Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.htm

8 October 2013

By email: consultation@oaic.gov.au

Re: DRAFT APP GUIDELINES 1 - 5

The Australian Privacy Foundation (APF) is pleased to provide comments on the draft Guidelines for the Australian Privacy Principles 1 to 5.

APF has had the opportunity to review the submissions of the Australian Communications Consumer Action Network (ACCAN) and of the former Deputy Privacy Commissioner, Nigel Waters and is generally supportive of the points made in those submissions.

General Comments

As stated in the draft Guidelines the APPs are the "cornerstone" of privacy regulation in Australia. This is why it is so important that the Guidelines ensure that they meet the following objectives:

1. They are clear and in plain language
2. They provide practical guidance on the interpretation and application of the APPs
3. They support best practice in privacy in Australia.
4. The Guidelines are regularly reviewed to ensure ongoing best practice and guidance (and to take account of recent judicial decisions)

We contend that only some of these objectives have been met. In particular:

1. There is no mention of review, this should be incorporated in the introductory parts of the Guidelines.
2. We have comments below that deal with issues of clarity and plain language
3. The Guidelines equivocate over a number of issues (again detailed below) which does not support best practice in privacy and causes ambiguity.
4. There are not enough practical and detailed examples to provide guidance to individuals and APP entities.

We also wish to raise concerns about the consultation process. The draft guidelines were released in parts with separate deadlines. The APP draft guidelines need to be considered as a whole both in consultation and review of submissions. The process used leads to a

situation where the organisations putting in submissions have a very fragmented view of the Guidelines.

Our general comments are:

1. The introductory chapters are quite long and not easily accessible.

2. Extensive cross referencing to the key concepts within the guidelines for the actual APPs should be added to improve comprehensibility.

3. There should be a box at the beginning of the whole document that summarises the document with a master contents page.

4. The key points at the beginning of each Principle are supported.

5. The Guidelines should be in plain language and avoid technical language as much as possible.

6. There should be lots of detailed examples to provide guidance in commonly occurring situations. The examples should be in boxes and in a different colour. It is a lot easier to understand a key point with a clear detailed example.

7. The language of the Guidelines should be direct language and as specific as possible.

8. A good precedent for best practice guides are the ASIC Regulatory Guides. Where possible the APP Guidelines should be structured and written in a similar way.

9. Given the length of the Guidelines an index should be produced to make the Guidelines more accessible.

10. If there are relevant legal decisions by a Court, Tribunal or the OAIC then these should be mentioned and referenced.

Chapter A – Introductory Matters

Who is covered by the APPs?

This section refers back to the Act. Readers should not have to perform a complicated exercise of legal interpretation to guess the OAIC's interpretation of who is covered. It should refer to clear guidance on which organisations are APP entities and which are not. If this document does not exist it needs to be created and put on the OAIC privacy website, as well as included as a core feature of consultation and guidance documents.

Do the APPs apply to a contracted service provider under a Commonwealth Contract?

A.11 needs to be clear about the obligation being imposed. In particular, what needs to be covered in the contract? What information does the contracted service provider require to be fully aware of the obligations?

Do the APPs apply to a credit reporting participant?

This section should summarise when the APPs apply or apply in addition to Part IIIA of the Act. There has been constant confusion over many years about the interaction of credit reporting and the APP. We contend that:

1. The obligations are summarised
2. Credit reporting examples appear in the APPs to demonstrate instances where the interaction of APPs and credit reporting is significant.

Chapter B – Key concepts

APP Entity

B.5 This section needs to clarify whether a sole trader is a small business operator. There are many sole traders in Australia and their obligations need to be clear.

B.7 should clarify that an agency is a Commonwealth agency.

Collection

B.15 should be clarified. Reading the newspaper is not collecting information but keeping a folder of clippings or saved articles would arguably be collection. The example needs to change or be clarified.

All examples should be separate, highlighted and with sufficient detail to cover the issue. This example needs further detail.

Consent

It is important to model and recommend the most beneficial and trustworthy approach to consent, and distinguish 'bad' or dangerous approaches. Spell out the dimensions of 'good' consent:

1. **Express**, rather than implied

2. Effectively **informed**, rather than uninformed, or formulaically notified

3. **Revocable**, rather than permanent

4. **Prior** to, rather than after the moment for choice

5. **Un-bundled** and un-tied, rather than bundled with other choices that are not necessarily essential for the exercise of the choice

Express or implied consent

Consent is a key right for individuals. This section is important in providing guidance on obtaining consent.

Practical examples should be given of consent and implied consent.

