ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Practical Data Security Takeaways from Australia's Recent Privacy Determinations

Compliance and Ethics

Technology, Privacy, and eCommerce

The Privacy Act of 1988 (Privacy Act), which includes the 13 Australian Privacy Principles (APPs), is Australia's federal law regulating the collection, use, and disclosure of personal information. Recently, the Office of the Australian Information Commissioner (OAIC) has stepped up its

enforcement of the Privacy Act. This article reviews OAIC's recent privacy determinations and discusses practical data security related takeaways that can help companies ensure compliance.

Salient aspects of the Privacy Act

Unlike many privacy laws around the world, there is an exemption in the Privacy Act for small business operators that have an annual revenue of less than AU$3,000,000. However, certain small businesses must remain in compliance, regardless of their annual revenue. These companies include credit reporting bodies, businesses that buy or sell mail lists, businesses that maintain tenancy databases, certain employee associations, and health service providers. Another significant aspect of the law is the Privacy Act's extraterritorial scope. Unlike current EU Directive regulations, and similar to the European Union's recently passed General Data Protection Regulation (GDPR), the Privacy Act applies to companies that have an "Australian link." An entity has an Australian link if it was formed in Australia, if it conducts business in Australia, or if personal data was collected by an entity in Australia.

Enforcement of the Privacy Act

The main agency in charge of the enforcement of the Privacy Act is the OAIC. Among other things, the Privacy Act empowers the OAIC to: (1) provide guidance to privacy regulations under the Privacy Act, (2) monitor privacy related issues of entities regulated under the Privacy Act, (3) conduct investigations related to the act or practices of an entity regulated under the Privacy Act, and (4) resolve privacy complaints by conciliation. If not resolved by conciliation, entities covered under the Privacy Act need to comply with OAIC determinations, which may include financial fines or orders made by the OAIC.

Unlike regulatory agencies in other countries, in which the agency in charge investigates the matter and if it has findings, issues an enforcement action, the Australian process is much more conciliatory. Following the investigation of a complaint and prior to an administrative enforcement, the OAIC attempts to resolve the dispute through a mediation process with the goal of reaching a suitable settlement for both sides. The vast majority of complaints are resolved in the conciliatory process before an OAIC determination. Unfortunately, the OAIC has not released information on conciliation resolutions.

What we can learn from privacy determinations

OAIC's privacy determinations provide guidance to APP entities about the practical expectations of the OAIC, in addition to any ambiguous areas of the Privacy Act in which there may be discrepancies among the public, the law, and the entity in question.

Protection of information

Inadequate protection of personal information was among the top categories of privacy complaints received by the OAIC in 2016. Furthermore, 10 of the 14 determinations made since 2012 involved an APP (or NPP) regulated entity not taking reasonable steps to secure personal information.

According to the Privacy Act, APP 11.1 provides that if an entity holds personal information, the entity must take reasonable steps to protect information from misuse, loss, and unauthorized access. The OAIC guidelines state that "reasonableness" depends on a number of considerations, including the

nature of the entity, sensitivity of the personal data, adverse consequences for data subjects in event of a breach, and the practicality of implementing various countermeasures. In addition to other practices, the OAIC guidelines recommend implementing reasonable management strategies for IT security, access security, and physical security.

When determining a reasonable course of action, entities should consider balancing the privacy interests of an individual against the interests of the entity. We further recommend that entities consider the following when determining whether their data security steps and strategies are reasonable and adequate.

1. Privacy practices should be adequate and documented.
It is important to take reasonable steps to secure personal information. A large Australian insurance company was held to be in violation of NPP 4.1 (the predecessor law to APP 11.1) for providing a client's Tax File Number (TFN) to an unauthorized third party. The company stated that they did not actively collect TFN information and if the information was collected, it would have been "redacted." However, the company could not meet the burden of proof that they had a process in place to redact TFN information or prove that in that specific instance, the TFN information was actually redacted. Therefore, the OAIC found that the company did not take a "reasonable step" to secure information.

