HERBERT SMITH FREEHILLS

GUIDE TO BIG DATA AND THE AUSTRALIAN PRIVACY PRINCIPLES

Australia
Legal Briefings

In May 2016, the OAIC released the draft Guide to assist entities to undertake big data activities in accordance with privacy laws.

IN BRIEF

- The Office of the Australian Information Commissioner (OAIC) has released a draft 'Guide to Big Data and the Australian Privacy Principles'[1] (Guide) for consultation.
- The OAIC recognises the value in and importance of big data activities and aims to strike a balance between the benefit that can be obtained from big data activities and the protection of personal information and privacy.
- The Guide proposes various measures entities should take when personal information is collected, dealt with and maintained for the purposes of big data activities.

THE GUIDE

In May 2016, the OAIC released the draft Guide to assist entities to undertake big data activities in accordance with privacy laws. The draft Guide is targeted at entities that are governed by the Australian Privacy Principles (**APPs**) in the Privacy Act 1988(Cth) (**Privacy Act**), that is, the Federal public sector and many private sector companies (including companies with an annual turnover of more than $3,000,000 and health service providers). The draft Guide also serves as a useful model for entities that are not subject to the APPs.

Once finalised, the Guide will not be legally binding but will, however, guide the OAIC in its performance of its role under the Privacy Act.

WHAT IS 'BIG DATA'?

'Big data' describes the relatively recent phenomenon surrounding the mass creation, collection and processing of data. Whilst there is no single definition, big data is generally '*high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization*'.[2] Today, over 2.5 quintillion bytes of data are created each day.[3]

The OAIC recognises that big data can be a valuable tool for businesses to engage with data and analytics to benefit their business and engage with customers in a more personalised and relevant way. However, given the volume of 'personal information'[4] that may be collected or created through 'big data activities',[5] big data activities may require additional steps be taken to maintain personal privacy.

GENERAL RECOMMENDATIONS

The Guide makes two key general recommendations to entities prior to engaging in big data activities.

Firstly, the OAIC recommends that entities integrate and embed privacy into their culture, processes and systems at the outset ('*privacy by design*'). This ensures that privacy is embedded into an organisation or a project, rather than being considered as an afterthought. Entities engaging in big data activities should design privacy into the project, including by conducting a privacy impact assessment to identify risks and make appropriate recommendations.

Secondly, information collected and used for big data activities should be de-identified where possible. De-identification brings the information outside the scope of the Privacy Act and would enable a business to use and maximise the value of the data more freely. Relevant considerations for entities include: what method of de-identification is appropriate for the nature of the data, the appropriate uses and disclosures of the de-identified information, the stage at which de-identification should occur and the cost, difficulty, practicality and likelihood that the information can be re-identified.

THE AUSTRALIAN PRIVACY PRINCIPLES AND KEY CONSIDERATIONS

The OAIC's application of the APPs to big data indicates that entities undertaking big data activities can do so in compliance with their APP obligations, including through notifications to individuals addressing the big data activities. In particular, the OAIC suggests that an entity engaging in big data activities should:

1. limit the collection of personal information to the extent reasonably necessary to undertake its big data activities.

2. carefully outline in a privacy notice when personal information will be used or disclosed for big data activities, as this will often be a ‘secondary purpose’ to the purpose for which the information was initially collected, as well as whether information will be used for direct marketing purposes.

3. ensure that individuals have a real opportunity to select which uses, collections or disclosures of their information they consent to and which they do not.

4. notify individuals if information will be disclosed to third parties, including overseas recipients (which is often the case in big data activities).

5. notify individuals of the details of any information collected from third parties and ensure that the privacy notices of these third parties notify individuals that such disclosures may occur.

6. provide more dynamic, multi-layered and user centric privacy notices such as ‘just-in-time’ notices, video notices and privacy dashboards rather than relying on a single static privacy policy.

7. ensure that individuals have a simple means of opting out of future marketing communications or requesting their information no longer be used for such purposes. An entity should also consider whether their big data activities are facilitating direct marketing by other organisations to which they provide data. This is important given that big data activities are often performed for the purpose of informing direct marketing activities.

8. keep track of the types of information being collected to reduce the risk of using or disclosing sensitive information for direct marketing purposes without individuals’ consent.

9. where possible, de-identify information before sending information overseas for big data activities (as may occur through the use of overseas cloud or internet-based platforms) or if information needs to be retained for future big data activities.

10. take reasonable steps to ensure that overseas recipients of information do not breach the APPs, as the Australian entity will remain accountable for any breach.

11. take rigorous steps to maintain the quality of information used for big data activities, as the information has the potential to become outdated or inaccurate due to the large quantity of information which is collected from a variety of third party sources and is often retained for long periods of time.

12. implement procedures to assess the quality of information, such as recording when information was received, and check that third party sources of information have also implemented appropriate practices, procedures and systems.

13. take reasonable steps to monitor and protect against the security risk posed by big data activities. This is because such activities are 'honey pots' of valuable and sensitive personal information, often held for long periods of time.

KEY TAKEAWAYS

Big data activities pose potentially greater risks to personal privacy due to the very nature of the activities – that is, they involve large sets of data (and may result in the creation of personal information through the aggregation of different data sets) which are often sourced from or shared with third parties, sourced originally for different purposes and retained for long periods of time.

Businesses engaging in big data activities (including entities that themselves perform big data analytics or rely upon the results of such analytics) should therefore be mindful of the increased risk of invading personal privacy and refer to this Guide to ensure their activities comply with the Privacy Act.

In many respects the draft Guide is consistent with other guidance materials prepared by the OAIC, including the APP Guidelines.[6] Accordingly, entities currently engaging in big data activities should already be complying with many of the draft Guide's recommendations. However, the Guide also highlights some areas likely to prompt those entities to revisit their practices, particularly in respect of:

1. providing more specific information about big data activities in privacy notices, without being overly detailed.

2. where personal information will be handled for multiple purposes, the degree of choice offered to individuals about which purposes they do and don't accept.

3. providing more dynamic, multi-layered and user centric privacy notices rather than relying on a single static privacy policy.

4. strengthening data quality procedures, including recording when personal information was collected, whether it is an opinion and whether it was collected via creation.

5. where third parties are involved, the assessment of those third parties' privacy policies, notices, practices, procedures and systems.

The Government has invited public comments on the draft Guide, which must be received by Monday 25 July 2016.

ENDNOTES

1. Office of the Australian Information Commissioner, 'Consultation Draft: Guide to Big Data and the Australian Privacy Principles', 2016.

2. Gartner, 'The Importance of 'Big Data': A Definition', cited in Department of Finance and Deregulation, 'The Australian Public Service Big Data Strategy', 2013.

3. IBM, 'Bringing big data to the enterprise'.

4. 'Personal information' is defined in the Privacy Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable (s 6).

5. 'Big data activities' include big data analytics, as well as the handling and collection of personal information before and after such analysis.

6. Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines', 2014.

LEGAL NOTICE