Article Information

Author: Tim Clark
Service: Corporate & Commercial, Information Technology, Intellectual Property

Are you compliant with the Privacy amendments? The OAIC provides its assessment one year on

Tim Clark, Partner, and Philip Chow, Lawyer, outline the current position of the Office of the Australian Information Commissioner a year on from Australia's privacy reforms, and look ahead at what is next for privacy strategy and compliance for commercial organisations.

***Tim Clark, Partner**, and **Philip Chow, Lawyer**, outline the current position of the Office of the Australian Information Commissioner a year on from Australia's privacy reforms, and look ahead at what is next for privacy strategy and compliance for commercial organisations.*

In March 2014, significant changes to the Privacy Act commenced, including a new set of Australian Privacy Principles (APPs) which set out how private sector organisations must collect, use, disclosure and handle the personal information of individuals. The regime is enforced by the Office of the Australian Information Commissioner (OAIC). One year on from these changes, the OAIC has indicated that its focus now will be on governance and assisting organisations to build a culture of privacy. It has commenced targeted assessments of the privacy statements of 20 of the most visited websites in Australia. There are further plans to conduct more assessments in the coming year.

In addition, the Privacy Commissioner has recently handed down a decision requiring Telstra to provide all "metadata" (including network data such as IP address information, URL information and cell tower location information) in response to a customer request. While this decision was decided under the previous privacy regime, and Telstra has indicated that it will lodge an appeal, the decision provides a useful insight into how the OAIC may approach the issue of what constitutes "personal information."

A new focus for the OAIC

For the first year of the new privacy law, the OAIC focussed on developing guidance and working with organisations to ensure that they have all the tools and information required to understand the changes.

In early May this year, the OAIC used national Privacy Week to announce that it would shift its focus from an educational, preparatory phase towards a more strategic approach regarding privacy awareness and enforcement. As part of this, the OAIC has reviewed the privacy statements of organisations running 20 of the most visited websites in Australia, including the websites of large banks, social media platforms and news organisations. These entities are arguably sufficiently well-resourced to ensure compliance with privacy laws. However, over half of the privacy statements were found to be deficient in some way. For example, almost half of privacy statements failed to outline how that organisation deals with complaints about privacy.

The problems with the privacy statements were not caused by a lack of detail – the OAIC calculated that the median length of the statements was 3,145 words (with the Privacy Commissioner being reported to say that one privacy statement had over 18,000 words). In this review, the OAIC re-iterated that privacy statements should be kept simple as well as tailored to the business and its audience.

Given the OAIC's new focus on privacy awareness and enforcement, it is an opportune time for businesses to review their privacy statements to ensure full compliance with the Privacy Act in light of the Privacy Commissioner's finding. Legal compliance policies and programs should also be re-examined to identify if there are areas of compliance risk requiring attention. Piper Alderman would be pleased to assist your business in this process.

Telstra metadata decision

The OAIC's decision in the matter of Ben Grubb and Telstra provides insight into the Privacy Commissioner's views as to what constitutes "personal information". Ben Grubb, a journalist for Fairfax, successfully argued that Telstra should provide "all the metadata information Telstra has stored" about him in relation to his mobile phone services (with the exception of inbound call records). Grubb has stated that he requested the information from Telstra as research for an article about the Federal Government's metadata laws.

Telstra initially provided Grubb with only his outbound mobile call details and his data usage session times. However, during the course of the determination, it decided to provide him with all metadata records except for "network data" and incoming call records. The key consideration was whether the metadata constituted "personal information" such that Grubb would have the right to access this information under the then applicable National Privacy Principles (now replaced by the Australian Privacy Principles).

The interesting question in this case was whether "network data" (such as IP address information, URL information and cell tower location information) constituted "personal information".

Under the Privacy Act, "personal information" includes information about an individual from which their identity is "apparent" or "could reasonably be ascertained". The Privacy Commissioner found that network data did constitute "personal information" even when it was captured across 13 network management systems and needed to be matched with subscriber information in order to identify the user. Grubb's identity was not "apparent" from the network data as his identity could not be identified on the face of the information alone (without the use of the extraneous material).

However, the Privacy Commissioner considered that Grubb's identity was ascertainable with "a good degree of certainty" by cross-referencing the network data with other data held in Telstra's customer management and subscriber record systems to identify the individual. Telstra had contended that an individual's identity could not "reasonably" be ascertained and that having to provide access to metadata as "personal information" under the Privacy Act would be burdensome in terms of complexity, time and cost. The Privacy Commissioner rejected this claim, noting that Telstra had 120 staff with expertise in data retrieval of this kind and that Telstra had also made a public statement stating that customers can access their metadata on request.

In respect of incoming call records, the Privacy Commissioner accepted that the records included information about both incoming callers as well as the customer and agreed with Telstra's submission that it should not be required to provide that information This was on the basis that, under the National Privacy Principles, an organisation may refuse an individual access to their personal information where the access would have an unreasonable impact on the privacy of other individual. The Privacy Commissioner noted that people with a silent line, or those who block their line or number, do not wish (and would not reasonably expect) their phone number to be disclosed to the recipient of the call.

Whilst Telstra has indicated that it will appeal the OAIC decision, the decision is important to a range of businesses which retain "de-identified" information as part of its business processes. If this decision is upheld on appeal, businesses may need to treat "de-identified" information as "personal information" in circumstances where the identity of the individual could potentially be ascertained when cross-referenced with other databases. "Personal information" must be dealt with in accordance with the Australian Privacy Principles, which entails compliance obligations relating to the collection, disclosure, use and storage of the information. As a result, some businesses may need to change their processes to ensure compliance with the Privacy Act.

Piper Alderman would be pleased to assist your business in reviewing its practices. For further information, please contact Tim Clark.