What's in a name?

Allan Yeoman

28 April 2017

Enforcement powers and the Naming Policy under New Zealand's Privacy Act

New Zealand's Privacy Act provides a number of enforcement options to deal with information privacy breaches by organisations holding and using personal information (referred to in the Act as 'agencies'). Those powers have not, however, changed significantly since the Act first received royal assent on 17 May 1993. In the meantime, the internet, social media platforms, smartphones, big data and vast customer databases have been behind an astronomical increase in the scale and sensitivity of personal information collected and used. With that, of course, comes an increased risk of misuse and likelihood of harm.

While reform has been on the New Zealand legislative agenda for some time, the recently introduced 'Naming Policy' provides New Zealand's Privacy Commissioner with a useful (if interim) stick with which to wave at transgressors of the Act's Privacy Principles.

Status quo – the Act, the role of the Privacy Commissioner and the Human Rights Review Tribunal

The Privacy Act was enacted to promote and protect individual privacy, establish principles with respect to the collection, use and disclosure of personal information, and appoint the Privacy Commissioner.

However, the Commissioner's role is not, and has never been, focused on enforcement. The Office of the Privacy Commissioner is instead charged with promoting education about privacy principles, monitoring legislation, and issuing codes of practice specific to particular types of information or information processing.

The Commissioner also acts as a mediator of sorts, receiving and hearing complaints from those that feel that their privacy has been interfered with in some way. The Commissioner may also commence an investigation on their own initiative (known as an 'own motion investigation'). When presented with a complaint, the Commissioner will investigate the situation and act as a conciliator between the individual(s) concerned and the agency alleged to have breached the Act. The majority of complaints made to the Privacy Commissioner are resolved or settled in this way.

However, the Commissioner has no statutory powers to award a complainant compensation for breaches of the Act, or to order apologies or changes in practice. For complaints to be taken any further, they need to be referred or appealed to the Human Rights Review Tribunal, a specialist forum established under the Human Rights Act 1993 (the Tribunal). There are two routes that a privacy-related complaint can take to reach the Tribunal: the Commissioner may refer the matter to the Tribunal, or the complainant can take the matter there directly. The decision of the Tribunal on a Privacy Act complaint is legally binding, and the Tribunal is able to award a variety of remedies. These include:

- declaring that the action of the defendant is an interference with the privacy of an individual
- awarding damages of up to NZ$200,000
- issuing an order that restrains the defendant from continuing or repeating the interference with privacy,

and other relief as it sees fit.

The Tribunal's highest award to date was for NZ$168,000 in 2015. The case (which became known as the 'Facebook Cake Case' [1]) arose from an employment dispute in which the complainant shared privately to friends over Facebook photos of a cake that she had decorated with obscenities referencing the complainant's former employer. Having heard about the cake, a senior manager of the employer pressured one of the complainant's friends (and former colleagues) to show them the photo, and then circulated the image widely amongst the company, its senior staff and recruitment agencies in the region together with a warning that the complainant should not be hired.

The Tribunal determined that the employer's conduct was a breach of one of the more fundamental privacy principles in the Act, preventing disclosure of information for purposes other than for which it was originally collected. The Tribunal awarded damages as compensation for humiliation, loss of dignity, injury to feelings and loss of income. Prior to the Facebook Cake Case, the highest award had been NZ$40,000 in the 2003 case *Hamilton v The Deanery 2000 Limited* [2],

where a treatment clinic disclosed sensitive personal information to immigration officials. The shift in quantum of damages indicates in part an increased concern with the potential seriousness of breaches in the current digital climate.

The introduction of the Naming Policy

In December 2014, the Naming Policy came into effect. Introduced by the Commissioner, the Naming Policy outlines the Commissioner's practice of naming agencies that have been found to have breached the information privacy principles in the Act.

In developing the policy, the Privacy Commissioner stated, "*We think it is time to 'name names' where it is warranted. Our view is that in certain circumstances, the Privacy Act is better served by revealing the organisations that have breached the law.*" Naming can occur in a number of ways, including through the publication of the Commissioner's case notes and associated media releases; annual reporting; formal reports to Ministers or Parliamentary committees; and publication of open letters calling upon agencies named in media reports to explain their actions.

The Naming Policy does not mean that all agencies that breach the privacy principles will automatically be named. Rather, the policy sets out the factors that the Commissioner will take into account in deciding whether to name an agency. Those factors include the seriousness of the breach, the number of people affected, whether there have been repeated breaches, and whether the agency has demonstrated an unwillingness to comply with the law. A key consideration will also be whether, in the circumstances, the public interest would benefit from identification of the agency, due to its deterrent effect, educative purpose, or other reasons.

