

Lessons from recent PRIVACY VIOLATIONS

News of data security breaches at major organisations that reveal thousands of individuals' personal information is not uncommon these days. Lyn Nicholson discusses the importance of privacy impact assessments to mitigate the risk.



Lyn Nicholson is
Special Counsel with
Holding Redlich Lawyers.

INADEQUATE SECURITY MAY BE A breach of the *Privacy Act 1988* (Cth), but the actions of customers and the media may create more havoc and opportunities for economic loss than regulator intervention, as the recent cases involving Telstra, Vodafone and Google illustrate.

Many clients may consider the *Privacy Act* and the National Privacy Principles (NPPs) innocuous, but the commercial ramifications of media reports regarding breaches of customer privacy can be significant and detrimental. Media reports have indicated Vodafone lost several hundred thousand customers as a result of its recent breach.

Prevention is always better than a disaster recovery cure. The ability to conduct a privacy impact assessment (PIA) and establish a legal due diligence defence for the treatment of personal information may also uncover weaknesses in systems that can be remedied before any breaches occur.

Privacy reform – where are we now?

The *Privacy Act 1988* (Cth) has been under review by the federal government

since January 2006. A wide consultative process was undertaken by the Australian Law Reform Commission (ALRC) and in 2008 a final report, *For Your Information*, was released.¹ The report was the largest in ALRC history and contained 295 recommendations.

In order to deal with all the recommendations, the federal government divided its response into two stages. In 2009, the government provided its response to stage 1 and, in 2010, exposure draft legislation dealing with credit reporting and the proposed new Australian Privacy Principles (APPs) was released. The exposure draft legislation has been subject to a senate committee review and its 15 June report recommends the proposed APPs be streamlined and simplified.

There is no date for the federal government's response to some of the more newsworthy recommendations in the second stage, including the introduction of a statutory cause of action for serious invasions of privacy and a mandatory notification for serious breach regime.

Why is privacy relevant?

The *Privacy Act* regulates how businesses in Australia deal with personal information and affects all organisations collecting it. Personal information is defined as being "information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion".²

For businesses that operate in the credit reporting, credit provision or health space, there are additional rules that apply. For other organisations, whose

annual turnover is in excess of \$3 million, the main application of the *Privacy Act* is the requirement to comply with the NPPs.

One of the ALRC's proposals was to remove the small business exemption for businesses with turnover under \$3 million and require them to also comply with the NPPs. There are 10 NPPs and they cover the following issues in relation to personal information:

1. Collection
2. Use and disclosure
3. Data quality
4. Data security
5. Openness
6. Access and correction
7. Identifiers
8. Anonymity
9. Transborder data flows
10. Sensitive information.

Powers of the Privacy Commissioner

The powers of the Privacy Commissioner (the Commissioner), whose office has recently been merged into the Office of the Information Commissioner (OAIC), in relation to enforcement of the NPPs are somewhat limited.

Unlike the Australian Securities and Investments Commission (ASIC) which can impose fines and place banning orders on individuals, or the Australian Competition and Consumer Commission (ACCC) which can impose significant fines, the Commissioner can investigate complaints from individuals and seek to settle those complaints, conduct an own-motion investigation into a suspected breach of privacy (where it has wide powers to obtain documents), and make public interest deter-



ILLUSTRATION: DEAN GORISSEN

minations in relation to particular applications of the *Privacy Act*. There is, however, no current ability to impose fines or banning orders for breach of the NPPs.

Telstra and breach notification

Recently the Commissioner published the results of its own-motion investigation of a privacy breach by Telstra Corporation Limited in late 2008.

Telstra was undertaking a mail-out to fixed-line customers when it became aware of a mailing list error. As soon as it became aware of the error, Telstra stopped the mail-out, commenced an investigation, and identified affected customers and alerted them to the incident. The error involved 60,300 incorrectly addressed letters being sent. Of these, 26 per cent were returned to the mail house.

The Privacy Commissioner's investigation found that:

- Telstra had breached NPP 2. This is because the incorrectly addressed letters identified that named individuals had an association with Telstra.
- Telstra had not breached NPP 4. This principle requires that an organisation take reasonable steps to protect personal information from misuse, loss or unauthorised access. The investigation concluded that the breach occurred despite Telstra having in place:
 - an agreement with the mail house cover-

ing privacy and confidentiality;

- conducting PIAs at the outset of mail-out initiatives;
- a formal approval process; and
- quality control procedures for staff handling personal information.