While having adequate procedures and policies in place are important in complying with the Privacy Act, it is equally important to take proactive steps to ensure that practices are understood and followed. Documenting security practices and creating audit trails ensures that an organization remains thoughtful about access provisions and creates defensible practices if and when challenged.

2. Financial information, while not "sensitive," is held to a higher standard of care.
As noted in APP 11.1, an entity holding personal data must take "reasonable steps" to prevent the misuse, loss, and unauthorized access of that information. The Privacy Act places a higher standard on entities that handle "sensitive" information. Sensitive information includes information such as health records, criminal records, race, sexual orientation, religion, political beliefs, and membership of political, professional, or trade organizations. According to the OAIC, while financial information is not per se labeled as sensitive information, it is still considered to be "more sensitive" than other kinds of information. One particular case that stood out was the NRMA Insurance Determination. At the request of the customer, the insurance company issued a certificate that lists all insurance policies under the customer's name. However, since the customer was also a joint insurance holder with another customer, the certificate also included a complete list of all of the joint insurance holder's insurance policies that were not co-insured policies. The disclosed information only included the individual's name, the description of the policy, and the policy number.

Regardless, the OAIC still considered the policy number, description of policy, and name to be a form of financial information that is "more sensitive" and should be held to a higher level of protection. Furthermore, the OAIC stated even if the risk of harm to the individual may not be high, the more information disclosed about a person, the more vulnerable they become to the misuse interference or inappropriate access to their personal information. Entities should consider identifying, segregating, and maintaining different security standards and policies for sensitive data as compared to non-sensitive customer data.

3. Review and enforce appropriate access controls.
While it is important to implement adequate security policies, standards, controls, and safeguards, it is essential to continuously manage and reassess these requirements. A large Australian bank received penalties for providing insufficient access controls in violation of NPP 4.1 when an employee

viewed the account information of a former employee who was engaged in a lawsuit against the bank. The former employee stated that certain employees who were adverse to her claim were allowed to access her account information. The former employee claimed that the employees that accessed to her account information hindered her proceedings against her former employer. The OAIC stated that the bank failed to put into place certain access control restrictions on her account information once it had knowledge of her lawsuit against the bank. It is possible that a periodic review of all processes that have access to customer information would have likely identified the issue and possibly prevented the determination.

Entities should consider periodically reviewing their security strategy, including access controls. Access controls should have an expiration trigger and be regularly reassessed by the grantor to ensure that access privileges have been removed when no longer needed. Entities should consider whether access to certain information is appropriate for a user, and use technical features to restrict and monitor access. Questioning new access requests or existing access privileges will ensure that minimal access is granted, and by limiting access, allow an organization to control the integrity and vulnerability of information and databases.

4. Entities must not forget to protect physical information
Typically, when individuals think about data security, they think about firewalls, encryption standards, and access controls. However, the OAIC enforced a determination against an Australian telecommunications company for failing to adequately protect physical information.

In this matter, customers were required to provide identification information, including a driver's license and Medicare card, in order to enter into a contract. After receiving that information, the company failed to adequately secure their customer's personal information in a proper manner. One journalist reported that it had abandoned physical copies of customer information in open shipping containers. Even though the company used locks on containers holding customer information, the OAIC noted that due to the nature and sensitivity of the information, its actions were not "reasonable." The OAIC noted that since the information was extremely sensitive, the company should have taken additional steps to secure sensitive personal information, even in a physical form.

It is important to remember that the Privacy Act applies to all forms of personal data, including information on paper documents. In this decision, the OAIC noted that depending on the sensitivity of the personal information, entities should consider the following steps to ensure the physical security of personal information:

a. Monitor the movement of physical files;
b. Implement physical access controls such as issuing a limited number of keys or passes to areas in which the information is stored;
c. Monitor and guard the location in which the information is stored; and,
d. Use a secure means of storage, such as a secure or locked room in monitored, guarded or staffed premises.

