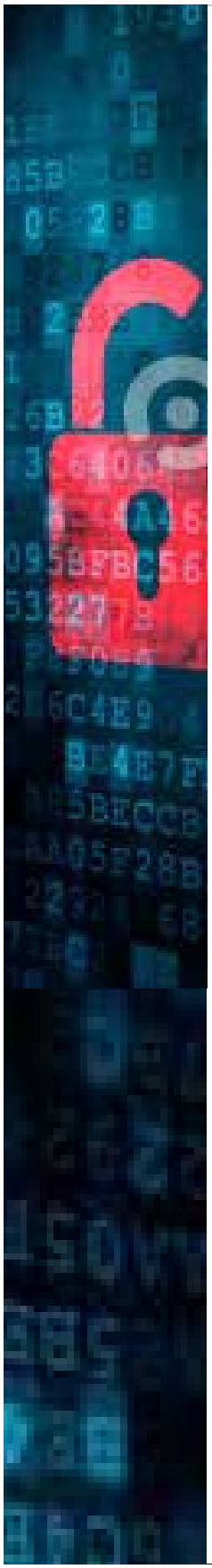

CYBER RISK AND PRIVACY: THE LEGAL VIEW

The current boom in cyber insurance policies is at least partly due to new cyber privacy laws being enacted in March. **Andrew Moore, Jane O'Neill** and **Jack Geng** investigate the new legal landscape

As Australian commentators continue to debate the relative merits of mandatory reporting of serious data breaches, the recent hacking attack on US retailing giant Target serves as a timely reminder of the risks faced by many businesses in the digital age.

On 19 December 2013, Target announced it was the victim of a coordinated and systematic hacking attack carried out on its computer network between 27 November 2013 and 15 December 2013. Target has subsequently confirmed that the attack compromised the credit and debit card details of up to 70 million individual customers.

The potential losses faced by Target are enormous with reports indicating that at least two separate class actions have been commenced by customers.

In the meantime, many businesses probably breathed a sigh of relief when mandatory reporting of serious data breaches was not incorporated during the recent tranche of privacy reforms in Australia. Any celebrations are, however, likely to be premature, as businesses come to terms with the full effects of reforms to the Privacy Act 1988 (Cth) (the Privacy Act).

THE PRIVACY ACT

On 12 March 2014, the newly amended Privacy Act comes into operation through the Privacy Amendment (Enhancing Privacy Protection) Act 2012. These amendments herald two significant changes for all affected businesses, including:

- Imposing additional regulatory obligations, and
- Conferring significant enforcement powers on the Office of the Australian Information Commissioner (the Commissioner).

The amended Privacy Act incorporates the newly created Australian Privacy Principles, which provide significant privacy enhancements for the collection, handling and use of private information by businesses.

The main changes include:

- Restricting the purpose and manner in which private information can be collected and used by a business, including the requirement that any private information collected must be reasonably necessary to the business' functions or activities
- Unless exempted, any sensitive information must be obtained with the express consent of the individual
- Taking reasonable steps to notify the relevant individual that their personal information is being collected, and to ensure the private information being collected is accurate and accessible by the relevant individual, and
- Taking reasonable steps to protect any personal information held by the business.

These changes apply to businesses with an annual turnover of $3m or more, and to any prescribed businesses as defined under the Privacy Act, such as those providing health services.

The Commissioner has also been granted significant powers under the Privacy Act to:

- Investigate any complaints received in relation to breaches of the Privacy Act, or to investigate any breaches on its own initiative
- Accept enforceable undertakings from businesses against further breaches of the Privacy Act, and
- Impose civil penalties for serious or repeated breaches, including fines of up to $1.7m for businesses and $340,000 for any individuals.

The Commissioner will maintain its pre-existing power to award monetary compensation to complainants for any losses or damages as a result of any breaches (enforceable via the Federal Court or Federal Circuit Court).

Businesses should be taking steps now to ensure they have a compliant privacy policy and are aware of the changes. The consequences of failing to adequately protect customer data will be significant.

MANDATORY REPORTING

In 2013, the then Attorney General introduced the Privacy Amendment (Privacy Alerts) Bill 2013 (the Proposal). Under the Proposal, if any business believes there has been a serious data breach, it must notify the Commissioner and take reasonable steps to notify the affected individual/s.

Serious data breaches include:

- Any unauthorised access to, or disclosure of personal information (including where personal information is lost), and
- Where there is a "real risk of serious harm" to the individuals affected by the breach.

Under the Proposal, 'harm' includes harm to reputation, economic and financial harm.

The Proposal was passed by the House of Representatives, but has since lapsed in Parliament.

Despite a change in government, the issue of mandatory reporting still looms on the legislative agenda. In June 2013, the then shadow Minister for Justice indicated in principle support for the mandatory reporting:

"...the Coalition supports the broad principles in this bill [mandatory reporting]; there are still some concerns that require thorough investigation... the coalition will wait for the Senate committee's report into this bill, and we reserve the right to propose appropriate amendments".

It is clear that the Privacy Act will not include any mandatory reporting requirements, but only time will tell whether the Coalition government intends to revisit this issue.

REGULATORY AND LITIGATION RISKS

While mandatory reporting has not been introduced, businesses still face significant regulatory risks caused by data breaches as the amendments to the Privacy Act require businesses to take reasonable steps to protect any personal information and the Commissioner has the power to investigate and impose civil penalties of up to $1.7m.

The failure to notify any affected individuals of serious data breaches may also increase litigation risks for any affected businesses.

It is important to remember that had the Proposal been adopted, the obligation to notify would only be required in circumstances where there is a "real risk" that an individual may suffer serious reputational damage or suffer serious economic/financial harm. Accordingly, in circumstances where a "real risk" exists, it is likely that an individual who has suffered harm may have separate legal causes of action, and the failure to notify may simply exacerbate their losses. Whilst for large scale data breaches, the spectre of potential class action proceedings will also loom large on the horizon.

RISK MANAGEMENT

It is also important to bear in mind that, although there are no requirements for businesses to report serious data breaches to the Commissioner or to any affected individuals at this point in time, the changes to the Privacy Act most certainly increase the regulatory, reputational and litigation risks to businesses.

Due to the increasing threats emanating from data breaches, businesses need to consider appropriate risk management strategies, including holding appropriate cyber insurance cover for common first and third party liabilities for costs relating to:

- Forensic computer investigation and data recovery
- PR management
- Business interruption
- Breach notifications
- Third party losses, including settlements and judgments, and
- Defence costs, including litigation, regulatory investigation and fines.

"Cyber risk insurance is the next big thing in financial lines. In view of the increased exposure in the digital age and by virtue of reforms to the Privacy Act, it is not hard to see why"

Large-scale data losses tend to dominate media headlines, and potentially cause enormous losses for any affected businesses. However, the everyday reality of most cyber risks tends to be less spectacular, but no less real or devastating, as many small and medium businesses have discovered to their detriment.

Nevertheless, as the fallout from the Target data breach unfolds, it may be only a matter of time before we see similar large-scale data breaches in Australia. When such losses occur, any affected businesses must deal with the inevitable public backlash, and the full regulatory fall-out under the Privacy Act. IB

About the authors
Andrew Moore is a partner, **Jane O'Neill** is a senior associate and **Jack Geng** is a solicitor at Wotton + Kearney.