BUDDLE FINDLAY

Mandatory privacy breach reporting - where are we now?

Allan Yeoman

9 December 2021

One of the most notable changes made to New Zealand privacy law by the Privacy Act 2020 was the introduction of a mandatory privacy breach reporting regime. It has now been just over a year since the new regime came into effect.

To recap, the definition of 'privacy breach' includes unauthorised or accidental access to, or disclosure of, personal information, or an action that prevents an agency from accessing personal information, either temporarily or permanently. A 'notifiable privacy breach' is a privacy breach that causes or is likely to cause serious harm. Under section 114 of the Act, an agency must notify the Privacy Commissioner as soon as practicable after it becomes aware of a notifiable privacy breach.

The past 12 months have seen several high-profile cyber security attacks and privacy breaches, all of which will have tested the thinking under the new reporting requirements. Of more direct interest to many New Zealand companies and organisations however, the Office of the Privacy Commissioner (OPC) has recently published a report detailing the privacy breach notifications it received between 1 December 2020 and 31 October 2021. The report details the following key findings:

A total of 697 privacy breaches were reported to the Commissioner. Of those, one third met the threshold for serious harm, suggesting a (foreseeable) tendency toward over-reporting as organisations came to grips with the new requirements and adopted a conservative approach. Almost four times as many breaches were reported between this period than between 1 December 2019 and 31 October 2020.

Over one third of serious breaches involved emotional harm. Emotional harm is involved where a breach leads to 'significant humiliation, significant loss of dignity or significant injury to an individual's feelings.' Treated separately from other types of harm commonly reported, such as reputational harm (14%), identity theft (13%) and financial harm (11%), the emotional consequences of privacy breaches can clearly cross the threshold of 'serious harm' and trigger reporting obligations.

Human error was by far the most common cause of serious privacy breaches. This affirms an already well-known phenomenon. Human error accounted for 62% of serious privacy breaches reported, and within that category, the most common type of error was email error (such as sending an email to the wrong person, attaching the wrong documents, or not BCC'ing when sending to multiple recipients). In comparison, only 25% of serious breaches were caused by malicious attacks and 6% by theft of information. The remainder were attributable to system fault and other causes. The OPC will be in equal parts encouraged and frustrated that such a large proportion of reported breaches are preventable.

All sectors experienced privacy breaches, but Health Care and Social Assistance and Public Administration were the industry classifications that reported the highest number. Over half of serious privacy breaches were reported by the public sector, a third by the private sector and the rest by the non-profit sector. The OPC notes that a high number of notifications from an industry is perhaps a sign of greater awareness of the obligation to report privacy breaches, rather than an indicator of poor privacy practices.

Less than half of all serious breaches were notified within 72 hours of identification. In June 2021, the OPC set the expectation that notifiable breaches should be reported within 72 hours of an agency becoming aware of it. Contrary to this expectation, most breaches in this period were reported outside of the 72 hour window – one in four were reported within 10 days, 15% were reported within 30 days and 9% were reported more than a month after the agency knew about the breach. We expect this will become an area of focus for the OPC in the second year of the mandatory notification regime, and further guidance and clarification around when the 72 hour clock starts ticking (ie, when the agency becomes aware of the breach, or when it decides that it's a *notifiable* breach) would be helpful.

Only 61% of individuals affected by the privacy breach had been contacted by the time the breach had been reported to the OPC. Although the OPC understands the process of notifying all affected individuals can take longer than the 72 hour window, the report expresses concern some agencies are failing to tell people that their personal information has been involved in a breach, noting that there are only limited grounds for not informing affected individuals (as set out in section 116 of the Act).

What next?

2021 has been a settling-in period for the mandatory notification regime, with many businesses forced to make judgment calls about whether or not to notify and (based on the OPC's data) appearing to err on the side of caution. With greater experience of

the regime, and additional guidance from the OPC, is it hoped that a more consistent approach to notification and serious harm thresholds will be developed, leading to greater certainty about when notification is required.

It's also possible that the OPC will look to take a more hands-on approach in monitoring breach reporting and calling out instances where it considers reporting obligations haven't been met. Based on the OPC's report, ensuring that breaches are reported to the OPC within 72 hours, and that affected individuals are notified, may be near the top of the OPC's watch-list for 2022.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659