Pitblado LAW

Privacy Breaches in Manitoba

A Mitigation and Prevention Primer

Author: Andrew Buck, Lawyer

Overview: The Importance of Having a Plan

A privacy breach is typically defined as the unauthorized use of, or access to, personal information or personal health information. In most cases, privacy breaches involve stolen, lost, or mistakenly disclosed personal information about clients, patients, students, or employees. Ideally, an organization should prioritize the creation of a privacy breach response plan because, more often than not, an immediate response is crucial and therefore, it is necessary to establish a plan before a breach occurs. This whitepaper broaches the topics of: legislation and requirements regarding notification, the current and future landscape of privacy breaches, components of a breach response plan, and breach prevention strategies.

The Future Direction of Privacy Legislation

The *Personal Information Protection and Electronic Documents Act (PIPEDA)* is Canadian law that lays down the groundwork for how private sector organizations collect, use, and disclose personal information, while engaged in commercial activity. For the federal public sector, the *Privacy Act* deals with how personal information is handled by government departments and agencies. Provinces have their own privacy laws which apply to public sector activities at the provincial level. All of these laws are grounded in values and rights closely linked to those outlined in the Constitution that are deemed necessary to a free and democratic society; the Supreme Court has stated, for example, that the *Privacy Act* has "quasi-constitutional" status.

Ongoing amendments to *PIPEDA* are moving that law toward requiring notification of privacy breaches. Those amendments are not yet in force, pending the passage of regulations that will flesh out the contours of reporting obligations. Manitoba also has proposed private sector privacy legislation that would require mandatory breach notification (though that law is not proclaimed in force and it is unclear when that will happen, if ever). That said, given the developments under *PIPEDA*, it is simply a matter of time before mandatory privacy breach notification is a reality.

Current Landscape: To Notify or Not to Notify?

Currently, the general rule is that there is *no mandatory duty* in Canada to report a privacy breach, with a few notable exceptions:

Province	Sector/Type of Information
Alberta	Private Sector Organizations
Ontario	Health Information
New Brunswick	Health Information
Newfoundland & Labrador	Health Information
Manitoba	Proposed for Private Sector Organizations

Current provincial requirements for reporting privacy breaches in Canada.

