

18 April 2008

Privacy Law E-alert

Owning up to leaving the files on the back seat of the car: *draft voluntary information security breach notification guide*

On 15 April the Office of the Privacy commissioner released a consultation paper seeking comments on the draft voluntary information security breach notification guide released on the same day. The guide has been prepared partly in response to recent incidents in the UK and USA when large amounts of sensitive information were lost, stolen or otherwise unlawfully disclosed.

National Privacy Principle 4.1 ("**NPP 4.1**") requires private sector organisations to take reasonable steps to protect personal information from misuse, loss and unauthorised access, modifications or disclosure. Situations where personal information collected by an organisation is lost, stolen or otherwise unlawfully disclosed suggest that the organisation is not complying with NPP 4.1.

Although the *Privacy Act* does not require organisations to report incidents to the Privacy Commissioner when information is lost, stolen or unlawfully accessed or disclosed, the Privacy Commissioner considers that voluntary breach notification is good privacy practice. In addition, while voluntary notification will not cure any breach of NPP 4.1, it may allow the organisation to manage the consequences of the breach and, in particular, mitigate the damage to its reputation.

The way in which the Privacy Commissioner recommends that an organisation should respond to an information security breach is similar to the way in which an organisation would respond to a breach of any of its management policies. The advantage of the guide is that it has a privacy focus which should facilitate an appropriate response to information security breaches.

While the guide focuses on the response to information security breaches, it is a timely reminder of the importance of organisations conducting periodic privacy audits and reviewing their privacy policies and procedures to ensure that they accurately reflect how the organisation manages personal information. It is likely that many organisations have privacy policies that were adopted when they first became subject to the NPPs. Our understanding of the extent of the obligations imposed on private sector organisations has grown considerably since that time.

Comments on the draft are invited by 16 June 2008.

Copies of the guide are available at <http://www.privacy.gov.au/business/consultations/index.html> or from us.

If you have any questions about the guide or the way in which your organisation manages personal information please contact:

John Kell +61 2 9391 3163 jkell@hunthunt.com.au

Catherine Logan +61 2 9391 3267 clogan@hunthunt.com.au

Disclaimer: The information contained in this e-alert is not advice and should not be relied upon as legal advice. Hunt & Hunt recommends that if you have a matter that is legal, or has legal implications, you consult with your legal adviser. If you no longer wish to receive this e-alert or any other publication from Hunt & Hunt, please email us at unsubscribe@hunthunt.com.au.