasses all records in existence and under an institution's control when it receives an access request. This is despite the fact that a technical safeguard is available, particularly for the most commonly used wireless device, the BlackBerry. Similarly, no system has been developed or implemented to effectively monitor the use of wireless devices to ensure that instant messages are being properly identified and preserved for access purposes.

In light of these circumstances and based on all the information we obtained and reviewed during the investigation, we concluded the following:

1. The current use of instant messaging, without any technical safeguard, presents an unacceptable risk that government information in an institution or ministerial office will be permanently deleted with no means of being recovered or retrieved.
2. Proposed or existing TBS policies, and training in institutions and ministerial offices do not adequately protect the right of access to information sent or received by instant message.
3. The enabling of instant messaging in the absence of any technical safeguard undermines the right to an effective, independent review of complaints about institutions' handling of access to information requests by our office.
4. TBS's *Implementation Report No. 115: Access to Records in a Minister's Office—Prime Minister's Agenda case* is inconsistent with the right of access and the decision of the Supreme Court of Canada in the Prime Minister's agenda case, to the extent that it instructs institutions to satisfy unnecessary criteria prior to tasking ministerial offices for records that could fall within the scope of an access request.
5. The quasi-constitutional right of access to information outweighs the supposed operational requirements for enabling instant messaging identified in the course of our investigation.

[13] This observation is based on how emails were treated at the time period covered by our investigation.

## Duty to document

During our investigation, we were told that instant messages are the equivalent of telephone conversations. In recent investigations, British Columbia's and Ontario's Information and Privacy Commissioners found that government officials were not properly documenting and preserving electronic or verbal exchanges of information.[14]

Existing federal policy instruments set out general requirements for ensuring government officials document decisions and decision-making processes.[15] However, these are not currently codified in law. The *Library and Archives Act* does speak to the retention and disposition of records but does not impose an obligation on government officials to document their decisions and how they are made. Other laws require that only certain types of records be prepared and maintained.[16] No federal statute or regulation sets out a comprehensive and enforceable legal duty to create records documenting decision-making processes, procedures or transactions.

Various federal Information Commissioners have noted that access to information has no meaning when government officials do not create records. As reported in his 1999–2000 annual report, for example, then Commissioner John Grace noted the following:

> The whole scheme of the *Access to Information Act* depends on records being created, properly indexed and filed, readily retrievable, appropriately archived and carefully assessed before destruction to ensure that valuable information is not lost. If records about particular subjects are not created, or if they cannot be readily located and produced, the right of access is meaningless. The right of access is not all that is at risk. So, too, is our ability as a nation to preserve, celebrate and learn from our history. So, too, is our government's ability to deliver good governance to the citizenry.

The following year, former Commissioner John Reid picked up the theme:

> The Government of Canada should establish a legal framework for information management which would, as a primary feature, require federal departments, agencies and institutions to create and appropriately maintain records that adequately document their organization, functions, policies, decisions, procedures, and essential transactions.

He subsequently recommended in his proposed Open Government Act that freedom of information legislation include provisions requiring the creation of records and a related offence for failure to do so with the intent to deny a right of access.[17]

---

[14] British Columbia Information and Privacy Commissioner's Investigative Report F-13-01, *Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia*, March 4, 2013; Ontario Information and Privacy Commissioner's Special Investigative Report, *Deleting Accountability: Records Management Practices of Political Staff*, June 5, 2013.

[15] TBS' *Policy on Information Management* and *Directive on Recordkeeping*, for example.

[16] The *Financial Administration Act,* for example.

[17] See the Information Commissioner's annual reports for 1993–1994, 1996–1997, and 1998–1999 to 2005–2006; special report to Parliament, *Response to the Report of the Access to Information Review Task Force*; Draft Bill, Open Government Act; *Response to the Government's Action Plan for Reform of the* Access to Information Act *(and Bill C-2)*; and evidence given before the House of Commons Standing Committee on Access to Information, Privacy and Ethics, March 9, 2009.