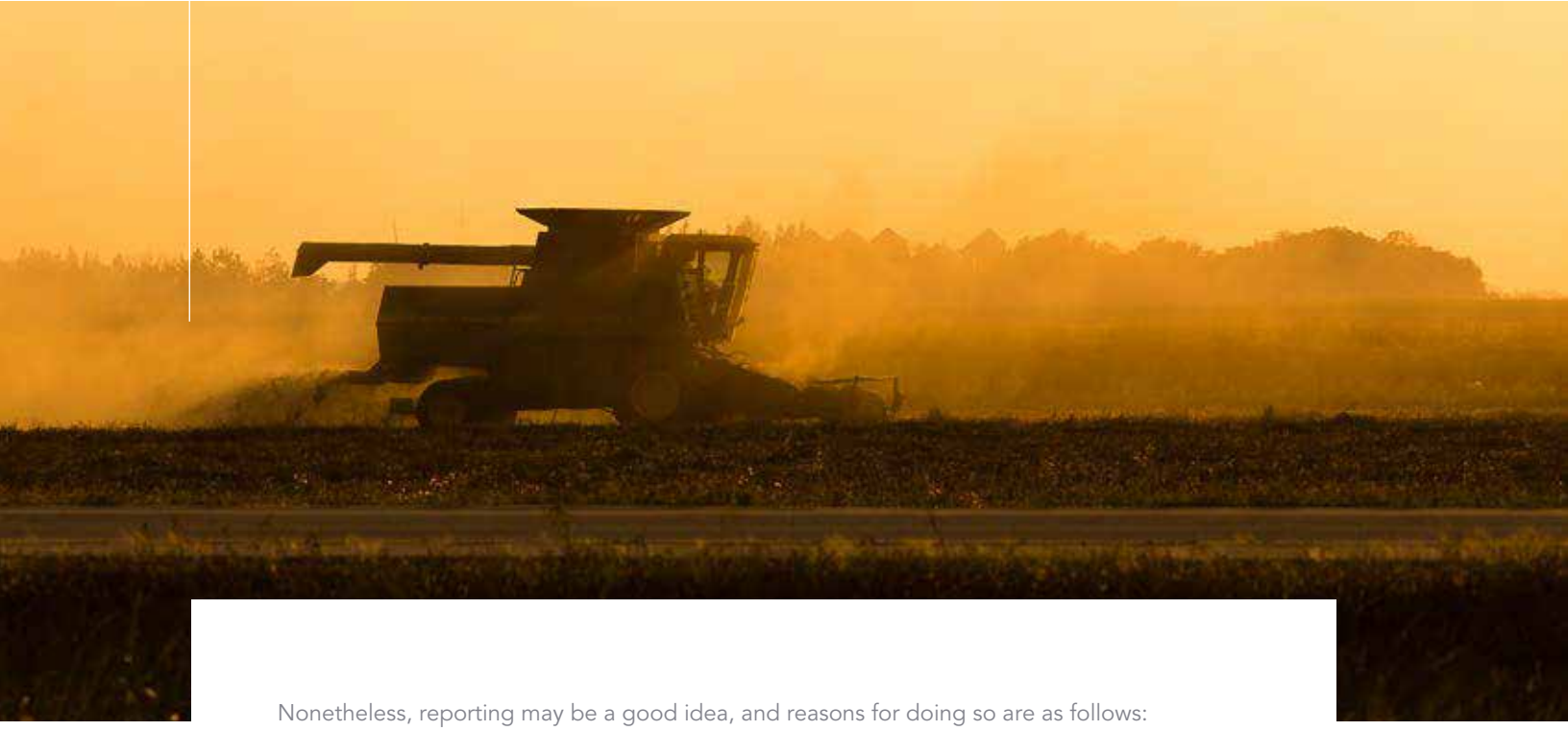
As noted above, once *PIPEDA*'s breach notification regulations are in effect, private sector businesses which are subject to *PIPEDA* will be required to report privacy breaches.

Consequences of Noncompliance

Once mandatory breach notification is in force under *PIPEDA*, organizations which knowingly fail to report or record breaches could be found guilty of an offence punishable by fines of up to $100,000. They may be named (and shamed) by the Office of the Privacy Commissioner of Canada (OPC), and consequently risk suffering the PR fallout of such an event.

Voluntary Notification

For organizations which have suffered a privacy breach and for which mandatory notification is not currently required, a decision about notification itself can be an involved process of weighing the reasons for, and against, reporting the breach. Organizations usually prefer to avoid drawing attention to the breach (think, "If a tree falls in the forest and nobody is around to hear it, does it make a sound?"), especially if the consequences of the breach are minor in nature. This includes both negative consequences at the client or customer level, as well as unfavourable external PR. In addition, information disclosed as part of breach reporting might then be used against the organization in future litigation.



Nonetheless, reporting may be a good idea, and reasons for doing so are as follows:

- The risk of potential negative PR due to *not reporting*, if the breach is later discovered, may outweigh the initial blowback from notifying
- As a preventive measure, getting in front of a breach can reduce eventual exposure to liability, if a breach is litigated (as was the case in *Lozanski v. Home Depot*)
- It is a practice of being a good corporate citizen

Harm & Varying Degrees of Severity

Some breaches are more serious than others, and when assessing a privacy breach, it is important to consider whether a "real risk of significant harm" is created by the breach.

Possible harm to affected individuals or a group may include:

- Risks to their physical safety/security risk
- Identity fraud or theft
- Hurt, humiliation, reputation damage, damage to relationships
- Loss of business or employment opportunities
- Loss of trust
- Loss of assets
- Financial exposure

If it is determined that a breach does *not* cause a real risk of significant harm, then an organization might choose not to report it. However, the organization should carefully consider notification, regardless of how severe the breach is determined to be. While notification may not be legally required, it is a generally a good practice to be transparent - and it may very well save your organization's reputation in the long run.

