benchtv
a benchmark production

Précis Paper

The Privacy Amendments
(Notifiable Data Breaches) Act 2017 (Cth)

A discussion on the new mandatory data breach notification scheme in Australia together with the associated amendments to *The Privacy Act* and the effects that these will have on businesses and practitioners.

Discussion includes

- **What is a mandatory data breach notification scheme?**
- **Which data breaches are notifiable?**
- **Are there any exemptions to notification?**
- **Which businesses will be subject to the mandatory data breach notification scheme?**
- **What instigated the introduction of this legislation?**
- **Who is responsible for data breaches involving jointly held information?**
- **Risk management for businesses**
- **Notification of a data breach**
- **Enforcement and penalties**
- **Is the scheme effective?**
- **Takeaways for legal practitioners**

Précis Paper

The Privacy Amendments (Notifiable Date Breaches) Act 2017 (Cth)

1. **In this edition of BenchTV, Charles Sweeney (Partner – Cooper Grace Ward, Brisbane) and Adelaide Hayes (Associate – Cooper Grace Ward, Brisbane) discuss the new mandatory data breach notification scheme in Australia together with the associated amendments to *The Privacy Act* and the effects that these will have on businesses and practitioners.**

What is a mandatory data breach notification scheme?

2. **The new scheme was introduced pursuant to legislative amendments to the *Privacy Act 1988* (Cth) ("Privacy Act"), namely *The Privacy Amendments (Notifiable Data Breaches) Act 2017* (Cth) ("Amending Act")**
3. **These amendments commenced on 22 February, 2018 and require certain businesses to notify the Privacy Commissioner and affected individuals if an eligible data breach occurs.**
4. **A data breach may occur if there is any loss or interference with personal information.**
5. **Personal information is any information or an opinion about an identified individual or an identifiable individual.**
6. **A data breach occurs if any personal information is lost or subjected to any unauthorised use, disclosure, loss or interference.**
7. **For example, this can occur when an employee leaves a device on public transport or when a person sends an email containing personal information to the wrong recipient, as well as when systems are hacked or someone engages in fraud to improperly gain personal information.**

Which data breaches are notifiable?

8. **The mandatory data breach notification scheme only applies to data breaches that are likely to result in serious harm to the individual whose information has been compromised.**
9. **Serious harm is not defined by the Amending Act but is intended to encompass a broad spectrum of harms, such as physical, psychological and financial harms.**
10. **The Amending Act sets out some of the considerations for determining whether a data breach is likely to or will result in serious harm. These include the type of information included in the data breach, circumstances of the breach (for example, was it malicious or accidental?) and the nature of the harm that may result.**

Are there any exemptions to notification?

11. **There are some limited business specific circumstances that provide exemptions to notification. However, the most notable exemption is the 'remedial action' exemption.**
12. **If a business suffers a data breach, but takes action afterwards that would lead a reasonable person to conclude that the data breach is no longer likely to cause serious harm to the individuals whose personal information has been compromised, then the data breach is taken to never have been eligible for notification and the business does not need to notify the Privacy Commissioner or the affected individuals.**
13. **The types of remedial action that will be appropriate depend on the circumstances of the breach. For example, if a mobile phone containing personal information is lost, one form of remedial action is to remotely delete the information before personal information on the phone is accessed. If these measures are taken quickly and the phone has password protections such that it can be confident that the information was deleted prior to being accessed, the business will not be required not to notify an eligible data breach.**
14. **Another key example of a data breach occurs when a person sends an email to an unintended recipient. If the sender contacts the unintended recipient immediately and the recipient agrees to delete the email, this may also constitute effective remedial action.**

Which businesses will be subject to the mandatory data breach notification scheme?

