Office of the Australian Information Commissioner - Australian Privacy Principles (APP) Guidelines Chapters 6-11

Submission
as prepared by:

Australian Mobile Telecommunications Association and Communications Alliance

October 2013

Introduction

The Australian Mobile Telecommunications Association (AMTA) and Communications Alliance (the Associations) welcome the opportunity to provide this submission in response to the Office of the Information Commissioner's (OAIC) Draft Australian Privacy Principles (APP) Guidelines (Draft Guidelines).

The Associations have a number of concerns relating to the Draft Guidelines. These include, but are not limited to, the following:

- the requirement to define a single, primary purpose when seeking consent;
- the lack of definition of 'reasonable period of time' as it relates to direct marketing;
- behavioural information collected through web browsing being defined as personal information;
- the prescriptive guidance relating to information to opt out of direct marketing;
- the requirement to offer a verbal opt-out as part of a telemarketing call;
- the lack of clarity relating to when an APP entity 'discloses' information to an overseas recipient;
- the lack of clarity relating to 'reasonable steps' taken by an APP entity entering into contractual arrangements with overseas entities; and
- the lack of information relating to what overseas jurisdictions would be considered to be 'subject to a similar law or binding scheme'.

The Associations

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

APP 6 - USE OR DISCLOSURE OF PERSONAL INFORMATION

The Associations have concerns with a number of the concepts outlined in the Chapter 6 of the Draft Guidelines.

Primary Purpose

As the Associations asserted in the previous submission to the OAIC, the requirement to specifically define a single, primary purpose is not practical and is contrary to the way in which commercial entities operate. The interpretation in the Guidelines means it is unclear whether a purpose such as 'marketing' would be considered too broad.

It is unrealistic to suppose that an entity can 'prioritise' the purpose for collecting personal information when, in reality, there are many reasons of equal importance which require it do so. As such, the Draft Guidelines should allow a degree of flexibility which reflects the reality of commercial operations and the fact that businesses often have multiple 'primary' purposes for collecting personal information.

Elements of Consent - Current and Specific

The Associations request that the OAIC provides additional guidance relating to what is considered to be 'current and specific consent'. The guidelines should state that consent is current by default and only expires as a result of a specific circumstance arising, for example if an individual actively withdraws their consent.

Requirement to make a written note of use or disclosure for this secondary purpose (Clause 6.64)

The Associations note the requirement in clause 6.64 to make a written note of the use of disclosure relating to 'enforcement related activities'. While it is noted that Clause 6.66 states that *"this requirement does not apply where a law prohibits the entity from making such a record"*, the Associations are concerned that the requirement to make the note may create an additional security risk.

The Associations seek assurances from the OAIC that the current reporting frameworks as outlined by enforcement and regulatory bodies, such as ASIO and the ACMA, are sufficient. Any requirements in the APP Guidelines should not exceed the current requirements of these agencies. In our view, any additional requirement would be an unnecessary and onerous regulatory burden. Further, the Associations seek confirmation that APP entities should not be required to create an additional security risk through the creation of records.

APP 7 – DIRECT MARKETING

Definition of 'Reasonable Period of Time' (Clause 7.6)

The Associations seek practical guidance from the OAIC in relation to the definition of a 'reasonable period of time' as it relates to implementing a request by an individual to not use his or her information for the purposes of direct marketing.

It is the Associations' view that a 'reasonable period of time' should align with the timeframe in the Do Not Call Register Act 2006, which is 30 days.

Data Stored on Cookies (Clause 7.11- 7.12)

The Associations object strongly to a definition of direct marketing given at clause 7.11 which includes the following example:

> *"displaying an advertisement on a social media site that an individual is logged into, using personal information, including data stored on cookies relating to websites the individual has viewed"*

As the Associations asserted in our previous submission, the collection of information through cookies on websites should not be considered personal information.

It is not appropriate to consider the collection by cookies of behavioural information obtained through an individual's web browsing as personal information. The Associations request that the bullet point quoted above be removed from the Draft Guidelines.

Clause 7.12 gives examples of where marketing is not direct marketing and therefore not covered by APP7. It would be helpful if the example of online behavioural information and/or information collected via cookies was added to this list to reflect the point that behavioural information is not, by default, personal information.

'Reasonably Expects' – Internet Banking (Clause 7.19)

The Associations are concerned with the use of the example of phone numbers being used as a secondary form of authentication for internet banking and request that this example be removed from the Guidelines. Given the security and privacy risks associated with this method of authentication, the Associations' members are opposed to the implications of this method being published as a legitimate example of verification.

Prominent Statement to Opt Out (Clause 7.29)

The Associations are supportive of the Guidelines providing for an individual to be notified of his or her ability to opt out of direct marketing in a prominent way. However, the Associations object to the specification of a particular font size, particularly the requirement for the opt-out statement to be 'at least the same font size as the main body of text in the communication'. This is impractical and too specific. Further, it is unlikely that any consumer would have an expectation that information informing an individual how to opt out be the same font size as the main body of the text.