Breach Responses: Key Steps

Consider the following steps, once a breach has occurred:

Think about engaging external legal counsel immediately, as a measure to protect all discussions with those who work to remediate the breach with privilege. For instance, if the organization's lawyer engages forensic experts and/or a PR firm, that effectively clothes those discussions with privilege that may protect them from being disclosed in later proceedings.

Assessing and Diagnosing the Breach

The first step in diagnosing the breach is notification of the person responsible for security in your organization, so that she or he can gather all pertinent details, including:

- What information was available?
- Who could see it? For how long?
- How many individuals were affected?
- How did it happen?
- How and when did you find out?
- Can you track who accessed it?
- Is there an ongoing risk or possible further exposure of the information?

In the course of getting answers to these questions, your organization may require forensic help - it is important to get a complete understanding of the extent of the problem so a proper course of action can be selected. Regardless of whether the breach is determined to meet the "real risk of significant harm" reporting threshold under *PIPEDA*'s breach notification regime, records of *all* data breaches must be kept.

Breach Responses: Key Steps continued.

Containing the Breach and Taking Steps to Reduce Harm

Depending on the nature of the breach, different routes may be taken to contain the breach at hand. Examples of breach containment include: stopping the unauthorized practice, shutting down or limiting access to the system or database that was breached, or remedying weaknesses in physical security. This may also be an opportune time to come up with a plan to prevent the occurrence of breaches of a similar nature, and to demonstrate that your organization has taken steps to ensure the chances of a similar breach in future are minimal.

Once the breach has been contained, it is crucial to take steps to reduce harm. This applies to the affected individuals, as well as inside your organization. It is also prudent to consider proactively offering harm reduction services to affected individuals - credit monitoring or providing information about how to obtain a new Social Insurance Number, for instance. Evaluate the possible uses of the breached information and take steps to minimize possible harm.

Notification

If notification is appropriate, the OPC may be notified, along with the individual(s) affected by the breach and any other organizations that might assist in minimizing the risk of harm to the affected individuals. This notification should be sent as soon as feasible after the organization determines a breach has occurred. The notification should contain sufficient information to provide the recipient an understanding of the significance of the breach (such as the date of the breach, description of the circumstances of the breach, and a description of the breached personal information) as well as an outline of the steps the organization has taken to control the situation and to mitigate any further harm.

The notification must be conspicuous and given directly to the affected individual(s), provided that it is feasible to do so. It should also recognize the impact of the breach on the individual(s) (the organization may consider including an apology), and offer the individual(s) steps that could be taken to reduce harm, as well as sources of information about how to protect against identity theft. Contact information for an individual within your organization who can answer questions or provide further information should also be included.

Note that the exact content and procedural requirements of notification are subject to regulations under PIPEDA which are yet to be released.

Proactive Steps for Preventing a Privacy Breach

It is a useful exercise to take proactive steps to prevent a privacy breach. Begin by imagining your organization's response to a breach, and asking the question, "Would we be prepared if a privacy breach occurred?" Continuing along this vein, it may also be useful to assign responsibility to people within your organization specifically related to preparation and/or mitigation of a breach (and in particular, designating a person who is ultimately responsible for these measures).