The current Commissioner has called for the *Access to Information Act* to be amended to include a comprehensive legal duty to document decision making, with appropriate sanctions for non-compliance. For example, in a September 2013 speech, she included the duty to document among the amendments required to modernize the Act, noting that this is particularly necessary in light of new technological developments:

> Unless a government official makes a conscious effort to record that information elsewhere, it is lost to the public. This duty to record is one of the casualties of the instant messaging environment.[18]

## Recommendation to Parliament

1. That Parliament amend the *Access to Information Act* to add a comprehensive legal duty to document decisions made by federal government institutions, with appropriate sanctions for non-compliance.

## Recommendations to the Treasury Board Secretariat

1. That TBS develop and implement a government-wide policy that instructs government institutions to disable instant messaging on all government-issued wireless devices, save for when all of the following conditions are met:

    a) There is a *bona fide* operational need that cannot be satisfied by other means that warrants enabling instant messaging on an individual user's wireless device.
    b) An adequate technical safeguard mechanism is both available and implemented to ensure that instant messages (whether or not of business value) are archived on a government server for a reasonable period of time.
    c) Individual wireless users, to whom the instant messaging function is enabled, based on a demonstrated *bona fide* operational need, do the following:

        i) undertake mandatory information management training focused on the information management risks associated with instant messaging, as well as the obligations and responsibilities imposed by the *Access to Information Act*; and
        ii) sign a terms of use agreement, under which they agree to ensure that any instant message of business value and/or that falls within the scope of an access to information request is properly identified and retrieved.

2. That TBS issue guidance requiring that ministerial offices be tasked without delay when records of potential relevance to an access request might exist in a ministerial office or on a wireless device used by a member of the ministerial office's staff.

[18] Remarks to the Canadian Legal Information Institute Conference, Ottawa, September 2013: http://www.oic-ci.gc.ca/eng/media-room-salle-media_speeches-discours_2013_5.aspx. See also the Commissioner's 2010–2011 annual report: http://www.oic-ci.gc.ca/eng/rp-pr_ar-ra_2010-2011_1.aspx.

# Appendix A: Response from the President of the Treasury Board to our recommendations

President of the Treasury Board
Ottawa, Canada  K1A 0R5

October 8, 2013

Ms. Suzanne Legault
Information Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Dear Ms. Legault:

Thank you for your letter dated September 12, 2013 regarding the results of your investigation into the management and preservation of non-email text-based messages. I have given your conclusions and recommendations careful review.

The Government of Canada is committed to openness, transparency and Canadians' right of access to government-held information. Since 2006 the Government of Canada has made unprecedented improvements to Canadians' abilities to access government information and records of all types. The 2006 *Federal Accountability Act* expanded the coverage of the *Access to Information Act* (the Act) to cover some 250 institutions, including Crown Corporations. As a result, this government has both received and responded to more ATI requests than any previous government — 43,664 in 2011–12 alone.

All employees are expected to conduct their professional activities according to the *Library and Archives of Canada Act*, the *Access to Information Act*, the *Privacy Act*, the Values and Ethics Code for the Public Sector and principles set out in Accountable Government: A Guide for Ministers and Ministers of State. I agree that mandatory training for all users of government-issued devices is important to ensure that expectations are met.

Non-email text-based messaging services such as pin-to-pin are a means of informal communication that are inherently transitory in nature. I nevertheless acknowledge that non-transitory records of business value, which are the exception in non-email text-based messaging, must be preserved, for example by being forwarded into the email system. I will therefore take steps to reinforce this obligation with all those to whom wireless devices are issued who are subject to the Act. I look forward to working with you on the appropriate language for the guidance issued to all public servants regarding their obligations.

Regarding the Treasury Board of Canada Secretariat's guidance in its *Implementation Report No. 115*, I agree that ATIP coordinators may consider tasking their Ministers' office when the request is received and when the two-step control test has been satisfied, as laid out in the Prime

Minister's Agenda Case. To that end, please find attached an amended *Implementation Report No. 115* that I intend to publish shortly.

I would like to thank you for sharing your recommendations on this matter. I take Canadians' right of access to information seriously. I will do everything in my power to ensure that all employees adhere to their responsibilities under the Act.

Yours sincerely,

[Original signed by]

The Honourable Tony Clement, P.C., M.P.

Attachment: Implementation Report 115

cc.: Ms. Yaprak Baltacioglu, Secretary, Treasury Board of Canada Secretariat
Ms. Corrine Charette, Chief Information Officer of the Government of Canada