benchtv
a benchmark production

Précis Paper

Data Breach Reporting Requirements

A discussion of the new Notifiable Data Breaches scheme that has been introduced into the *Privacy Act* 1988 (Cth).

Discussion Includes

- Personal information
- The Notifiable Data Breaches scheme
- What data breaches are caught?
- Investigating data breaches
- Exceptions to notify
- Preparation by organisations

Précis Paper

Data Breach Reporting Requirements

1. In this edition of BenchTV, Eli Fisher (Senior Associate – HWL Ebsworth, Sydney) and Ben Gulson (Associate – HWL Ebsworth, Sydney) discuss the introduction of the new Notifiable Data Breaches scheme under the *Privacy Act 1988* (Cth), what is covered by this scheme and what this means for organisations.

Personal Information

2. The new Notifiable Data Breaches scheme was introduced into the *Privacy Act 1988* (Cth) and came into effect on 22 February 2018.

3. The *Privacy Act 1988* (Cth) makes reference to personal information. Personal information is defined as information or an opinion about an identifiable person or a reasonably identifiable person. It is still considered personal information whether the information or opinion is true or not, and whether it is recorded in material form or not.

4. Common examples of personal information include an individual's name, date of birth, bank account details, address, medical records, and so on. It is essentially any information that reasonably identifies a person.

5. Personal information can relate to an individual, but it can also relate to more than one individual. There will be many examples where an individual's personal information is intertwined with other people's personal information, for example a marriage certificate will contain an individual's personal information, and the personal information of their spouse.

The Notifiable Data Breach scheme

6. The Notifiable Data Breaches scheme has been introduced into the Privacy Act 1988 (Cth) (the Act). This scheme basically introduces new obligations to both notify the Privacy Commissioner and affected individuals when an eligible data breach occurs, and conducting an assessment when you suspect that a data breach may have occurred.

7. The primary purpose of the data breach is to ensure that individuals who may have been affected by an eligible data breach are able to protect themselves as best they can. This may mean monitoring their bank accounts to ensure that no money has been taken, to make sure there has been no identity theft or the changing of passwords, etc.

8. The aim is to allow individuals and the Privacy Commissioner to assist in mitigating the negative effects of a data breach. For organisations, the idea behind having this is to enhance accountability on their part, and also to better prepare them for when things like this do happen so that they can be a part of the solution.

9. The Act refers to APP entities which includes basically every large organisation in Australia. The technical definition of an APP entity is an organisation that has an annual revenue of $3 million or more.

10. The scheme also refers to government agencies, certain small specific types of organisations such as healthcare providers and credit reporting bodies, tax file number recipients and other bodies that, for example, trade in personal information. Small businesses can also be caught by the scheme if they carry on certain types of activities, or if they are related to an APP entity.

11. However, the scheme only applies to entities and personal information holdings that are already subject to the security requirements under the Act. Acts and practices of APP entities that are exempt under the *Privacy Act 1988* (Cth) will also be exempt from the new scheme, for example employment records.

What data breaches are caught?

12. Not all data breaches are caught by the scheme. Any data breach that occurred prior to 22 February 2018, unless it is a continuing breach, will not be caught by the new Data Breach scheme.

13. For a data breach to be eligible under the scheme, there is essentially three criteria that need to be fulfilled:
    1) There needs to be an unauthorised access to, unauthorised disclosure of, or loss of, personal information.
    2) A reasonable person would conclude that serious harm could befall the individuals who are affected by the breach.
    3) You have not been able to prevent the likely risk of serious harm with remedial action.

14. An obvious example of a data breach would be a hacker breaking into a system and retrieving data from the server. An employee going through sensitive customer records without any legitimate purpose may also be considered a breach under this scheme.

15. Another example could be an employee accidentally disclosing a confidential file, perhaps by accidentally sending an email to the wrong person. An employee leaving personal

information on public transport or in a public space by accidentally leaving a phone or other device may also be a breach if that device has access to personal information, for example through emails.

16. However, just because these things take place does not necessarily mean that we are dealing with an eligible data breach that requires you to notify the Privacy Commissioner or the potentially affected individuals. Before notification you must consider whether there is a likelihood of serious harm.

17. Assessing whether there is a likelihood of serious harm is an objective assessment that is determined from the view point of a reasonable person sitting in your position with the information that you have at your disposal. It is not about whether serious harm is possible, but whether it is more probably than not.

18. The scheme helpfully sets out a non-exhaustive list of items that you would consider when you are making that assessment. For example, you should consider the types or type of personal information involved in the data breach, for example does it involve sensitive information? Health records, for example, are considered more serious than something like a name or date of birth.

19. You should also consider the circumstances of the data breach – for example, whose information is it, how many people did it affect, and what protections were in place?

20. The nature of the harm that may result from the data breach should also be considered. Serious harm is not defined in the Act, but in the context of a data breach serious harm to an individual may include physical, psychological, emotional, financial and/or reputational harm. Therefore the nature of harm that is caught by this scheme is fairly broad.

21. If you have what would otherwise be an eligible data breach, the final question is are we able to do anything to mitigate the serious harm to such an extent that you do not now need to notify the Privacy Commissioner or any affected person? For example, if a smartphone with personal information is lost, there are tools available that have the ability to wipe the device remotely so that the information cannot be accessed.

<u>Investigating data breaches</u>

22. There are two thresholds at play under the *Privacy Act 1988* (Cth):
    - Whether you have reasonable grounds to believe that an eligible data breach has taken place.

- Whether you have reasonable grounds to suspect that an eligible data breach has taken place.

23. If you believe that a breach has taken place, you must notify the Privacy Commissioner and the affected persons. However, if you reasonably suspect a breach has taken place (which is a lower threshold), then there is a different scheme in place.