Furthermore, organizations should consider implementing physical safeguards within their organization and requiring that their vendors also implement at least the same safeguards when handling data. Organizations should also consider periodically auditing a vendor's security practices.

Future considerations

The OAIC received an 18 percent increase in the number of privacy enquiries in 2016. As organizations brace and prepare for future investigations, organizations should work closely with its own electronic and physical security teams by considering recent findings and taking appropriate action to evaluate their own controls and safeguards. A strong security posture includes adequate security provisions with practices that are documented and align to the requirements. Where possible, technical controls, including access restrictions and audit logs, should be used to monitor and enforce security practices. Finally, sensitive information warrants additional security protections, regardless of whether it is maintained in an electronic or physical format. To maintain an adequate security strategy, it must addresses cyber, access, and physical security requirements.

Further Reading

1 Section 6D of the Privacy Act.

2 Id.

3 The Explanatory Memorandum to the Privacy Amendment Bill of 2012 states that entities who have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, carry on a “business in Australia or an external Territory.”

4 Directive 95/46/EC.

5 Section 5B of the Privacy Act.

6 Section 5B(1B) of the Privacy Act.

7 Id at Section 27.

8 Id at Section 40A; with limited exceptions, the OAIC is required under the Privacy Act to make reasonable attempts to conciliate the complaint.

9 According to the OAIC, over 97 percent of privacy complaints are resolved prior to a determination and within 12 months of the initial filing.

10 Prior to revision of the Privacy Act in 2014, the APPs were separated into the Information Privacy Principles (IPPs) for government entities (known as IPP entities) and the National Privacy Principles (NPPs) for private sector entities (known as NPP entities), now cumulatively referred to as APP entities.

11 See Office of the Australian Information Commissioner list of determinations at www.oaic.gov.au/privacy-law/determinations/ (last accessed December 18, 2016); as of December 18, 2016.

12 Section 11 (Schedule 1) of the Privacy Act.

13 Office of the Australian Information Commissioner, Australian privacy Principles Guidelines, Section 11.7 (December 17, 2016).

14 Id.

15 Balancing the interest of individuals against the interest of the entities is an objective of the Privacy Act, stated in Section 2A.

16 Decision of Australian Information Commissioner, HS and Amp Life Ltd, [2015] AlCmr 81, Sections 1 and 2 (17 December 2015).

17 Id at Section 49.

18 Id at Sections 62 and 63.

19 Id at Section 64.

20 See definition of “sensitive information” in Section 6 of the Privacy Act.

21 Decision of Australian Information Commissioner, IR and NRMA Insurance, Insurance Australia Limited, [2016] AlCmr 37 (17 December 2015).

22 Id at Sections 10 to 13.

23 Id.

24 Id.

25 Id at Section 86.

26 Id at Sections 87 to 89.

27 Decision of Australian Information Commissioner, KA and Commonwealth Bank of Australia Limited, [2016] AlCmr 80 (25 November 2016).

28 Id at Sections 7 and 8.

29 Id at Sections 60 and 61.

30 Id at Sections 86 to 88.

31 Decision of Australian Information Commissioner, IY and Business Services Brokers Pty Ltd t/a TeleChoice, [2016] AlCmr 44 (30 June 2016).