We contend that best privacy practice is to obtain express consent and not use implied consent at all. What was introduced as an ancillary means for dealing with exceptional

situations where express consent was effectively impossible or too difficult to obtain has evolved into the first choice. The presumption and starting point should revert to the 'express consent as first preference' approach, and all efforts should be directed to encouraging a move in this direction.
(In particular, the assumption in many "Big Data" systems designed for the much weaker protections of US law is that consent can basically be inferred or ignored, subject to a vague and unhelpful clue appearing somewhere in documentation the individual is asserted to be bound by. This assumption is inimical to the protection of privacy of Australians. Government and corporate abuses of "Big Data" models have recently become controversial as they come to light, in part because of the disregard of notions of informed consent.)

The impression given by this section is that APP entities can use implied consent as long as they have lots of disclosure. While effective disclosure is important for any consent model, the impression that disclosure can routinely bypass the preference for express consent is a flawed approach.

It is well known that disclosure is often very ineffective. Individuals have had many years of being worn down, and being in effect, trained to ignore the fine print of privacy disclosure statement. Even if the individual read it, they often believe it is not negotiable and will not reveal the key relevant facts in a comprehensible manner, so it is not read closely, or understood.

For disclosure to be effective it needs to be very targeted and highlighted, and tested.

The disclosure suggested in this section would not be well targeted disclosure as it does not provide guidance on what that should look like.

We contend that in relation to the factors for opt-out at B.27 that:

- Compliance with all the factors should be required. By stating "the more that the following factors…are met" encourages APP entities to test just how few factors they can get away with which is a poor result for the privacy of individuals.
- The individual must have received the information. The use of "likely" is ambiguous and difficult to test. The APP entity must demonstrate with evidence that the information has been received. Even with receipt of the information this does not mean the individual will read it.
- Guidance on what "clear and prominently represented" means? Does this mean big print at the bottom of a web page? An outcomes focus should be required: does the information actually get discovered? Do readers actually understand the implications for their choice?
- It is unclear how an APP entity could work out how to comply with ensuring the individual is aware of the implications of not opting out. This lack of clarity will ultimately mean that individuals could get very poor, basic and ambiguous disclosure on the implications.
- Where disclosure is relied on, its use needs to be based on evidence of its effectiveness in making recipients actually aware of the potential risks and implications of their consent. Since the acceptance of risk hinges on understanding the implications of the disclosure, user-centred design or learning effectiveness evaluation methods should be required to be applied to determine whether a disclosure actually works for this purpose of deciding whether to give consent.

- Opting out should be free. It is a concern that the Guidelines mention cost. This should be explicitly prohibited. Cost barriers are inappropriate for protection of personal information security and privacy. If anything, the incentive should go the other way: higher risk choices (for the individual) should be candidates for cost recovery.
- The consequences of failing to opt-out should be articulated clearly for the individual. It is not clear what the OAIC considers to be serious.
- If an individual opts out this must be acknowledged.

Voluntary = revocable

A key feature of the concept of "voluntary" is that the consent can be withdrawn, or is revocable. This should be made clear. (See below.)

Bundled consent

This section defines bundled consent at B.32. Bundled consents are a major problem for individuals.

At B.33 it is stated that bundled consents have the potential to undermine consent. This statements needs to be a lot clearer and more detailed. We contend that bundled consents cause enormous confusion, and the consent is worthless due to the overload of data.

Consent for personal information use and disclosure should be unbundled from other choices. We contend that there should be a clear statement that there is a presumption that bundled consents are not consent.

Current and specific

B.36 gives the individual the right to withdraw consent. As above, revocability is a key feature of 'good' consent. Withdrawal of consent needs to be easy, accessible and include an acknowledgment. Detail needs to be provided on what this means.

There should be some means for confirming that the withdrawal has been acted upon, and the outcome.

If however consent, once given, is intended never to be subject to revocation or withdrawal, this should be treated as a high risk model (since the individual may not fully appreciate the implications of their choice at the time of making it, becoming aware only later), and this risk should be drawn to their attention, with an explicit plain English statement like:

"**WARNING**: Once you agree to consent to give your personal information, we will refuse to comply if you later attempt to change your mind and withdraw your consent, so think very carefully about it before you give consent. It's your one and only chance."

<u>Consent must be Current</u>

When information and business systems change significantly, the consent may no longer be based on the new use model and the implications for the individual, so past consent based on earlier information and previous system parameters may need to be considered as no

longer current, and sought again, with information about the changes compared to the last version for which consent was sought. Guidance should be given for when this should be done. In particular, a trigger should be when new third parties, especially offshore third parties, gain access to the information, or new uses are to be made by third parties already disclosed.

