AUDIT REPORT OF THE PRIVACY COMMISSIONER OF CANADA

Federal
Annual Privacy Reports

Section 72 of the *Privacy Act*

2009

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

AUDIT OF FEDERAL ANNUAL PRIVACY REPORTS

The audit work reported here was conducted in accordance with the legislative mandate, policies, and practices of the Office of the Privacy Commissioner of Canada

This report is available on our Web site at www.priv.gc.ca.

For copies of reports or other Office of the Privacy Commissioner publications, contact:

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

Telephone: (613) 995-8210, or 1-800-282-1376
Fax: (613) 947-8210
E-mail: publications@priv.gc.ca

Table of Contents

Main Points

What we examined

We looked at the extent to which federal institutions were complying with the Treasury Board Secretariat's (TBS) reporting requirements for departmental Annual Privacy Reports (APRs) to Parliament. In assessing compliance, the audit focussed on the 2006-07 APRs for the 25 federal organizations most involved with personal information, and another eight, which were randomly selected (see Appendix 1).

Why it's important

Annual Privacy Reports provide a picture of how, in delivering programs, Federal Organizations manage the personal information of Canadians. The audit was timely in the context of the *Federal Accountability Act*, which became law in December 2006. That Act expanded the scope of the *Privacy Act* and increased to 250 the number of organizations subject to it. These changes resulted in many more organizations submitting APRs, on the administration of their privacy activities under the *Privacy Act*. Therefore assurance as to the quality and usefulness of the information in these reports is warranted.

In a 2006 report on *Privacy Act* reform, the Office of the Privacy Commissioner (OPC) argued for the need to strengthen the reporting requirements of section 72 of the Act. In that report, we stated that the *Privacy Act* should ensure greater transparency, accountability and oversight over the activities of government institutions, including more stringent reporting requirements to Parliament.

What we found

All but four of the 170 organizations that were required to table an Annual Privacy Report for 2006-07 did so. Most federal institutions that this audit examined complied with most, if not all, of TBS's mandatory reporting requirements for APRs. However, many reports failed to provide anything beyond what we would call a "basic" level of information. They did not provide a clear picture of either an organization's privacy practices, or its approach to managing the risks associated with personal information it collects.

Only three of the reports that we reviewed went beyond providing only basic level information and discussed their privacy protection activities in greater detail, describing not only what measures they have implemented, but also how and why they were implemented. The enhanced reports present a much clearer picture of the organizations' privacy activities.

Federal institutions are not required to report privacy breaches in their APRs. Requiring this information would contribute to better accountability with respect to privacy activities in departments. The Commissioner has recommended that the *Privacy Act* be amended to require breach reporting.

APRs are not always readily accessible on the Web. Only 16 of 33 organizations that we examined had made their annual reports on the *Privacy Act* available on their websites. Where annual reports were posted, they were often difficult to find or out of date.

Introduction

1. The privacy challenges facing the federal government today involve—among other things— intrusive technologies, sharing and mining of data, commercial interests in personal information, and national security concerns.

2. Federal expectations concerning privacy protection are set out, in part, in Canada's *Privacy Act*. Departments and agencies are to report annually on their administration of the Act in a report, as required by section 72 of this legislation. In fulfilling their reporting obligations, departments and agencies are responsible for following requirements established by the Treasury Board Secretariat (TBS). Accordingly, effective accountability and transparency regarding how departments and agencies handle personal information in the delivery of programs is required so that Canadians may be assured their privacy is being respected.

Focus of the audit

3. The audit focussed mainly on determining the extent to which federal institutions were complying with the reporting requirements established or prescribed by the Treasury Board Secretariat.

4. Specifically, we assessed the Annual Report on the *Privacy Act* of 33 institutions (see Appendix 1) against the eight mandatory and seven optional reporting requirements set out by TBS (see Appendix 2). We focused our analysis on the 2006-07 annual reports, as not all organizations had tabled their 2007-08 reports at the time of our field work.

Observations and Recommendations

TBS works with departments to maintain and improve their privacy-management practices

5. As the designated Minister under the *Privacy Act*, the President of the Treasury Board establishes policies and guidelines for managing personal information in departments and agencies. These policies and guidelines cover a wide range of areas extending beyond core service-delivery initiatives relating to privacy.

