

Eye on Privacy



To Notify or Not to Notify

Pat Flaherty and Jana Stettner*

There are a growing number of cases of organizations reporting the loss, mistaken disclosure or theft of personal information collected in the course of commercial activities. Perhaps one of the largest cases of loss of personal information occurred last November, when it was reported that the British government lost two computer disks containing the names, addresses, National Insurance numbers, and in some cases bank account information, of over 40% of the British population.^[1] This example, while not in a commercial context, illustrates the potential for

large scale loss of sensitive personal information, creating a risk of harm, including identity theft, to affected individuals.

While there is currently no express obligation in the *Personal Information Protection and Electronic Documents Act*^[2] (*PIPEDA*) for organizations to notify affected individuals or privacy regulators when breaches occur, government and regulators are paying increasing attention to this issue. Other jurisdictions are also paying close attention, with the majority of US states having already adopted legislation with mandatory breach notification requirements, including in some cases large fines for failure to comply.^[3] This article will discuss provisions of *PIPEDA* and *Ontario's Personal Health Information and Protection Act*^[4] (*PHIPA*) that are relevant to the issue of notification, the status of the government's consideration of amendments to *PIPEDA* to include a mandatory notification requirement, as well as best practices for organizations to follow until such time as any amendments are made.

PIPEDA and PHIPA

While there is no express requirement in *PIPEDA* for organizations to notify affected individuals or privacy regulators that there has been a privacy breach, this does not preclude the Office of the Privacy Commissioner (OPC) from taking the position that notification is nevertheless required under the mandatory principle in Schedule 1 that personal information be protected by "security safeguards" appropriate to the sensitivity of the information.^[5] ^[6] For example, where affected individuals may be able to take steps to prevent the unauthorized use of information that has been lost, the OPC may take the view that, under the security safeguard principle, the organization is required to notify affected individuals of the breach.

Unlike *PIPEDA*, section 12 of *PHIPA* contains an express obligation for health information custodians to report the theft, loss or unauthorized access of personal health information, regardless of the circumstances or risk of harm to individuals. Section 12 requires notification to be made at the first reasonable opportunity, but does not articulate the specific manner by which notification is to be made nor does it require privacy regulators to be notified.

Amendments to PIPEDA

While no specific amendments to *PIPEDA* have been tabled, the OPC has recommended amendments to make notification of breach to affected individuals mandatory.^[7] The government has also been considering this issue.

The House of Commons Standing Committee on Access to Information, Privacy and Ethics (Committee) tabled a report in May of last year which did not recommend the creation of a general duty to notify in all cases, but instead proposed that organizations have a duty to report certain defined breaches to the Commissioner, who would then make the determination of whether affected individuals should be notified.^[8]

The government responded to the Committee's report in October.^[9] It supported mandatory notification of individuals and

regulators for breaches where there is a “risk of significant harm to individuals”, but did not support a general requirement to provide notification of all breaches. The government also did not support the Committee’s proposal that the Commissioner make the determination of whether affected individuals are to be notified, stating instead that organizations must make this determination on a case by case basis based on an analysis of the risk of harm. In light of the government’s response to the Committee’s report, it seems unlikely that *PIPEDA* will be amended to require a duty to notify in all cases of breach.

OPC’s Guideline and Best Practices

While *PIPEDA* itself does not speak directly to the issue of when notification is required, the OPC has published a guideline to assist individuals in determining whether notification is appropriate.^[10] The guideline lists factors for organizations to consider and states that if a breach creates a risk of harm to individuals, those individuals should be notified. The guideline further encourages organizations to report material privacy breaches to the appropriate privacy commissioner(s) so that they are better able to respond to public inquiries.

In making the difficult determination of whether to notify affected individuals and regulators, it is useful for organizations to consider the purposes notification is intended to serve. The primary purpose of notifying affected individuals is to enable them to mitigate the risk of harm. Accordingly, whether there is in fact a risk of harm and whether it is possible for the affected individuals to mitigate that risk will be important considerations for organizations in determining whether notification is appropriate.

In cases where individuals are notified, it may also be appropriate to notify the relevant privacy regulators so that they are equipped to deal with any questions or complaints they may receive. The primary purpose of notifying privacy regulators of a breach is for them to identify problems of a more systemic nature in an organization which need to be addressed.

In this respect, the OPC’s guideline, though it does not create a statutory obligation, may be asserted by prospective plaintiffs as creating a standard of care or best practice that could be relevant when determining whether notification should have been made.^[11] Finally, while organizations may view risk of harm to reputation or brand as the largest downside of notifying affected individuals of a breach, there may in fact be more harm to reputation if an organization fails to notify and any preventable harm results.

* *Pat Flaherty and Jana Stettner are with the Toronto office of the law firm Torys.*

[1] *British Govt. Loses Data on Almost Half Its Population (21 November 2007)*, Wall Street Journal.

[2] S.C. 2000, c.5.

[3] *PIPEDA Review Discussion Document: Protecting Privacy in an Intrusive World (18 July 2006)*, Office of the Privacy Commissioner of Canada.

[4] S.O. 2004, c. 3.

[5] See section 4.7 (Principle 7) in Schedule 1 to *PIPEDA*.

[6] Organizations must also consider whether, aside from any statutory obligations, they have a contractual obligation to notify affected individuals of a breach.

[7] *News Release: Privacy Commissioner releases privacy breach guidelines (1 August 2007)*, Office of the Privacy Commissioner of Canada.

[8] House of Commons, Committee on Access to Information, Privacy and Ethics, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, Fourth Report, 1st Session, 39th Parliament, May 2007.

[9] Industry Canada, “Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics”, *Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*.

[10] *Key Steps for Organizations in Responding to Privacy Breaches (28 August 2007)*, Office of the Privacy Commissioner of Canada.

[11] See *Somwar v. McDonald’s Restaurants of Canada Ltd.*, (2006), 79 O.R. (3d) 172 (S.C.J.), which involved a motion to strike out a claim for invasion of privacy as disclosing no reasonable cause of action. Justice Stinson denied the motion to strike holding that the time has come to recognize invasion of privacy as a tort in its own right.



Eye on Privacy: The OBA Privacy Law Review is published by the Privacy Law Section of the Ontario Bar Association. The Editors welcome submissions on privacy law matters of interest to our members.

The articles that appear in this publication represent the opinions of the authors. They do not represent or embody any official position of, or statement by, the OBA except where this may be specifically indicated; nor do they attempt to set forth definitive practice standards or to provide legal advice. Precedents and other material contained herein are intended to be used thoughtfully, as nothing in the work relieves readers of their responsibility to consider it in the light of their own professional skill and judgment.