It should be noted that the requirement in the current Draft Guidelines is more onerous than both the Australian Consumer Law and the Telecommunications Consumer Protections Code.

In the Associations view, it should be sufficient to require an APP entity to provide information on how to opt out which is prominent and easy to read.

Verbally Opt-Out of Direct Marketing Calls (Clause 7.30)

The Associations have concerns with the implications of Clause 7.30. In particular:

> *"Telling the recipient of a direct marketing phone call that they can verbally opt out from any future calls"*

The Associations object to the prescriptive requirement to provide individuals with an opportunity to opt out of every telemarketing call. Commercial APP entities, such as those in the telecommunications industry, should be able to manage the way in which they communicate with their customers, so long as they comply with requirements to give opportunities to opt out of direct marketing activities. The Associations consider the proposal in the Draft Guidelines is only one way that this objective could be met and that there are alternative, more positive ways to offer an individual to opt out. For example, a marketing call could begin with a question such as *"Have you got some time at the moment to speak with me?*" If 'no' then *"Is there another time that is more convenient?*" and if still 'no' then *"Would you prefer to opt out of receiving these calls in the future?*" In the Associations' view, this is a far better conversation to have with an individual than what is currently proposed in the Draft Guidelines and it still provides an individual with the opportunity to opt out.

The Associations also draw the OAIC's attention to the fact that there are already regulations that cover telemarketing activity in the telecommunications industry. For example, the Telemarketing and Research Industry Standard 2007 requires a call to be terminated when *"the call recipient asks for the call to be terminated or otherwise indicates that the call recipient does not want the call to continue"*[1].

Finally, the Associations note there are opportunities for individuals to opt out of all telemarketing activities by registering on the Do Not Call Register. Given this context, the Associations request that the prescriptive requirement to advise the recipient they can opt out of direct marketing calls should be amended in way that allows an individual the opportunity to do so.

APP 8 – Cross Border Disclosure of Personal Information

The Associations have concerns relating to the following clauses of APP 8.

Accountability – (Clauses 8.1, 8.2, 8.53 & 8.54)

The Associations believe the Guidelines should be clear about accountability.. That is, they should explicitly state that an APP entity will be accountable for any breach of privacy if it occurs through the fault of an overseas recipient of that information, as if the APP entity had made the breach. That is, the information included at Clauses 8.54 and 8.54 could be stated up front within this Chapter of the Guidelines.

When does an APP entity 'Disclose' Personal Information? (Clause 8.8)

The Associations seek clarification with regard to 'disclosure' in the context of release of information to an overseas recipient. The way in which commercial entities provide personal information to overseas entities is more complex than is described in the Draft Guidelines.

The Draft Guidelines state:

> *"In the context of APP 8, an APP entity will disclose personal information to an overseas recipient where it:*

[1] Telemarketing and Research Industry Standard 2007, http://www.comlaw.gov.au/Details/F2007L00815/Html/Text#param5

- *Shares the personal information with an overseas recipient*

- *Discusses the personal information at an international conference or meeting overseas*

- *Sends a hard copy document or email containing an individual's personal information to an overseas client*

- *Publishes the information on the internet, whether intentionally or not, and it is accessed by an overseas recipient."*

An APP entity may have a commercial relationship with an overseas entity that may, technically, have 'access' to personal information yet it may never actually be accessed. That is, the commercial reality of the operation of business entities means that overseas recipients may have the opportunity to retrieve information yet may never avail themselves of this opportunity.

As such, has the APP entity 'disclosed' the personal information at the time of providing technical access, or when the information is actually accessed? The Associations request that the OAIC provide additional clarification or guidance on this point.

Personal Information to a Contractor (Clause 8.12)

The Associations request that the OAIC provide some specific examples of the types of security measures that an APP entity may have taken which would, in the OAIC's view, complied with the requirements of clause 8.12. That is, examples of control environments which the OAIC would consider to be sufficient to meet the requirements of this clause.

When will an APP entity have taken reasonable steps? (Clause 8.14)

The Draft Guidelines state:

"the appropriate steps for an entity will depend upon circumstances that include:
…

- *The entity's relationship with the overseas recipient. Additional steps may be required if an entity discloses information to an overseas recipient to which the entity has not previously disclosed personal information.*

- *…*

- *Existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information. For example, additional steps may be required where the recipient has limited safeguards in place*

- *…"*

The Associations contend that these clauses do not provide sufficient guidance. As such, further clarification of these points is necessary. That is, could the OAIC provide examples of additional steps that would be considered to have complied with this obligation?

The Associations also note that dot points 1 and 3 of this Clause are repetitive.