6. Although TBS is responsible for developing privacy policies and guidelines, the day-to-day responsibility for handling personal information rests with the federal institutions that use it in delivering their programs and services. They are responsible for managing personal information, and taking early and effective action to rectify any deficiencies that have been identified.

7. TBS, in conjunction with the Office of the Privacy Commissioner, actively monitors and supports departments in addressing specific risks, vulnerabilities, control deficiencies, and other significant issues as they arise. To this end, TBS works in partnership with departments to improve their privacy management frameworks and assists in taking appropriate action where failures in privacy may occur.

8. Section 72 of the *Privacy Act* requires government institutions to submit annual reports to Parliament on the administration of the *Privacy Act*. For the reporting year 2006-07, TBS had identified a series of reporting requirements for

these reports (TBS Implementation Bulletin No. 107) that organizations were required to address (see Appendix 2). The structure and design of the reports were left to the discretion of institutions.

The majority of organizations required to do so tabled a report, and most met TBS's basic reporting requirements

9. An organization that does not table an annual report on its administration of the *Privacy Act* is in non-compliance with the Act. We found that 166 of the 170 institutions that were required to report did so. Of the four institutions that did not, two informed us that they were not aware of this reporting requirement. A third was a new organization that was not yet operational, and the fourth did not table a report because the document had not been completed on time.

10. Most institutions complied with the reporting requirements outlined in Implementation Bulletin 107 (see Appendix 2). They provided information that satisfied the Bulletin's mandatory "elements" or requirements. However, we found substantial differences in the quality and content of reporting across our audit sample.

Few reports provided a clear picture of departments' privacy activities

11. Ultimately, the practice of annual reporting should be about meaningful accountability and driving improvements in privacy practice, not just meeting basic reporting requirements. TBS requires Annual Privacy Reports to provide information that would better enable Parliament and the public to understand what an organization does with the personal information of Canadians and how it goes about managing risks to privacy. However, in many cases, these reports did not reflect this requirement.

12. Of the 33 annual reports that we examined, 27 had reported on their privacy activities in a manner which we would describe as "basic". Four reported in a manner that we would describe as "enhanced". No federal institution within our sample reported in a manner which we considered "exemplary". Two organizations, in our opinion, failed to meet the reporting requirements and were given an "incomplete" rating. Exhibit 1 summarizes ratings.

13. Those institutions which we gave a "basic" rating fulfilled most of TBS's reporting elements. However, the information they provided seldom went beyond a summary-level description of activities. These reports rarely provided substantive information on the organization's privacy practices. Nor did they present other key information such as the privacy risks associated with departmental activities.

14. For some notable exceptions and examples of more comprehensive reporting, please see Exhibit 2.

15. The two incomplete reports failed to fully respond (or at all) to at least five of the eight mandatory reporting elements. In the case of one of the organizations, its single-page submission was of particular concern, given the vast quantity of Canadians personal information that it holds. Not only did it fail to provide insight into its practices for privacy protection, it also failed to fully account for its administration of the *Privacy Act*.

16. Although the 2007-08 reports were beyond the scope of this audit, we reviewed copies of the 2007-08 reports from both organizations. They had improved sufficiently to warrant a "basic" rating.

Some institutions did not address all the mandatory reporting requirements

17. In accounting for their administration of the *Privacy Act*, government institutions were obliged to report upon the eight elements listed as "mandatory" in Appendix 2. An additional seven reporting requirements applied to institutions who had undertaken certain activities during the year. Collectively, these fifteen reporting requirements are intended both to ensure accountability for responsibilities under the Act, and to promote a broader understanding of how privacy issues are being addressed in the delivery of government programs and services.

18. In 19 of the 33 Annual Privacy Reports that we reviewed one or more mandatory items were missing. Which elements were missing varied; some omissions were of more concern than others. Items most often absent from annual reports included, but were not limited to:

- an overview of the types of disclosures made pursuant to subsections 8(2)(a) to 8(2)(m) of the *Privacy Act* during the fiscal year,
- description of Privacy Impact Assessment activities; and
- the reporting of any new data sharing of personal information among internal data banks and with other organizations.

19. Recommendation: At a minimum, TBS should ensure that institutions report on all mandatory items, so that the Annual Privacy Reports provide a picture of how, in delivering programs, the personal information of Canadians is managed.

