

Issue No. 2 October 2008

# Commercial Law Update

## Privacy law overhaul – big changes on the way

- *One set of united privacy principles applicable to both private and public sectors*
- *The end of the “small business” and “employee records” exemptions from strict privacy law compliance*
- *The compulsory reporting of major personal information security breaches*
- *A statutory right to privacy*

*These are just four of 300 recommendations in the Australian Law Reform Commission’s extensive report into Australia’s privacy laws released last month.*

### Big changes coming

Big changes are on the way to cope with advances in information collection and storage and also surveillance technologies.

The recommendations will be implemented in two phases.

The first phase - incorporating more urgent and less contentious reforms – is expected within 12-18 months. A timetable for the second phase is yet to be announced.

Although substantially amended over the last 20 years, Australia’s privacy legislative regime dates back to 1988. Unfortunately, it predates much of the technology it must regulate – making it ill-suited to emerging demands. The *Privacy Act* will, therefore, become technologically neutral to ensure its ongoing relevance.

The proposed reforms are expected to have a particular impact on a number of industries and certain business activities. Some of these are discussed below.

### Small business

The ALRC has recommended that small businesses (those with an annual turnover of less than \$3 million) cease to be exempt from privacy law compliance. In effect, this will mean that an extra 2 million businesses will need to make sure that all of the information they gather on employees and customers is



**Suzanne Harmer** Special Counsel  
**T +61 3 9321 7854**  
 sharmer@rigbycooke.com.au

## Inside

*Privacy law overhaul – big changes on the way*

Pg 1- 2

### Important Notice

*This publication contains comments of a general nature only and is provided as an information service. It is not intended to be relied upon, nor is it a substitute for specific professional advice. No responsibility can be accepted by Rigby Cooke Lawyers or the authors for loss occasioned to any person doing anything as a result of any material in this publication.*

collected, stored and used within the law or be exposed to stiff fines in the event of breach. The proposal has not been well received by stakeholder bodies and will be deferred until the second phase of reform. There is concern that this will prove to be a significant compliance burden on the small business sector.

### Employees

Another recommendation advocates the removal of the existing “employee records exemption”. This will mean that companies will have to ensure that personal information on employees is up-to-date and accurate as well as available on request for inspection by workers and is not disclosed to anyone else unless in accordance with the statute.

### Health

Most states are in the process of introducing electronic systems to manage health records. Consequently, a consistent national system has been recommended to regulate the use of these records, particularly when they are to be transferred across state borders.

The reforms will address a number of issues, including the ownership rights of patients over their medical records when a practice is sold and the regulation of information-sharing between health professionals. These changes will be some of the first to be implemented.

### Banking and finance

The report recommends reforms that will give banking and finance institutions the ability to collect far more information from current and potential customers, including:

- the number of credit products
- credit limits
- dates that the accounts were opened and closed

The recommendations have been made with a view to prescribing stricter and more responsible lending practices within the industry.

### Cross-border data flows

Measures are proposed that will regulate cross-border data flows. Australian companies who send personal information overseas will be liable for what happens to that information. This will have serious implications for companies who, for example, operate call centres or data warehouses offshore.

To avoid liability, companies will need to inform customers and obtain the customer’s consent to their personal information being sent overseas.

### Personal information security breaches

A personal information security breach occurs when personal information is subject to loss or unauthorised use, access, disclosure, copying or notification. The breach can be malicious or accidental.

Compulsory reporting of major personal information security breaches has received strong support, including from the Privacy Commissioner. The proposed changes will require the Privacy Commissioner and affected individuals to be notified if specified personal information has been accessed or disclosed without authority, and the breach posed a serious risk of harm to the individual. These recommendations will be implemented in the second phase of the reforms.

In the meantime, and seemingly in anticipation, the Privacy Commission has released a guide to handling personal information security breaches. The purpose of the guide is to help organisations develop a strategy to respond to situations where there is a security breach. Whilst notifying

individuals is not yet a requirement, the guide recommends that in some situations it may be appropriate to notify individuals where the security of their personal information has been compromised.

You can view the Guide via this link:

[Guide to handling personal information ....](#)

### Statutory right to privacy

The ALRC has recommended the creation of a new tort giving rise to a statutory cause of action for privacy breaches. An individual will be able to commence proceedings where there was a “reasonable expectation” of privacy about a matter and that privacy was invaded in a way that would seriously offend a person of “ordinary sensibilities.” It might apply to interference with home or family life, unauthorised surveillance, or disclosure of sensitive facts relating to an individual’s personal life.

Defences would be available, such as that the conduct was authorised, the disclosure was in the public interest, or privileged under the laws of defamation. It would not be a defence that the disclosed information was true.

The effect of this proposed change in the law will be felt most by the media because of the impact on the ability of news outlets to report, in particular, on the lives of celebrities and other public persons.

More information on this subject is available from Suzanne Harmer (\*) Special Counsel – contact details are shown on page 1.

*\* This Update was prepared with the assistance of Lucy Fitzpatrick, Articled Clerk.*

#### To unsubscribe from this publication

If you do not wish to receive publications of this type from us in the future, please notify us by one of the following methods:

- Send an email to [marketing@rigbycooke.com.au](mailto:marketing@rigbycooke.com.au)
- Send a fax message to “Attention: Rigby Cooke Marketing” on fax number +61 3 9321 7900
- Send a letter to “Attention: Rigby Cooke Marketing”, GPO Box 4767UU, Melbourne Vic 3001

Your request to remove you as a subscriber should include the word “unsubscribe” and your full email address to allow us to correctly identify your removal from our lists.

#### Reprinting articles

Articles in this publication may be reproduced in whole or in part, provided that appropriate recognition is given to the author and the firm, and prior approval is obtained.

To obtain approval, please contact Rigby Cooke on +61 3 9321 7852 or email [marketing@rigbycooke.com.au](mailto:marketing@rigbycooke.com.au).

**rigbycooke | lawyers**

Level 13, 469 La Trobe Street  
Melbourne Vic 3000  
T 61 3 9321 7888  
F 61 3 9321 7900  
[www.rigbycooke.com.au](http://www.rigbycooke.com.au)