Chapter 20
Auditing Privacy Impact Assessments: The Canadian Experience

Jennifer Stoddart

20.1 Introduction

In early 2007, the Office of the Privacy Commissioner of Canada (OPC) embarked on a project to measure the extent to which privacy issues arising from government operations were being appropriately managed. The audit, titled Assessing the Privacy Impacts of Programs, Plans and Policies,1 was the first of its kind in Canada and, to the best of our knowledge, the only comprehensive evaluation of the implementation of privacy impact assessments (PIAs) worldwide. It was an important initiative, not only for its findings – many of which can be applied cross-jurisdictionally – but also for its salutary effects on PIA practices government-wide. While the primary objective of the audit was to assess compliance with the government’s policy on PIAs, it has served as importantly to promote an understanding of PIAs as an effective risk management tool.

Canada is generally accepted as a leader in privacy impact assessment.2 Within the general statutory regime governing privacy matters in the public sector, mainly the Canadian Charter of Rights and Freedoms3 and the federal Privacy Act,4 PIA remains the most comprehensive model in place to assess the effects of federal initiatives on an individual’s privacy. Indeed, PIAs are mandated by government for all new or substantially modified programs involving the creation, collection and

---


J. Stoddart (✉)
Privacy Commissioner of Canada, Ottawa, ON, Canada
e-mail: Lindsay.Scotton@priv.gc.ca
handling of personal information.\textsuperscript{5} As such, they have been – and continue to be – a core component of the federal government’s privacy compliance regime.

Notwithstanding Canada’s policy requirements, PIAs have not always been performed as and when required.\textsuperscript{6} As recently as 2007, nearly 70\% of federal government departments reported that they did not have a formal management framework in place to support the conduct of PIAs.\textsuperscript{7} Despite the government’s aim of ensuring that privacy protection was a key consideration in a project’s initial framing, PIAs were often completed well after program implementation. In many cases, PIAs were not completed at all. What explains the paradox of seemingly strong privacy prescriptions and failing federal grades? Had the burden of privacy impact assessments become too great? What other models exist to better promote privacy analysis in the development and scoping of new initiatives involving personal information?

This chapter sets out to answer some of these questions by reference to the results of our audit of PIA practices in Canada. It is both a report on our audit observations – what we found – and an essay on the effects of our review – what we feel has been accomplished. We begin by reviewing the most important findings from our audit. Herein, we share some of the measurement tools we employed in assessing the quality of PIA practices within the Canadian federal government. Next, we revisit some of our key policy recommendations. This section is intended to assist other jurisdictions involved in the development of PIA regimes with lessons learned from Canada. We conclude by reflecting upon the most important outcomes of our audit: better PIA practices, shared insight and expectations regarding PIA outcomes, and greater compliance with what is required. Throughout the chapter, we hope to impress upon the reader the value of audit, not just as an instrument for privacy enforcement, but also as a means of shaping the personal information-handling practices of organisations involved in potentially privacy intrusive programs.


\textsuperscript{6} See PIA Audit, supra fn. 1 at ¶ 1.1.

\textsuperscript{7} Ibid. at ¶ 1.36.