The Commissioner noted a number of the positive actions Telstra took on becoming aware of the breach, including notifying customers in accordance with the OAIC Guide to handling personal information security breaches.⁴

While there is currently no mandatory requirement to notify individuals of a privacy breach in Australia as there are in a number of other jurisdictions, any organisation that has breached privacy laws should comply with the OAIC Guide as best practice.

The Google breach

While Google was taking pictures for its street view mapping service over a number of years, it was also collecting unsecured wireless network data. Google did this not only in Australia, but in other countries. When it was first reported in 2010, it was dubbed by the then Federal Communications Minister Stephen Conroy as "the greatest single breach of privacy in history".

"[Vodafone's] use of shared login IDs reduced the effectiveness of audit trails to monitor access control."

The Australian Federal Police (AFP) investigated whether Google had breached telecommunications laws and whether it was possible to pursue criminal charges. In December 2010, the AFP concluded that while Google's activities may have constituted a breach of the *Telecommunications (Interception and Access) Act 1979* (Cth), the evidence and the difficulty of prosecuting a case meant that the police were not going to pursue the matter further.

In coming to this decision, the AFP also took into account the undertakings that Google had given to the Commissioner to prevent similar events occurring in the future. The Commissioner conducted an investigation into the Google street view data collection and, in July 2010, obtained from Google quite an extensive undertaking.

Google's undertaking

The Commissioner found that the collection of the personal information by Google would have breached the *Privacy Act* and the undertaking involved four key steps:

- publishing an apology to Australians on Google's official Australian blog in relation to the collection of the unsecured wi-fi data;
- conducting a PIA on any new street view data collection activities in Australia that included personal information;
- providing a copy of the PIAs to the Commissioner; and
- regularly consulting with the Commissioner about personal data collection activities arising from significant product launches by Google in Australia.

The undertaking was to last for three years and the Commissioner noted that it would be reviewed following any reforms to the *Privacy Act*. It was a significant achievement, given that the Commissioner had no strict legal powers to enforce sanctions.

A large and important aspect of the undertaking related to conducting a PIA. The Commissioner has published a Privacy Impact Assessment Guide³ for organisations, which might be considered "best practice" in reviewing whether new products and services comply with privacy laws. It is a rigorous process to conduct and includes taking into account views of stakeholders. For any commer-

cial corporation, it is a significant issue as it involves consideration of commercial practices from a broader perspective.

For Google to provide a copy of the PIA to the Commissioner is, we consider, a significant step. It is an undertaking that would not have been given lightly and means Google is sharing, in a very transparent way, its approach to privacy with the Commissioner. This might allow the Commissioner to open an "own motion" investigation in relation to Google's activities if it considered the assessment had been conducted in such a way as to not satisfy the Commissioner's concerns.

Recommendation

For Australian businesses, the case raises the prospect of positive documentation of privacy compliance by conducting a PIA review. In the event of an investigation by the Commissioner, an organisation's PIA can be reasonably argued as a due diligence defence under the law where there is uncertainty.

We suggest that companies dealing in significant personal information consider undertaking some form of PIA for each new product or service that uses personal information as a way to test compliance and also as a risk management tool.

Vodafone

In January 2011, there were substantial reports in the *Sydney Morning Herald* in relation to alleged breaches of the *Privacy Act* by Vodafone. In particular, the allegations were that significant numbers of customer records were publicly available and accessible on Vodafone's website and only protected by single passwords that changed every three months.

The consequences of the media reports, apart from being damaging to Vodafone, were that the telecommunications giant commenced its own investigation into the allegations to determine whether in fact they were true and, if so, what it could do to protect its position.

Vodafone's internal investigation established that customer information was not, and had not been, publicly available on the internet or via its website but also provided less positive findings.

In particular, Vodafone found that its technology and login ID and password systems were not as robust as they could have been and, as a result, a small number of staff may have breached internal policies relating to the appropriate use of login IDs and passwords.

Vodafone implemented a number of additional security measures as a result of the internal investigation, including ensuring that authorised dealers and employees were granted access through a secure web portal and via secure login IDs and passwords.

Stores and dealerships were also issued

with unique store login IDs to be used in conjunction with a store password to further protect security.

The tiered access system was reviewed, limiting the number of persons who had access to more detailed information and reducing the scope of some of the personal information made available at the basic access level.