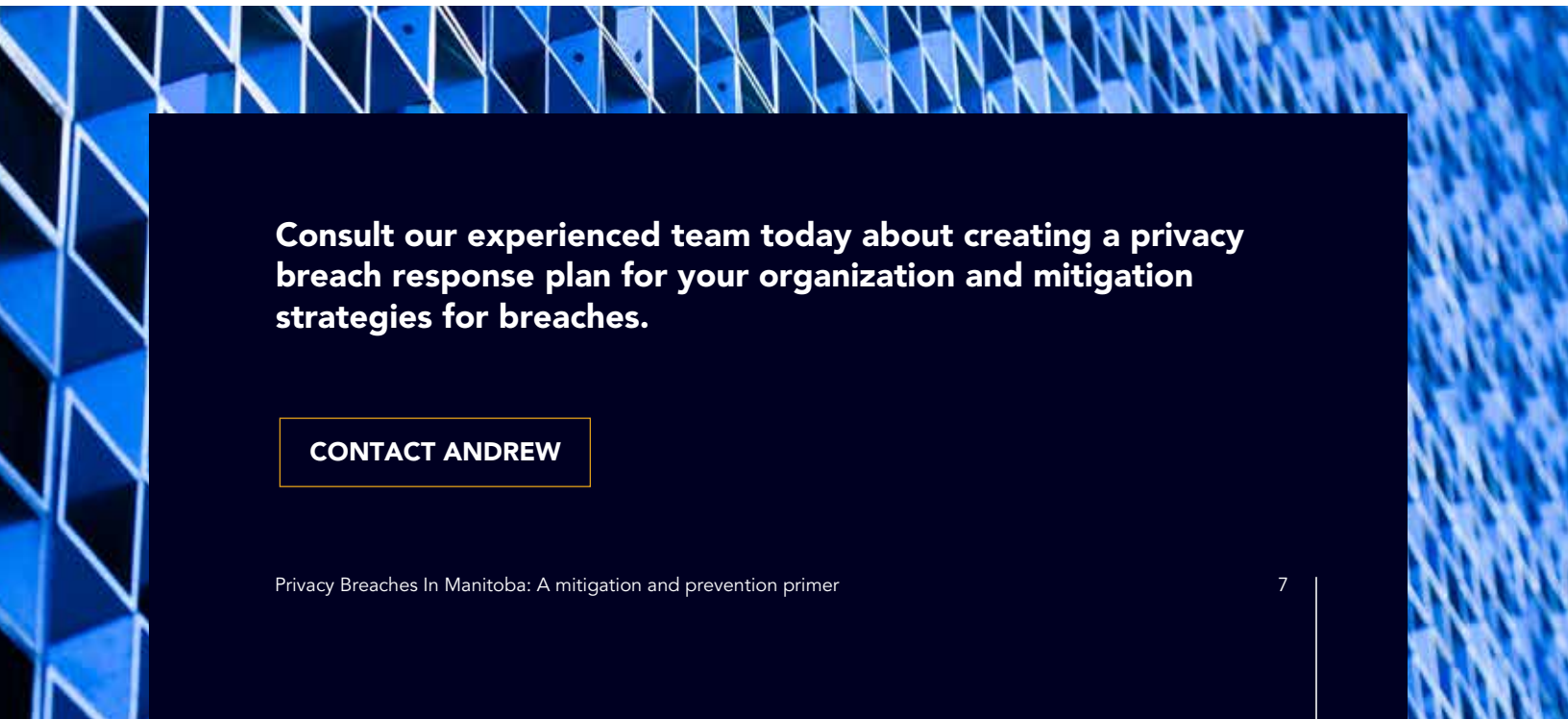
The Self-Audit Process

To perform a self-audit, evaluate your organization with the following questions:

- Where within our systems and structure might there be possible exposure of sensitive information?
- Where are our weaknesses in how we store or transmit information?
- What are possible threats to the integrity of how private information is handled within our activities?
- How likely are we to suffer a privacy breach? Are there are any steps we can take to avoid problems?

Preparing a Breach Response Plan

To help ensure preparedness for a privacy breach, your organization should prepare reporting procedures that make it easy to be quick and decisive, if a breach occurs. The appointment of a Privacy Officer for your organization is a good first step (and is in fact required by privacy laws), along with the creation of a Privacy Breach Checklist that covers the details of the privacy breach, mitigation and prevention measures, and notification particulars. Having a system in place allows an organization to respond professionally and consistently if a privacy breach occurs, and in so doing, reduce harm to the organization and affected individuals alike.



Consult our experienced team today about creating a privacy breach response plan for your organization and mitigation strategies for breaches.

CONTACT ANDREW

Pitblado LAW

BUSINESS LAW

ANDREW J.D. BUCK
Lawyer

P. 204.956.3569
F. 204.957.0227
E. buck@pitblado.com

www.pitblado.com