15. **The Amending Act will affect any business that is usually subject to the Privacy Act. This includes businesses that have an annual turnover of $3,000,000 or more), and irrespective of turnover, health service providers, any business that is required to report to AUSTRAC, operates a Residential Tenancy database, provides services under Commonwealth Contracts or trades in personal information.**
16. **In addition to this, the Amending Act will apply in a restricted sense to some special categories of businesses, including credit providers, credit reporting bodies and tax file number recipients. A credit provider includes banks, credit card issuers, other financial institutions, businesses substantially dealing in the provision of credit and any business that provides deferred terms of payment for at least 7 days such as some accounting firms and law firms.**

What instigated the introduction of this legislation?

17. **The amendments to the legislation were instigated by the growing recognition around the world of the value of personal information and the volumes of sensitive information being stored by businesses.**
18. **Prior to the introduction of the Amending Act, there were limited sanctions for poor information handling practices, particularly with respect to data breaches, which was recognised as a flaw in the system.**
19. **The Amending Act has been introduced to hold businesses accountable for their information handling processes and to ensure that individuals are given notice of serious data breaches so that they can respond effectively to them and reduce the risk of harm that may be suffered as a consequence.**
20. **The Amending Act has also brought Australia into line with similar data breach reporting requirements in other jurisdictions.**

Who is responsible for a data breach involving jointly held information?

21. **Personal information will be considered to be 'jointly held' if one party has legal ownership or control of the records containing the information but one or more other parties have physical possession of the records.**
22. **The modern business outsources its technology systems and will typically host data with third party service providers that may have data centers located in numerous countries around the world. Under the Amending Act, any data breach that occurs along that supply chain will apply in respect of all businesses involved in that supply chain.**
23. **This is because all parties that jointly hold personal information will be jointly liable for any data breach in respect of that information.**
24. **Businesses that jointly hold personal information will also be jointly discharged from their obligations to assess a data breach and notify of an eligible data breach (as required) if one of the relevant businesses completes an assessment or submits a notification for the data breach.**
25. **As a result, it is important for businesses to conduct information handling due diligence when they engage third party service providers. It would also be helpful to implement defined measures for dealings with jointly held information. This may be achieved by incorporating terms into agreements with third parties, which allocate responsibilities for notification and assessment and require co-operation in the event of data breaches.**

Risk management for businesses

26. Businesses are encouraged to put preventative measures in place, prior to a data breach occurring so that they are prepared in the event of a data breach and to reduce the likelihood that they are involved in a data breach.
27. One important step to protect a business against data breaches is to improve cyber security by conducting regular software updates, upgrading password protections, requiring multi-factor authentication, encrypting information and providing regular staff training on cyber risks.
28. It is also useful for businesses to conduct regular reviews of information handling practices and appoint a privacy officer responsible for overseeing privacy compliance.
29. Other preventative measures may include:
    i. obtaining written consent to release the personal information of a client;
    ii. de-identifying information that is no longer required in the business;
    iii. using secure recycling bins and disposal units to ensure that documents cannot be accessed by unauthorized persons;
    iv. auditing physical and technological securities;
30. We also recommend that businesses implement a data breach response plan. These plans have been strongly endorsed by the Privacy Commissioner.
31. One of the requirements under the Privacy Act is that businesses need to take reasonable steps to protect the information that they hold.
32. Without having a data breach response plan, a business may find it difficult to demonstrate that it has taken reasonable steps to protect information in its custody.
33. Broadly, a data breach response plan sets out detailed procedures for 4 steps:
    i. assess;
    ii. contain;
    iii. respond; and
    iv. review.
34. The data breach response plan is an internal document which is targeted at employees of an organisation and allocates responsibilities in the event of a breach.
35. Businesses have 30 days in which to investigate and determine whether a data breach is notifiable or not, therefore it is important to have measures in place in advance to be able to respond swiftly and comply with the new laws.

<u>Notification of a data breach</u>

1. The Amending Act sets out specific issues that need to be addressed in any notification of an eligible data breach to the Privacy Commissioner or affected individuals.
2. If a business is required to notify a data breach, a written notification may be submitted to the Privacy Commissioner through the online form on the OAIC website.