32 Id at Sections 3 to 8.

33 Id.

34 Id at Sections 33 and 35.

35 Id.

36 Id at Section 34.

37 Office of the Australian Information Commissioner, Annual Report 2015-2016, Pg. 12.

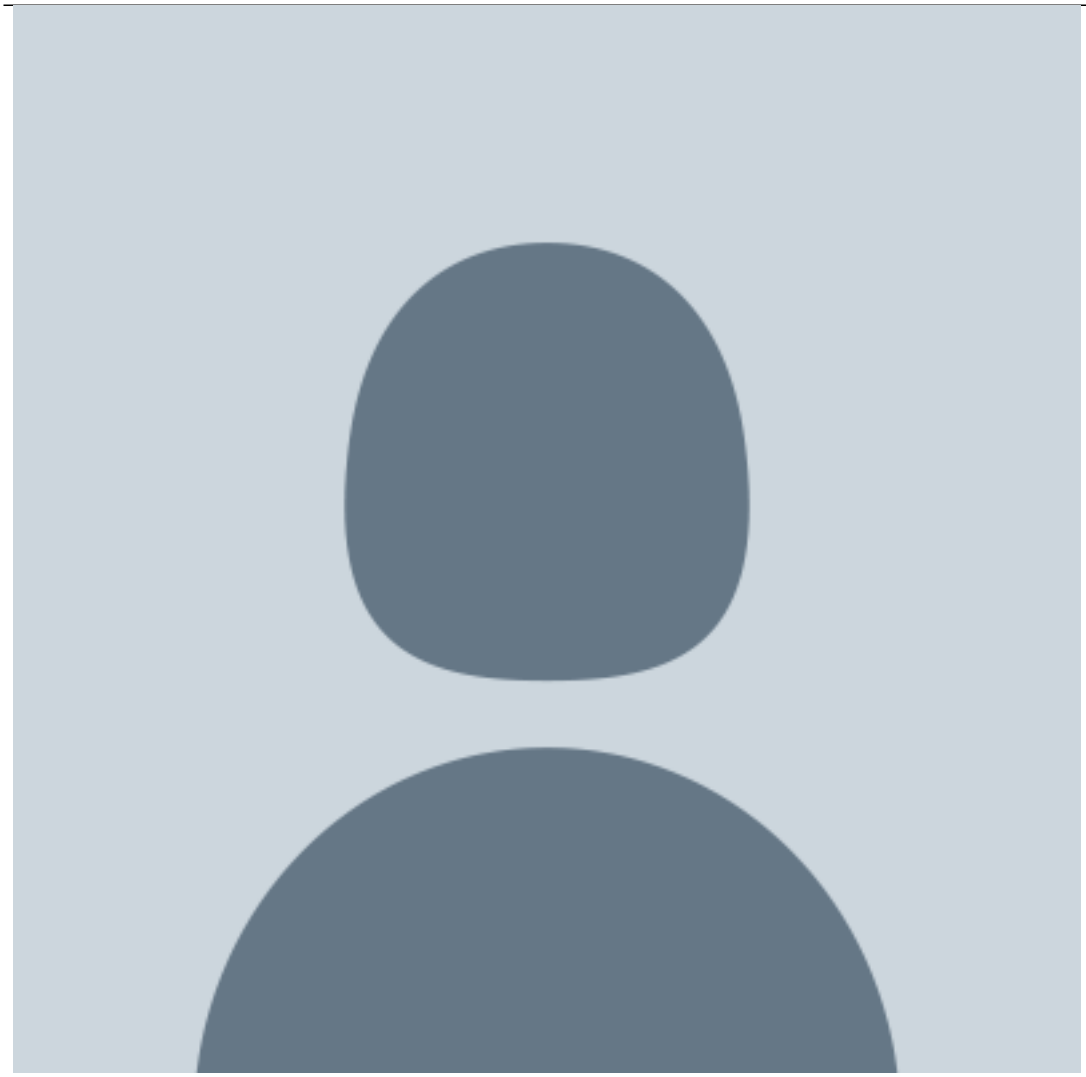
Deanna Tyler

Senior Data Privacy and Security Attorney

Seagate Technology LLC

She drives a strong culture of privacy by leading a cross functional team of stakeholders across the organization.

David Chen



Associate

the Boulder, Colorado office of Bryan Cave

He practices with the firm’s technology, entrepreneurial, and commercial practice client service group, where he focuses on technology transactions, data privacy, and security matters.