Field Notes

January 22, 2013

Alberta Privacy Commissioner Issues Report on Privacy Breaches

by Anne Côté
Area of Coverage - Privacy

Alberta's new Privacy Commissioner, Jill Clayton, has released a report on the first two years of mandatory privacy breach reporting in Alberta (the "Breach Report").

Under Alberta's private sector privacy law, the *Personal Information Protection Act* ("PIPA"), a privacy breach that presents "a real risk of significant harm" must be reported to the Privacy Commissioner, who can then require an organization to notify affected individuals. Relevant "harms" include risk of identity theft, damage to reputation, and risk to personal safety.

As of the end of April 2012, 151 breach reports had been received by the Privacy Commissioner. Of these reports, 63 cases (42%) involved a real risk of significant harm. In the remainder of the matters, this threshold was not reached, PIPA was determined not to apply, or the matter was still under review.

The Breach Report shows that a majority of the 63 reported cases meeting the real risk of significant harm threshold involved human error or lost or stolen unencrypted electronic devices:

- **22 breaches were caused by human error**. These incidents included inappropriate disposal of personal information, emails sent to the wrong individuals (or viewable to all individuals in a mass email), faxes sent to the wrong person or to an unsecure fax, loss of files and portable memory sticks, and unauthorized disclosure of passwords. The most common form of human error was mail and courier errors caused by delivery to the wrong individual.
- **18 breaches were caused by theft**. These breaches were primarily due to office and car break-ins resulting in the loss of computer devices, although in a few cases paper documents were also stolen.
- **14 breaches were caused by electronic system compromises**. These breaches were typically found to occur as a result of targeted attacks by external hackers seeking to extract large amounts of data. In one incident, 50 million individuals were affected.
- **9 breaches were caused by a failure to adequately control access to electronic or paper files**. One case in particular involved files that were accessible to the public via the Internet.

Where a real risk of significant harm was found, the Breach Report indicates that most of the personal information breached was considered to be of high sensitivity, such as social insurance numbers, drivers' license numbers, or credit card numbers. The Breach Report also indicates that the following circumstances were likely to lead to a real risk of significant harm:

- where information was apparently stolen for nefarious purposes;
- where recipients could not be determined;
- where electronic devices containing personal information had no encryption and no audit capability, making access possible and unknown; and
- where a large number of individuals were affected and where there was a likelihood that the personal information could be used for a nefarious purpose (such as "phishing" for more personal information).

The Breach Report also offers some commentary on when reporting is not required. Where no real risk of significant harm was found, the personal information involved was typically of low sensitivity (such as names, addresses, phone numbers, membership information, email addresses, product purchase information, and low risk financial information such as mortgage balance and RESP balance). Even where sensitive information was breached, reporting was not required where the organization used strong encryption methods or

auditing capability, thus making access to the information highly unlikely. Typically, reporting was not required where recipients were few and known to the organization, or where the information was returned or confirmed destroyed in a relatively short time frame.[1].

The Breach Report offers further guidance on prevention of privacy breaches. In addition to measures intended to protect against specific risks to personal information, organizations should implement the following basic steps:

1. **Limit collection** of personal information only to that which is reasonably needed to meet business and legal purposes.

2. **Develop policies** and procedures with privacy protection in mind, including breach notification procedures, and update these policies and procedures regularly.

3. **Train staff** to understand the importance of protecting personal information and of breach notification. Consider implementing staff confidentiality agreements where necessary.

4. **Ensure proper controls** are in place for contractors and other third parties with access to personal information, and include a requirement that the contractor or third party promptly notify the organization in the event of a privacy breach.

5. **Limit retention** of personal information only to that period necessary to meet business and legal purposes and then securely destroy the information or render it anonymous.

A determination of whether to report a privacy breach is only one aspect of privacy breach management. Organizations must respond as quickly as possible to a suspected privacy breach because containment of the personal information may minimize harm to affected individuals, and may even prevent a potential breach from becoming an actual breach. Once a breach situation has been adequately investigated, organizations should also consider whether to revise existing policies and procedures, and whether to implement additional policies and procedures. Being proactive about these matters can save an organization from the next potential privacy breach.

Footnotes:

1. In Order P2012-02, the Adjudicator determined that the reporting threshold would not have been met where mail containing a reassessment of educational qualifications was sent to a professional also undergoing the reassessment process, who returned the mail to the organization. Importantly, the fact that the unintended recipient was a stranger unknown to the affected individual militated against any risk of humiliation or damage to reputation.