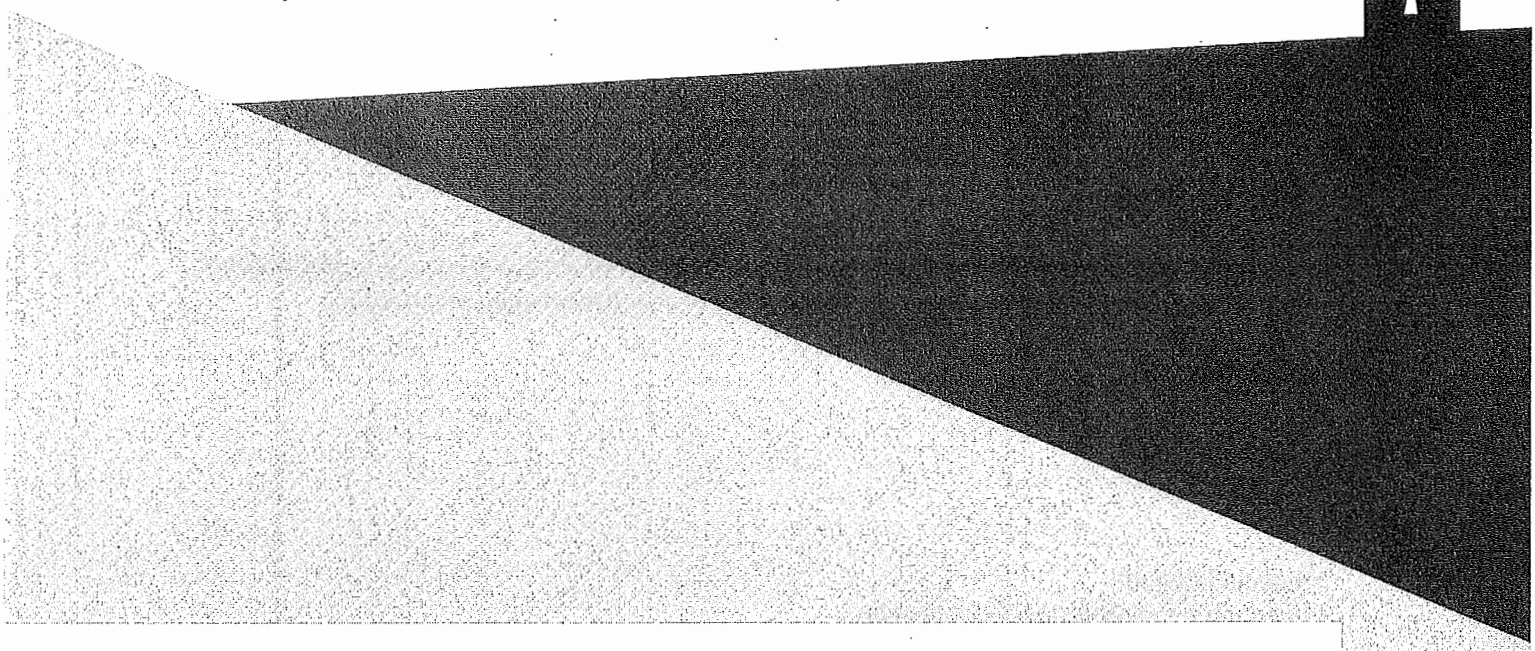
H. Bell
13.12.17
email

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

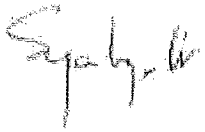
November 2013

The Honourable 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

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.

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)

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.*

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.

	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.

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 *all* 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.

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.

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.

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