20. Treasury Board Secretariat Response: "TBS provides annual feedback to all institutions on the quality and content of their annual reports. This feedback includes a detailed summary of the reporting requirements that were not addressed."

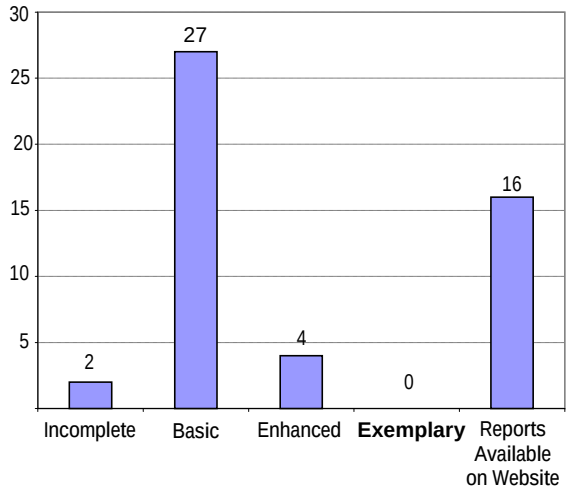
Statistics on requests for access to personal information do not show trends over time

21. Under section 12 of the *Privacy Act*, Canadian citizens and permanent residents have the right to access or request personal information about themselves contained in federal personal information banks. The Act requires that federal institutions must process requests for personal information within 30 days, though provisions exist to allow for extensions in processing time up to 60 days. (When an institution fails to respond to an individual's privacy request within legislated response times, our office may receive a complaint from that individual, which our Office logs and pursues on that person's behalf.)

Exhibit 1: Ratings of 2006-07 Annual Reports on the Administration of the *Privacy Act*

Key to the Ratings

Basic:
The institution met most, if not all, mandatory elements, and in particular, those we considered most critical. (We did not penalize an institution for failing, for example, to describe its mandate—an omission that we considered-less-than critical.



Enhanced:
The institution met all basic reporting requirements and reported on some of those elements in a manner which provided insight into its privacy practices.

Exemplary:
The institution would have to meet all basic elements and report on most in a manner which provided insight into its privacy practices, risks and issues.

Incomplete:
Entities failing to meet one or more critical and mandatory reporting element were assigned an "incomplete" rating.

22. To determine whether federal institutions are responding to individuals' requests for access to personal information in a timely manner, TBS requires each institution to provide a copy of their Statistical Report in its Annual Privacy Report in 2006-07. These statistics include information such as the number of requests from people for their personal information, and the time and cost of meeting these requests. All but one of the 33 reports that we audited provided the mandatory statistical information. As the numbers cover only the reporting period, the information does not indicate whether the organization, over time, is responding to requests in a more efficient manner or if any changes in policies or processes are making measurable differences in either the number of requests or the time to complete a request. Reporting on these trends would be a useful indicator that could allow institutions to better allocate resources.

23. Recommendation: TBS should require departments to provide multi-year statistics on access requests to personal information in their Annual Privacy Reports.

24. Treasury Board Secretariat Response: "TBS agrees that statistical trends analysis is useful and is confident the current TBS Statistics Review Project will enable the federal government to compile more meaningful data, analyze trends

and provide a comprehensive picture of its access to information and privacy program."

Some organizations went beyond providing only basic information in their reports

25. In reviewing organizations' APRs, we found several examples of good practices in privacy reporting notably by Statistics Canada, Canada Post Corporation and Correctional Services Canada. These organizations went beyond providing basic descriptions in their responses, discussing privacy matters of greater substance in a more comprehensive way. In other instances, departments reported on privacy matters such as reporting breaches, which are not required or mandated by law or policy.

Exhibit 2: Examples of enhanced practices in privacy reporting

Privacy Practices and Data Linkages • *Statistics Canada*
In its annual report on access to information and privacy, Statistics Canada clearly explained privacy practices and controls. Its reporting of privacy protocols and processes is particularly noteworthy, extending beyond the basic reporting elements mandated by TBS. For example, TBS required that institutions report only the number of new data matching and sharing activities undertaken and a short description of each. In its 2006-2007 report, Statistics Canada details all approved record-linking activities and provides the reader with insight into their purpose and the controls it has in place to ensure that personal information is protected.

