# Focus on Canadian Employment and Equality Rights

October 2012
Number 34



CCH
a Wolters Kluwer business

## BEYOND THE PRIVACY POLICY: NEW GUIDANCE

*— Timothy M. Banks. © 2012 Fraser Milner Casgrain LLP. Reproduced with permission.*

On September 5, 2012, the Information and Privacy Commissioner of Ontario ("IPC") released a new guidance paper, entitled "A Policy is Not Enough: It Must be Reflected in Concrete Practices". This guidance paper will be particularly useful for organizations seeking preliminary guidance on implementing the "privacy by design" principles developed by Commissioner Cavoukian.

The IPC outlines 7 steps for implementing privacy policies. Sensibly, the Commissioner acknowledges that there are no "one-size-fits-all" approaches for embedding privacy-by-design practices. Nevertheless, Commissioner Cavoukian notes that there are common steps to implementing a course of action. These steps are applicable to organizations of all sizes and complexity.

The following is a brief run-down on the steps and a few comments from my experience:

**Step One: The organization should develop and implement a privacy policy that is compliant with privacy laws *and* is tailored to the needs and risks of the organization.** As the Commissioner notes, "a generic policy, which does not consider the particular challenges of a given organization" is "not sufficient."

Too often, organizations simply copy the basic privacy principles from applicable privacy legislation without attempting to describe those principles in a concrete way in their organizational environment. The IPC recommends that if the organization deals with sensitive data, the organization should conduct a privacy impact assessment ("PIA"). Arguably, however, a PIA is useful whenever the organization is developing or revising a privacy policy or engaging in a new initiative. From my perspective, the PIA is particularly useful in (a) identifying practices that may create legal risks regarding an organization's data governance practices, (b) organizing conversations about the extent of collection, use and retention of personal information that is necessary to the success of particular initiatives, (c) identifying stakeholders within the organization that should be accountable for the protection of personal information collected and used in connection with the initiative, and (d) assessing the administrative, technical and physical procedures necessary to provide adequate protection of that personal information.

The development of an organization's privacy policy is not a "one-time" event. The IPC recommends at a minimum an annual review to determine the evolving legal and industry practice environment as well as whether the privacy policy of the organization and the procedures of the organization are consistent.

**Step Two: The organization should link each policy item to a specific action item.** For example, if a privacy policy provides that personal information will not be transferred in an unencrypted form over the Internet, then the organization must consider how to

implement that policy to prevent data transfers that are not encrypted. This may mean changes to the IT infrastructure to ensure encryption by default.

**Step Three: The organization should establish how the organization will demonstrate that the action items have been implemented.** Commissioner Cavoukian notes that effective change requires "buy in" from senior management and the demonstrable adherence to the policy by those who are accountable for the action item.

**Step Four: The organization should develop an education and awareness training program that is tailored to the working environment of the organization both in structure and content.** Initial training for employees on the organization's privacy practices is critical, but so is on-going education and awareness so that the organization's privacy practices are integrated into the employee's duties. The IPC recommends at least annual refreshers or certifications. There are diverse methods of education and awareness training. However, to be effective, they must be directly relevant to the employee's duties.

**Step Five: The Commissioner recommends the designation of a "Go to" person.** Employees should have a person that can address privacy concerns raised by employees and to assist them in assessing the implications of particular privacy practices.

**Step Six: Organizations must audit compliance: "Trust, but verify".** An organization should have a policy on the types of compliance audits that will be conducted and the procedures for those audits. The audit process should be documented.

**Step Seven: The last step is to prepare for a privacy breach.** Too often organizations are unprepared to handle a serious privacy breach. The Commissioner states that "[i]t is increasingly important that organizations of all sizes be prepare to react to data security incidents". An organization should have a data breach protocol so that the organization is able to react quickly and effectively. Privacy breach protocols assist in identifying the initial steps and persons accountable for reporting the breach, containing the breach, notifying affected individuals, investigating the causes and recommending remediation actions.

*Timothy Banks advises organizations on practical solutions to governance issues and litigation risk, particularly with respect to corporate records, privacy, e-commerce, data use and directors and officers responsibilities. He is a partner in the Business Law Department of the Toronto office of Fraser Milner Casgrain LLP* (www.fmc-law.com) *and head of the national lead for the firm's Privacy Practice. He blogs at* www.datagovernancelaw.com *and may be reached at timothy.banks@fmc-law.com.*