Vodafone liaised closely with the Commissioner during the course of its investigation and shared its results with the Commissioner. The Commissioner undertook its own review and while it found no personal information had been disclosed in breach of NPP 2, Vodafone did violate NPP 4 which requires it to

- weekend of the reports to be reverified and obtain new passwords;
- commencing an internal investigation;
- commencing an internal review of IT security and customer protection control;
- sending a bulletin to retail stores and dealers confirming exactly what had happened and correcting the inaccurate media reports. In addition, the bulletins reminded staff of their obligations in relation to unauthorised access;
- issuing a statement to the public;
- reviewing its IT security, including which users required which level of access and issuing individual login IDs for retail stores and dealers; and
- establishing a privacy hotline which enabled concerned customers to contact Vodafone and imposing a requirement on all retail stores to reset their passwords on a daily basis until new procedures were implemented.

Vodafone agreed with the Commissioner to undertake to make a number of changes to its systems. For business confidentiality and security reasons, those were not published as part of the Commissioner's report.



"Google is sharing, in a very transparent way, its approach to privacy with the Commissioner."

take reasonable steps to protect personal information from misuse and loss or from unauthorised access, modification or disclosure.

In its report, the Commissioner made a number of statements about what measures organisations could put in place to ensure they complied with NPP 4. These include:

- physical security measures;
- computer and network security;
- communication security, such as protection of emails from unauthorised interception; and
- security protocols to regulate the access of employees and others.

The Commissioner took the view that organisations need to be assessed in accordance with their own particular situation, and each organisation needed to consider a range of risk mitigation measures, including having appropriate IT security settings which conform to Australian standards. It noted that as Vodafone's business model included licensed dealerships, rather than company-owned stores exclusively, there were additional underlying security risks. Their use of shared login IDs reduced the effectiveness of audit trails to monitor access control.

The Commissioner formed the view that Vodafone had breached NPP 4 but had taken steps to resolve the situation as a matter of damage control and reputation management once the media reports broke. The steps it took included:

- immediately suspending passwords and requiring retail stores and dealers to contact the Vodafone helpdesk on the

A statutory cause of action Where are we in 2011?

FOLLOWING THE *NEWS OF THE WORLD* phone-hacking scandal in the UK, the Federal Minister for Privacy, Brendan O'Connor, issued a July press release on the topic of a right to privacy. Minister O'Connor's response was to state that a public issues paper will be issued shortly, canvassing the prospect of introducing a statutory right to privacy.

In the release he noted: "Privacy is emerging as a defining issue of the modern era, especially as new technology provides more opportunities for communication, but also new challenges to privacy."

While the Minister acknowledged the 2008 Australian Law Reform Commission (ALRC) report *For Your Information* and

its proposal to introduce a statutory right of privacy, he considered more public consultation necessary.

The *News of the World* phone-hacking scandal focuses on privacy in the context of media and public figures but it is a narrow one in comparison with the broader issues canvassed by the ALRC in its report.

Consider, by way of contrast, the media report on 16 July of details of a privacy breach at Australia's largest drug and alcohol testing company. In that case, the company had not properly secured the names and addresses of its customers, including those ordering paternity tests which were accessible via a Google search. Google provides companies with

guidelines on how to exclude data from its searches but the company did not follow them.

The Office of the Australian Information Commissioner (OAIC) is now investigating the claims. While this scenario has no media or celebrity focus, it is an example of the types of breaches the ALRC considered.

Chapter 74 of the ALRC report considered the best ways of protecting an individual's right to privacy, including canvassing the potential operation of statutory and/or common law models, and the practice in other jurisdictions (see below). It noted that since 1980, Australia has been a signatory to the International Covenant on

Civil and Political Rights, which recognises a right to personal privacy.

In addition, the ALRC had undertaken broad consultation and its report stated: "there was strong support for the enactment of a statutory cause of action for a serious invasion of privacy" (at 78.45).

Interestingly, the issues canvassed by the ALRC focused more on how the cause of action should be framed. Any further discussion should therefore focus not on whether there is a cause of action but how the scope of a breach giving rise to a cause of action should be framed.

Given changing views on what constitutes privacy, this would seem to be the challenge.

ALRC recommendations

Recommendation 74-1

Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, a serious invasion of privacy may occur where:

- there has been an interference with an individual's home or family life;

- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or
- sensitive facts relating to an individual's private life have been disclosed.

Recommendation 74-2

Federal legislation should provide that, for the purpose of establishing liability under the statutory cause of action for invasion of privacy, a claimant must show that in the circumstances:

- there is a reasonable expectation of privacy; and
- the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In determining whether an individual's privacy has been invaded for the purpose of establishing the cause of action, the court must take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression). □

ENDNOTES

1. www.alrc.gov.au/publications/report-108.
2. *Privacy Act*, s.6.
3. www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.pdf.
4. www.privacy.gov.au/materials/types/download/8628/6478.