Description of Privacy Program and Issue Resolution • *Canada Post Corporation*
The Canada Post annual report stated that privacy protection is an essential element of its business operations. It provided highlights of privacy related initiatives undertaken and those initiatives planned for the year ahead. In describing the Corporation's privacy program, Canada Post focused on privacy roles and responsibilities, awareness and training programs, and the risk mitigation activities that allow it to fulfill its responsibilities under the *Privacy Act* and to the public. Canada Post also discussed, in detail, privacy issues identified during the year and how they responded to them.

Privacy Breach Disclosures • *Correctional Service of Canada*
We noted that in its 2005-2006 annual report, Correctional Service of Canada identified the management practices and protocols it had implemented to handle breaches in the security and confidentiality of personal information under its control. The Department also disclosed the number of privacy breaches reported, acknowledging that corrective measures had been taken to prevent such breaches from recurring. This practice is exemplary, given that there is currently no mandatory reporting requirement for privacy breaches in the Treasury Board implementation guidance or under the *Privacy Act*.

It is not mandatory to report privacy breaches

26. TBS has developed guidance on privacy breaches (Guidelines for Privacy Breaches - 2007) for use by federal departments. It should be noted that federal

institutions are not required to report privacy breaches in their annual reports. But, through the monitoring and reporting on breaches of the personal information in their Annual Privacy Reports, federal institutions will be more informed and in a better position to manage and prevent future breaches from occurring. The Commissioner has recommended that the *Privacy Act* be amended to include breach reporting.

27. Recommendation: TBS should require departments to report privacy breaches and the steps taken to avoid future breaches in their Annual Privacy Reports.

28. Treasury Board Secretariat Response: **"**TBS will examine the question of privacy breach reporting in the context of its ongoing review of privacy policy instruments under the *Privacy Act*. TBS is currently seeking to reinforce the 2006 'Guidelines on Privacy Breaches' with additional policy requirements directed at ensuring that privacy practices of government institutions protect the personal information of individuals and that, in event of a breach, institutions have in place an action plan for addressing privacy breaches including procedures for notification of affected individuals and the OPC."

Annual Privacy Reports are not readily accessible to the public

29. For Annual Privacy Reports to be effective instruments of accountability, they must be publicly available. We found that only half the organizations (16 of 33) had made their annual reports on the *Privacy Act* available on their Web sites. Where annual reports were posted, they were often difficult to find, or out of date (five organizations did not post the 2006-07 report). While anyone can obtain copies of reports tabled in the House of Commons with a written request, this process is neither obvious nor convenient.

30. Recommendation: TBS should require departments to make Annual Privacy Reports available on their Web sites.

31. Treasury Board Secretariat Response: "TBS agrees that posting copies of the annual reports on institutional websites would facilitate public awareness of the governmental privacy program. For the 2008-2009 and subsequent reporting periods, TBS has recommended that institutions consider posting copies of their Annual Reports online to promote accessibility and transparency."

Conclusion

32. Almost all federal organizations in our sample met the basic, mandatory reporting requirements with respect to reporting on privacy matters under the *Privacy Act*. In responding to the mandatory reporting elements, most departments had complied with TBS's reporting requirements. However, with certain exceptions, they were not providing the kind of comprehensive information in their Annual Privacy Reports needed to provide Parliament and the general public with an accurate picture showing how they were managing their privacy programs.

33. This audit did not specifically assess the quality or adequacy of TBS's reporting requirements for APRs, however, we identified a few organizations went beyond the basic reporting requirements. When departments make a

reasonable effort to meet TBS reporting requirements, they can provide an adequate a picture on how they administer privacy matters.

About the Audit

Authority

Audit was conducted pursuant to Section 37 of the *Privacy Act* which gives the Office of the Privacy Commissioner of Canada the authority to examine the personal information handling practices of government organizations.

Objective

To determine whether select federal institutions adequately reported on how they manage the personal information of Canadians in their 2006-2007 Annual Privacy Reports.

Scope and approach

The reporting requirements described in TBS Implementation Bulletins 106 and 107 applied to all departments, Crown corporations and agencies subject to the *Privacy Act*. The audit focused on the 25 federal institutions that appear most active in the collection, use and dissemination of personal information, and another eight institutions subject to the Act, randomly selected. In selecting the former, we considered specific parameters such as the volume and sensitivity of personal information that they handle evidence of significant system or program investments, and the results of past reviews, including evidence of possible non-compliance with the Act.