Consent must be Specific:

The individual should be able to discover, before giving consent, the names of ALL third party companies and agencies who have and will be given access to and use of the personal information. There is often no practical reason to oppose such specific disclosure other than not wanting the individual to know the full extent of such third party disclosures. This sort of information is now a trivial matter to publish and collate online. (The list need not clog up the main disclosure statement, a simple online link will both avoid this clogging and enable those interested to discover the entities.) The list of such third party entities should be treated as a key element of the disclosure. It is no longer acceptable to just say 'we give access to our friends and partners'. The obligation to disclose the specific names, and keep the list up to date, should be considered a core reciprocal obligation to balance the exposure of the individual to those entities. It should not be permitted to be treated as secret or confidential.

Use

We have major concerns about the comments in B.109. We contend that the definitions on use, the interpretation of APP 1 (1.25 to 1.28) and APP 8 need to be consistent. See further discussion on this point on APP 1.

Chapter C – Permitted General situations

General comments

This chapter deals with exceptions to APPs. It is a serious matter to breach Privacy even if there is an exception and it is needed.

Our comments are:

- The Chapter needs to make the obvious point that even if there is an exception it is a serious matter to breach the privacy of an individual.
- The APP entity needs to have clear procedures in place
- The guideline needs workable examples
- The APP entity needs to keep detailed notes about the circumstances

Suspected unlawful activity

A "serious nature" needs to be defined and clarified. Is serious misconduct providing a false detail on an application form? Our experience is that there are a wide range of interpretations of "serious".

In addition, it is important that the “suspicion” be specific in relation to time, person and place. Recent abuses in the US have shown the extension of “suspicion” to cover generic, permanent, and whole of population surveillance.

It must be very clear (perhaps with an explicit statement) that this is a one-off, case by case anomaly, not an invitation to say in effect “everyone could be an offender, so we suspect everyone, so we can implement permanent ubiquitous collection in breach of the APPs”.

Alternative dispute resolution processes

It is not clear in this section whether the following processes are covered:

- Using an external dispute resolution scheme such as the Financial Ombudsman Service; or

- The Privacy Commissioner’s dispute resolution process

Chapter D – Permitted health situations

General comments

Given that networked electronic health records are likely to become the norm for all Australians, and they are created and used in an inherently complex environment, one focus of health care privacy regulation should be to move towards a coherent, accepted national electronic health records privacy and personal information security framework, simple and short enough for informed patients to use as the basis for understanding the rules governing how these records are handled, but detailed enough to describe the key features of the information, rules and entities involved. The continuing absence of such a framework creates an impenetrable barrier of complexity for those seeking to understand how the system as a whole fits together, and creates risk because of this.

The Guidelines should look forward to the creation of such a coherent overarching EHR privacy and personal information security framework, and encourage disclosures about specific health situation practices to be written to fit with it.

APP 1- Open and transparent management of personal information

We strongly support:

- Open and transparent management of personal information
- Easy access to plain language privacy policies, which are detailed enough to understand how they apply in common situations

The current situation in Australia is that individuals have:

- Very little understanding of where and how their personal information is held
- No idea how to manage their personal information
- Difficulty requesting their information; and
- Difficulty locating and reading privacy policies

While we strongly support encouraging a layered approach to privacy disclosures, the Guidelines have not address the other key problems which are:

- Finding the Privacy Policy in the first place. Currently privacy policies are often very well buried. Detailed guidance should be provided on making the policy prominent and accessible. An example should be provided of best practice.
- In addition, privacy policies are often split into multiple components with different names, no dates or version numbers, and held in separate places or parts of an online site. (Facebook and Google are good examples.) They should be required to be collated into one document, or a set of documents presented as part of a single coherent group. Where there are many different services from one provider, the policy should make clear which elements apply to which policy, ideally by providing a complete service-specific policy for each service, so the reader can find the full policy applicable to their use of a given service, not embark on a collation and combining exercise.
- Examples given on how to make the privacy policy usable for individuals not just as disclosure but to solve privacy questions and disputes.
- In particular, user-centred design or learning effectiveness evaluation methods should be required to be applied to determine whether a policy and disclosure actually works for this purpose (as well as for the purpose above of informing the decision to give consent).

Accessing and seeking correction of personal information

At 1.21 the second bullet point refers to a contact person. It should be a contact department or role given frequent staff changes (as suggested on the line below).

The contact method for this department or role should always include all of the following: the full name of the corporate entity, a postal address, a telephone address, a fax number, an email address, and a web address.