24. If you have only reasonable grounds to suspect, then the obligation is to conduct an investigation to work out whether or not you, after investigation, have reasonable grounds to believe there has been a breach. You are obligated to take all reasonable steps necessary to ensure that the investigation has taken place within 30 days. How you conduct the investigation is essentially up to you.

25. The scheme applies to Australian government agencies to the extent that they are operating overseas. It also applies to any organisation that has an Australian link which could be where the organisation is carrying on business in Australia, or it has collected, or is holding, information in Australia or in an external territory of Australia.

26. In circumstances where there is an entity that has legal ownership and control over the information, but you also have somebody who is physically in possession of it, if there is a data breach that happens to one or the other entity, it affects both entities. Both entities then have obligations to look into what has happened and notify if necessary.

27. In general, only one entity actually needs to comply with their obligations – the scheme leaves it up to the entities to decide who must investigate and notify. However, the Privacy Commissioner suggests that the party with the closer connection to the affected individuals should be the one taking the lead on investigation and notification.

<u>Exceptions to notify</u>

28. Once you establish that a breach is an eligible data breach, there are then some exceptions that may apply. These exceptions broadly relate to where notification would prejudice certain enforcement related activities, or where notification would be inconsistent with Commonwealth laws regulating the use of disclosure of information.

29. Exceptions can also apply where declarations are made by the Privacy Commissioner exempting or delaying notification for certain reasons. Breaches may also be exempt where data breaches are notified under s 75 of the *My Health Records Act 2012* (Cth).

30. To notify, you must first prepare what is known as a compliance statement and you then provide that to the Privacy Commissioner. You must then work out which individuals are affected by the breach, and you must notify them about the contents of that compliance statement.

31. The Privacy Commissioner has developed an online form to help organisations with compliance statements.

32. Generally the statement must include the identity and the contact details of the relevant organisation, a description of the eligible data breach, details of the kind of information involved in the eligible data breach and recommendations about the steps that affected individuals should take in response to an eligible breach.

33. When notifying, you can choose to either notify all of the individuals to whom the information relates of the contents of the statement you provided the Privacy Commissioner, or you can notify only those individuals who are at risk of serious harm.

34. If neither of these options are practicable, you must then publish a copy of the statement on your website and otherwise publicise the contents of that statement. The legislation says that you must make these notifications as soon as practicable after preparing the statement.

Preparation by organisations

35. Preparation is important because the last thing you want to be doing when you are dealing with a data breach emergency is working out whether you are caught by the scheme and what you are supposed to do in response. It is recommended that organisations preemptively look into these more basic questions – for example, are you caught by the scheme, and to what extent does it apply to your organisation?

36. To facilitate compliance with the new scheme the Privacy Commissioner is recommending that entities develop and implement what is known as a data breach response plan. The purpose of this plan is to ensure that you have a documented strategy for containing, assessing and managing a data breach incident from start to finish.

37. The plan should include a clear explanation of what a data breach is for that particular organisation, the steps and the escalation procedures that need to be taken if a data breach does occur, and the roles, responsibilities and authority of individuals within the organisation in the event of a data breach.

38. When developing this plan, you should have regard to the existing compliance processes and policies, disaster recovery plans, cyber security incidence response plans, insurance policies, and so on. You should also look at existing contracts to see whether they are imposing any privacy or data breach or security requirements that need to be considered as part of the plan.

39. Once you have a plan in place it needs to be supported by appropriate training for staff which can be tailored for each business unit.

40. There are a range of clauses that can be included in to new contracts to ensure that you have appropriate controls and remedies in relation to data breaches that may arise in the course of the relationship between the contracting parties.

41. In contracts where personal information will be jointly held, you may want to include clauses requiring counter parties to: communicate suspected data breaches to each other, to take certain steps to assess, contain, remedy breaches, to engage with you before notifying individuals or the Privacy Commissioner of a breach to the extent that is legally permissible under the Act, and so on.

42. Certain contracts and organisations will be dealing with such sensitive information that it may be worthwhile for these organisations to review contracts to see who will be managing what, and discuss with those parties what the arrangements would be if there was a data breach under the new scheme.

43. Broadly speaking, the new scheme does not require an entity to update its privacy policy. However, an organisation does need to maintain a current privacy policy, and this might be the impetus to review the privacy policy and the organisation's privacy compliance regime more generally.

44. The Privacy Commissioner has published a lot of really helpful general guidance about the scheme and that is available on its website: https://www.oaic.gov.au/. If you are after more specific advice for your particular organisation, it is worthwhile getting in touch with lawyers who specialise in this area.

BIOGRAPHY

Eli Fisher

Senior Associate – HWL Ebsworth, Sydney

Eli Fisher is a commercial lawyer with expertise across intellectual property, privacy, competition and consumer, and media laws. His experience spans a range of industries, including the media, entertainment and content industries, aviation, technology as well as manufacturers, importers and retailers of FMGG. Eli edits the Communications Law Bulletin, and sits on the Boards of the Copyright Society of Australia and the Communications and Media Law Association. Eli is completing a Masters degree at UNSW, duel-specialising in Media & Technology Law, and Innovation Law.

Ben Gulson

Associate – HWL Ebsworth, Sydney

Ben Gulson is an Associate in HWL Ebsworth's Commercial Group. He has acted for various State government and private sector clients in relation to major commercial projects involving complex software licensing and commercialisation agreements, multi-jurisdiction outsourcing agreements and other commercial and due diligence documents relating to information technology systems and software.

BIBLIOGRAPHY

Legislation

Privacy Act 1988 (Cth)

My Health Records Act 2012 (Cth)

Other

https://www.oaic.gov.au/