When will the APP entity have taken reasonable steps? (Clause 8.15)

The Draft Guidelines state:

> *"It is generally expected that an APP entity should enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs…"*

The Associations have two main concerns with this requirement:

1. Is this requirement retrospective? That is, will APP entities be expected to re-visit contractual arrangements with multiple overseas parties to ensure compliance with APP 8? If this was the case then the burden to comply with this clause will be extremely onerous and challenging.

2. The logistical challenges of dealing with large overseas organisations who, in most cases, have standard contractual terms that they require their contractual partners to sign up to. It may not always be possible to include, the specific requirements of the Australian Privacy Principles. This is not to say, however, that the Australian Privacy Principles will not be complied with in these circumstances.

In the Associations' view, the OAIC has grossly underestimated the difficulty of complying with this requirement. Contractual negotiations with large, overseas companies often require APP entities to accept the standard agreements and terms dictated by those companies. Further, it is highly unlikely that these large overseas companies would accept amendments to their standard terms as a result of the specific requirements of Australian law. As such, more practical guidance would allow the flexibility for APP entities to undertake their own risk assessment relating to the likelihood of a breach of the Australian Privacy Principles in each circumstance.

As such, the Associations seek clarity on what is required in relation to this clause and what will be considered to be 'reasonable steps' to comply.

Disclosure of Personal Information – Subject to a Similar Law or Binding Scheme (Clause 8.17)

The Draft Guidelines state that an APP entity may disclose personal information to an overseas recipient without complying with APP8.1 where:

> *"The overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way APPs protect the information"*

The Associations request that the OAIC be more precise when it allows for this exception to satisfy compliance with APP8.1. That is, the OAIC should provide a list of jurisdictions that meet the OAIC's view of a 'substantially similar' scheme. Without doing so requires the APP entity to make that judgement and, in turn, makes these Guidelines less helpful.

Withdrawing Consent (Clause 8.31)

The Draft Guidelines state that *"If an individual withdraws their consent, the entity must no longer rely on the original consent when dealing with the individual's personal information"*. The Associations request clarity regarding whether an APP entity would need to require the overseas recipient to de-identify the individual's personal information already in its possession.

APP 9 – Adoption, Use or Disclosure of Government related identifiers

The Associations request that at Clause 9.25, the Guidelines include a specific example, relevant to the telecommunications industry, in which it is reasonably necessary to use or disclose a government related identifier. That is, the standard identification check procedure that is used by telecommunications companies – as well as other businesses – necessarily requires the use and disclosure of government related identifiers. This should be included as an example of a reasonable use.

APP 10 – Quality of Personal Information

Examples of Reasonable Steps (Clause 10.9)

The Draft Guidelines give an example of reasonable steps that an APP entity could consider to ensure the quality of personal information as follows:

> *"reminding individuals to update their personal information each time the APP entity engages with the individual"*.

The Associations object to the inclusion of this example as a 'reasonable step'. It would be unnecessary, irrelevant and burdensome to both the customer and the APP entity to require a reminder to update personal details during every contact with a customer. Customers may ring their communications provider for a range of reasons, most of which are unrelated to updating personal details.

Further, many companies have invested significant resources in educating and empowering their customers with numerous options - including online options – to take responsibility for, and maintain the accuracy of, their personal information. These efforts should not be undermined by a requirement to remind an individual to update their details during every interaction.

Complete (Clause 10.20)

The Draft Guidelines provide a meaning of 'complete' as taken from the Macquarie Dictionary. The Associations contend that this meaning is not helpful from a practical sense. This is particularly concerning when there are a number of limitations regarding what

information an APP entity is allowed to collect and how it is so closely aligned with what an individual has consented to. It is possible that the definition of 'complete' as it is currently drafted, will serve to contradict other elements of the Draft Guidelines which relate to only collecting the information directly related to the primary purpose of consent.

In a practical sense, APP entities would have great difficulty in providing relevant and consistent training to its staff based on the guidance provided in the Draft Guidelines. The Associations request that further consideration is given to this definition and how it may be applied in a practical sense. We would support the inclusion of a new definition which provided greater clarity relating to what 'complete' means in the context of these Guidelines.

APP11 – Security of Personal Information

What are reasonable steps? (Clause 11.5)

Under Clause 11.5, the Draft Guidelines reference the adverse consequences for an individual if their personal information is not secured. The Associations contend that this clause should also reference APP 8. Referencing back to other relevant sections would ensure that the Guidelines are consistent.

Clause 11.7
The Draft Guidelines reference the OAIC's *'Guide to information security: 'reasonable steps' to protect personal information'*. Is it likely that this Guide will be amended for March 2014?

Personal Information Held by an Organisation (Clause 11.23)

The Draft Guidelines state that:
"where an organisation 'holds' (see paragraph 11.4 and Chapter B (Key Concepts) for a discussion of 'holds') personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information…".

The Associations seek further guidance on whether the obligation applies even when the APP entity does not physically 'hold' the information. If this is the case, the compliance burden would be significant.