3. **Generally, notifications to affected individuals should be given via the business' ordinary means of communication with that person.**
4. **Given the sensitivity of these notifications and the ramifications they can have on businesses that are notified, it is recommended that legal advice is sought prior to submitting any proposed notification.**

Enforcement and penalties

5. **The Privacy Commissioner has a broad range of enforcement powers under the Privacy Act.**
6. **The data breach notification scheme does not set out a new scheme for penalties, although the penalties have increased since the notifiable data breach regime came into force.**
7. **Generally, the Privacy Commissioner can award penalties against a non-compliant business if it is responsible for serious or repeated interferences with a person's personal information.**
8. **The difference between the previous regime and the new regime is that the new notifiable data breach regime will create more opportunities for serious or repeated interferences with personal information to arise.**
9. **For individuals, the Privacy Commissioner may impose penalties of up to $420,000 and for businesses, penalties of up to $2,100,000 may be imposed.**
10. **The Privacy Commissioner also has other powers to seek injunctions restraining a business from a certain activity, to make determinations for provisions of access and the issuance of an apology, and to seek enforceable undertakings that a business is going to do certain things going forward, such as implement response procedures and identify the privacy risks in the business.**
11. **There may also be significant commercial consequences if a business suffers a data breach, including damage to reputation, financial loss and potential contractual or tortious liability.**
12. **Data security is increasingly important to customers when considering whether or not to engage businesses for services so proper information handling is more important than ever.**

Is the scheme effective?

13. **We believe that the introduction of the scheme has been effective in highlighting the technical risks and some of the solutions to technical risks, such as multi-factorial authentication.**

14. **Reports released by the Privacy Commissioner have indicated that data breaches are extremely common and predominantly result from human error and malicious or criminal attacks.**
15. **These reports have also indicated that Health Service Providers frequently report data breaches. This is not particularly surprising due to the sensitivity of the information they hold as this may lead to a more cautious approach to notification.**
16. **Other common industry reports include the finance sector and legal, accounting and management services.**
17. **The new regime has increased business awareness of the issue of information security and handling and increased the level of investment in responding to the issue.**
18. **One risk arising from the scheme is that businesses may prematurely notify data breaches when they do not really need to. We expect that this results from a temptation to believe that notification solves the problem rather than implementing systematic changes to help prevent the occurrence of breaches in the first place.**

<u>Takeaways for legal practitioners</u>

19. **When it comes to information handling and data security, businesses need to take a holistic approach to prevention and response, taking into account the specific risk factors for their business.**
20. **This means that practitioners should work closely with their clients to prepare privacy policies, data breach response plans, third party protections and other relevant policies tailored to those business risks.**
21. **It is also clear that this is an area of steady growth in the legal market and there appears to be an emerging specialty area in privacy laws and data and cyber protection.**

BIOGRAPHY

Adelaide Hayes

Associate – Cooper Grace Ward, Brisbane

Adelaide is an associate in our corporate and commercial team with wide ranging experience in transactional and corporate advisory work such as complex mergers and acquisitions, corporate governance advice, shareholder issues and agreements and business sale and share sale transactions.

Adelaide also regularly assists clients with matters related to trade mark registration and protection, intellectual property ownership and licensing, technology, privacy, competition and consumer laws and the establishment and operation of not-for-profit and charitable organisations (and related tax advice).

Charles Sweeney

Partner – Cooper Grace Ward, Brisbane

Charles is a partner in Cooper Grace Ward's corporate and commercial group. Charles provides wide-ranging general commercial advice to clients, with particular areas of focus including corporate advisory and intellectual property / information technology.

Acting for listed and unlisted public and private clients, Charles advises across a broad range of industries, including agribusiness, financial services, technology and mining. Charles has served as a non-executive director of ASX listed companies and has practical experience of the issues faced by boards.

BIBLIOGRAPHY

Cases

***Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)**
Privacy Act 1988 (Cth)

Website

http://www.cgw.com.au/