



**BUCHANAN LAW**  
Intellectual Property and Technology

**23 April 2008**

[www.buchananlaw.com.au](http://www.buchananlaw.com.au)

## CLIENT BULLETIN

*The Office of the Privacy Commissioner has invited submissions on the Draft Voluntary Information Security Breach Notification Guide which encourages organisations to consider notifying individuals when the security of their personal information has been breached.*

Office Buchanan Law Pty Ltd  
Level 3,  
54 Marcus Clarke Street,  
Canberra ACT 2601

Postal GPO Box 579,  
Canberra ACT 2601

Tel 02 6221 9555

Fax 02 6162 3202

Email [info@buchananlaw.com.au](mailto:info@buchananlaw.com.au)

ABN 55 121 082 899

## **The Draft Voluntary Information Security Breach Notification Guide**

Arising from a recommendation in the Australian Law Reform Commission's Discussion Paper 72, *Review of Australian Privacy Law*, released in September 2007, the Office of the Privacy Commissioner (**OPC**) last week released the Draft Voluntary Information Security Breach Notification Guide (**the Guide**).

The Guide has been produced to assist private and government organisations in preventing and responding to information security breaches. The Guide states that an information security breach occurs when personal information is exposed to unauthorised access, use, disclosure or modification as a result of a breach of an agency's or organisation's information security.<sup>1</sup>

Compliance with the Guide, which draws on breach notification procedures applied in New Zealand and Canada, is voluntary. This falls short of the ALRC's recommendation that breach notification be mandatory. Furthermore, the Guide does not stipulate any consequences for an organisation or agency that has opted to comply with the Guide but has contravened one or more of its principles.

### **Responding to a breach**

Compliance with the Guide does not mean that an organisation must notify individuals of all information security breaches. Rather the Guide recommends that an organisation conduct a risk assessment to determine if the breach poses a real risk of serious harm to the affected individuals and, if such risks are present, the Guide recommends notifying the individual(s).

This process is divided out into four steps:

1. Contain the breach and do a preliminary assessment
2. Evaluate the risks associated with the breach
3. Consider notification
4. Prevent future breaches

The Guide recognises that in practice the line between these four steps is often blurred but offers guidance on what the OPC regards as "good privacy practice".

---

<sup>1</sup> Draft Voluntary Information Security Breach Notification Guide April 2008; Part B, Chapter 4, page 14



The question of whether a breach is likely to give rise to a risk of harm to the relevant individual is to be decided by the organisation who is responsible (directly or indirectly) for the breach, not the individual to whom the information relates. This is likely to cause some controversy amongst privacy advocacy groups.

The Guide gives emphasis to identity fraud, suggesting that a primary objective in developing this document was the minimisation of identity theft resulting from information security breaches. Some may argue that the emphasis on identity fraud as a consequence of lax privacy security practices has resulted in a document that focuses on the relevant organisation's assessment of a perceived risk to an individual, as opposed to the real and identifiable risks known to the relevant individual.

The OPC has correctly labelled this document a "guide". From a technical perspective it does not set out any specific signposts and acknowledges that "the main challenge is to determine what circumstances justify notification".<sup>2</sup> It does however draw attention to factors to be considered by organisations in deciding whether to notify an individual of a breach, including the sensitivity of the relevant information, the nature and context of the personal information, the potential use (or misuse) of that information, the source of the breach and the steps already taken by the organisation to mitigate damage.

Although some organisations are likely to find the Guide to be inconclusive at times, there is value to this document. Any organisation that deals with personal information in any shape or form will find this Guide useful in consolidating its privacy practices and in deciphering certain obligations under the Privacy Act.

#### **OPC Consultation**

The OPC is seeking comments by 16 June 2008 on the Draft Guide. Buchanan Law would be pleased to assist with the drafting of submissions or advising you more generally in relation to privacy obligations.

#### **Contact us**

Buchanan Law Pty Ltd  
Level 3, 54 Marcus Clarke St.  
Canberra ACT 2601

T + 61 2 6221 9555  
F + 61 2 6162 3202  
[www.buchananlaw.com.au](http://www.buchananlaw.com.au)

<b>Scott Buchanan, Director</b> <a href="mailto:scott@buchananlaw.com.au">scott@buchananlaw.com.au</a> M 0408 197 181	<b>Shaun Creighton, Senior Lawyer</b> <a href="mailto:shaun@buchananlaw.com.au">shaun@buchananlaw.com.au</a> M 0423 120 483
<b>Gary Lea, Associate</b> <a href="mailto:gary@buchananlaw.com.au">gary@buchananlaw.com.au</a>	<b>Monica Dawes, Lawyer</b> <a href="mailto:monica@buchananlaw.com.au">monica@buchananlaw.com.au</a> M 0438 455 139

Copyright & Disclaimer

© Buchanan Law Pty Ltd 2008

This newsletter is for general information purposes only and must not be relied upon as legal advice.

2

---

<sup>2</sup> Draft Voluntary Information Security Breach Notification Guide April 2008; Part B, Chapter 6, page 18-19