Criteria

We expected that:

- The Annual Privacy Reports should report against all TBS's mandatory reporting elements contained in Implementation Bulletins 106 and 107.
- The information presented in Annual Privacy reports in response to the reporting elements should provide a clear picture of how departments and agencies are managing their programs.

Audit team

Directors General: Trevor Shaw / Steven Morgan

Navroze Austin
Paul Zind

Appendix 1: Federal Institutions included in the Audit

- Agriculture and Agri-Food Canada
- Canada Border Services Agency
- Canada Post Corporation
- Canada Revenue Agency
- Canadian Heritage
- Canadian International Development Agency
- Canadian Security Intelligence Service
- Citizenship and Immigration Canada
- Correctional Service of Canada
- Department of Finance Canada
- Department of Justice Canada
- Elections Canada
- Environment Canada
- Export Development Canada
- Financial Transactions and Reports Analysis Centre of Canada
- Fisheries and Oceans Canada
- Foreign Affairs and International Trade Canada
- Health Canada
- Human Resources and Skills Development Canada
- Immigration and Refugee Board of Canada
- Indian and Northern Affairs
- Industry Canada
- National Defence and the Canadian Forces
- National Research Council Canada
- Natural Resources Canada
- Office of the Auditor General of Canada
- Public Safety Canada
- Public Service Commission of Canada
- Public Works and Government Services Canada
- Royal Canadian Mounted Police
- Statistics Canada
- Transport Canada
- Veterans Affairs Canada

Appendix 2: Reporting Requirements of TBS Implementation Bulletin No. 107

Reporting Elements

1. Introduction, including the mandate of your institution and a summary of your institution's privacy activities during the fiscal year, i.e. your institution did not process any requests or other undertakings that you would like to highlight. **(Mandatory)**
2. Description of how the institution is structured to fulfill *Privacy Act* responsibilities. **(Mandatory)**
3. A copy of the Delegation Order indicating what powers, duties and functions have been delegated by the head of the institution and to whom, or a statement that there has been no delegation. **(Mandatory)**
4. Statistical Report. **(Mandatory)**
5. Interpretation of the statistical report, such as the description of significant trends and details on the processing of requests, the application of exemptions and exclusions, completion times and extensions. **(Mandatory)**
6. A summary of significant changes/improvements to operations, policy, procedures, privacy protection, etc. **(Mandatory if applicable)**
7. Overview of institutional Privacy Act-related policies and procedures implemented or revised during fiscal year. **(Mandatory if applicable)**
8. Description of privacy related education and training activities, including briefing and awareness sessions. Indicate the number of sessions and the number of participants. **(Mandatory if applicable)**
9. Information on Privacy Impacts Assessments (PIA) and Preliminary Privacy Impact Assessments (PPIA):
   - the number of PIAs and PPIAs initiated
   - the number of PIAs and PPIAs completed
   - brief description of each PIA completed and the link to its summary on your institution's website
   - the number of PIAs forwarded to the Office of the Privacy Commissioner.

   (Mandatory)
10. An overview of the types of disclosures made pursuant to subsections 8(2)(a) to 8(2)(m) of the *Privacy Act* during the fiscal year. Note: Statistical information is not required – just a brief summary of all of the types of 8(2) disclosures made during the reporting year. **(Mandatory)**
11. The number of new data matching and sharing activities undertaken (this includes new internal data matching and sharing activities between different sections of the institution) and a short description of each activity. **(Mandatory)**
12. Privacy impact of any legislative, policy and service delivery initiatives or data matching or data sharing agreements. **(Mandatory if applicable)**
13. Description of major changes implemented (if any) as a result of concerns raised by the Office of the Privacy Commissioner, i.e. in her Annual Report to Parliament, reviews of PIAs, or other reviews/evaluations of how your institution administers the *Privacy Act*. **(Mandatory if applicable)**
14. Indicate if your institution had any Privacy complaints and summarize key issues arising from complaints and/or investigations during the fiscal year. **(Mandatory if applicable)**
15. Enumeration of the number of Appeals to the Courts during the fiscal year, i.e. applications submitted to the Federal Court – Trial Division, or the Federal Court of Appeal. (**Mandatory if applicable)**