Likely overseas disclosures

The outcome that is important here is that individuals are aware where their personal information is going. The Guidelines need to be completely clear about:

- How the information could end up overseas
- The role of clouds and overseas servers
- Routing of information
- The likely risks of data being removed from the jurisdiction of the APPs and OAIC, and hence of easy remedies for breach
- The degree to which the local data collector/user remains liable for abuses occurring out of Australia
- The relevance of on-shore handling of personal information by corporate entities which are subject to extraterritorial application of foreign law and regulation: do purported claims by a foreign government or litigant for access to personal information held on servers in Australia by a company regulated by that country have precedence over obligations imposed by the APPs? If not, how are conflicts resolved?

In our view, it is the reasonable expectation of a consumer that if their information leaves the country by any means then it is going overseas. This includes routing, servers, clouds and any other technical steps.

The Guidelines have to be clear, otherwise it is very likely that APP entities will simply argue for a technical loophole to avoid disclosure. This undermines the individual's control of their personal information.

We strongly recommend that the Guidelines are reviewed on this issue and:

- The Guidelines are clear and consistent on cross border information flows
- Eliminates loopholes by providing specific guidance on this
- Providing detailed examples
- The implications for data held in Australia by offshore companies is spelt out

To ensure it is clear to the APP entity on how to comply with this requirement, the word "likely" needs further clarification. For example, if the APP entity has sent personal information to that country before it should be disclosed as likely. In addition, if contracts are being negotiated with overseas service providers it would also then be "likely".

Further guidance should be provided on "impracticable". Given the rate of advance in Big Data and similar cloud capabilities, even if impracticable today it will often become practicable to implement restrictions the next round of technology changes. The Guidelines should assume that most such barriers will be amenable to routine elimination and require this to be written in to IT maintenance and change plans.

APP 2- anonymity and pseudonymity

Anonymity and Pseudonymity are key individual rights. Valuable in themselves, they are also essential to the exercise of many other personal and social rights including freedom of speech, association and belief.

They are deeply threatened by recent corporate and government initiatives, against the interests of individuals, designed to undermine them. The Guidelines should bring strong efforts to bear in support of their exercise in the face of these threats.

Pseudonymity

In relation to 2.6 another common example of pseudonymity is that of artists who wish to have a separate professional name. Add in some names for this, like "pen name", or "screen name", or the like.

Providing anonymous and pseudonymous options

2.13 deals with the privacy policy providing options for anonymity and pseudonymity. It states that "more" than a simple statement is required. There is no detail on what more is required. A list of matters and practical examples should be detailed in this section.

Given the active threats to the concepts and legitimacy of anonymity and pseudonymity, it would be worth including a simple statement that they are key individual rights, protected by law, and should be presumed to be offered as an option in every interaction.

The details listed at 2.14 do provide some practical examples to facilitate anonymous or pseudonymous contact, but this does not deal with information that should be contained in the privacy policy.

Requiring identification – impracticability

This section needs to clearly define the difference between "impracticable" and "required or authorised by law". The impracticable list of examples should be short. In particular, if the impractical provisions are being relied on for cost then the Guidelines need to provide an example of this.

APP 3 Collection of solicited personal information

Solicit and collect

We contend that this section needs to cover the requirement that the APP entity is required to have a clear system in place to record and identify the collection of personal information.

Collection for an APP entity's "functions and activities"

As the functions and activities are critical to defining whether collection is permissible, it would be useful to provide guidance on how this might be applied. For example, the functions of the organisation may be very narrow (and described in an annual report) and yet the activities are very wide-ranging. How are these issues determined?

The objective test described at 3.21 is a technical legal test. It would be useful to provide a detailed example on how this test could apply.

Collecting sensitive information

See comments above on Chapter C.

Collecting by lawful and fair means

The list at 3.65 should be expanded to include further examples including:

- Collecting by telephone where the purpose is misrepresented or unclear
- Collecting by requesting extra irrelevant information in competitions
- Collecting by pretending to be a charity or researcher

APP 4 – Dealing with unsolicited personal information

What is unsolicited personal information?

Paragraph 4.4 should be amended to provide guidance on how and by whom information is classified. A procedure needs to be put in place to ensure this occurs.

In relation to 4.6, the second example appears to be inappropriate. Ministers and Government departments should have a procedure of responding to correspondence.

The example in 4.7 is a good example and should be highlighted and further detail included on how to deal with the unsolicited information.

Thank you for your consideration.

Yours sincerely

Katherine Lane
Board Member
P: 02 82041350
E: kat.lane@cclcnsw.or