The road to reform

Resorting to naming non-compliant agencies has been seen by some as a sign of the Commissioner's frustration at the lack of effectiveness of the Act's current enforcement framework, and the Government's delays in introducing a new Privacy Bill to replace and modernise the Act.

In 2011, the New Zealand Law Commission (NZLC) published a detailed report on the Privacy Act, including a number of suggested areas for reform. Near the top of the NZLC's list were stronger enforcement powers for the Commissioner.

Three years later, in 2014, the Government responded to the NZLC's review of the Act, by acknowledging that privacy related risks had changed considerably since the Act was first passed in 1993, and particularly in recent times. Technological advancements in the way in which personal information is captured, stored, and shared by both public and private sector agencies (within and across borders) have led to increased demands on the Commissioner, growing concerns about private sector privacy practices, a proliferation of underdeveloped public sector privacy practices, a loss of public trust in agencies, and continuing privacy breaches – along with an increase in the cost of, and harm that can be caused by, those breaches. In this context, the Government noted that it is socially desirable for most privacy breaches to be avoided in the first place, rather than addressing the harm caused by breaches.

The Government subsequently recommended introducing three key changes to New Zealand's privacy laws:

- **First, making notification of privacy breaches mandatory.** This is currently voluntary, though very strongly encouraged by the Commissioner. The Government's proposal would introduce a two-tier regime, requiring notification to the Commissioner for 'material' breaches, and notification to both the Commissioner and the affected individuals when there is a real risk of harm. This change would also, of course, bring New Zealand closer into line with a number of comparable jurisdictions where mandatory breach notification has been implemented in recent years.
- **Second, the Government called for the Commissioner to have greater own motion investigative powers.** This would strengthen the Commissioner's existing powers to investigate possible breaches, and increase the penalty for non-compliance with requests for information from the Commissioner.
- **Finally, it was recommended that the Commissioner be given power to issue compliance notices** for privacy breaches as a result of a complaint, own motion inquiry, data breach notification or other avenue.

Although the Government rejected the introduction of fines, it noted that its position on fines was out of step with enforcement practices elsewhere, and conceded that the use of fines may become appropriate if guidance and early intervention alone are not effective.

On 3 February 2017, the Commissioner released six recommendations for reform of the Act, as part of his statutory mandate under section 26 of the Act to review and report back to the Government on the Act's operation. The Commissioner noted that rapid changes in technology and data science, and significant developments internationally (particularly the EU General Data Protection Regulation) - even since the Government's 2014 response - necessitate further matters of reform.

The Commissioner's recommendations relating to enforcement are set out below:

- **Granting the Commissioner the ability to require agencies to demonstrate their compliance with the Act**

and their privacy management plans. The Commissioner considers this is a necessary measure for systemic issues to be identified and addressed. It would also serve to complement the mandatory breach notification obligation and the Commissioner's proposed compliance notice power. The power would allow the Commissioner to require an agency to demonstrate its ongoing compliance by: (a) establishing a privacy management programme, (b) requiring a report to the Commissioner on steps taken to achieve compliance with that requirement, and (c) publicly reporting on its position with regard to its privacy management programme.

- **Introducing new civil penalties on application to the High Court for serious privacy breaches (up to NZ$100,000 for individuals and up to NZ$1 million for a body corporate).** Those levels would be more consistent with Australian law (among others) and comparable New Zealand laws (eg, the Unsolicited Electronic Messages Act 2007).
- **Narrowing the defences available for obstructing, or failing to comply with the requirements of, the Privacy Commissioner**. The Commissioner noted his experience of agencies finding it relatively easy to defend themselves against charges of obstructing or hindering the Commissioner's investigations breaches of the Act, or failing to comply with the Commissioner's lawful requirements, by relying on a 'reasonable excuse' defence contained in the Act.

The Commissioner's report and recommendations will be taken into account as part of the Government's proposed modernisation of the Privacy Act, a draft of which is expected later this year. However, with a general election to be held in September, there is every chance that privacy law reform will slip further down the Government's list of priorities. In the meantime, the Naming Policy offers the Commissioner a useful tool to encourage compliance with the Act - particularly for those agencies for whom reputational and brand impact focus the mind as effectively as legal or financial remedies.

This article was first published in the April 2017 edition of Data Protection Leader.

[1] *Hammond v Credit Union Baywide* [2015] NZHRRT 6

[2] (29 August 2003) HRRT 36/02, Decision No 28/03

Auckland

PwC Tower
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