Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

29 October 2013

By email: consultation@oaic.gov.au

Re: DRAFT APP GUIDELINES 6 -11

The Australian Privacy Foundation (APF) is pleased to provide comments on the draft Guidelines for the Australian Privacy Principles 6 -11.

APF has had the opportunity to review the submission of the former Deputy Privacy Commissioner, Nigel Waters, and we are generally supportive of the points made in his submission.

General Comments

The general comments made in our first submission still apply to Guidelines 6 to 11. Our 1st submission dated 8/10/13 available at http://www.oaic.gov.au/privacy/privacy-engaging-with-you/current-privacy-consultations/draft-australian-privacy-principles-guidelines/submissions-on-the-draft-app-guidelines-2013.

The additional general comment that we will now add is the importance of incorporating the findings of the *Community Attitudes to Privacy Survey,* Research Report 2013 (the Report). The Report was released after our first submission. We commend the OAIC in continuing to commission these reports.

A remarkable omission from the Survey, noted in the media, was any question about digital spying on Australians by local and foreign governments. This is the great international privacy controversy of the age, and has been clearly on the public agenda in Australia since attempts to discourage public discussion of long term Data Retention proposals failed in 2012. The question of how to protect privacy from the expansion of law enforcement Big Data tools into territory once protected by effective judicial oversight is central to this. The APPs must cover this question, so a decision not ask about it is questionable.

We note also, as a further sign of failure to engage stakeholders from the “data subject” side, that the regulator has ended the previous practice of having regular interaction with community, consumer advocacy and individuals, while jointly hosting events with industry and government. The danger of “regulatory capture” is raised in these circumstances.

It is vital that the key findings of the Report are addressed in developing the APP Guidelines but there is no evidence that this has been done in developing the Guidelines. There are no references to the Report in the Guidelines and there is little point in surveying individuals if those findings don't inform the work of the Privacy Commissioner in developing best practice in privacy. It is noted that the Report found that 82% of the surveyed participants are aware of the privacy laws. The corollary question is whether any of those surveyed could understand the privacy laws and find them accessible and understandable? This question should also be applied to the Guidelines as our concern remains that the Guidelines are not accessible or easily understood.

APP 6 – Use or disclosure of person information

Individuals often feel that they have no control of their personal information. The Report found that 33% of the survey participants had problems with the way their personal information was handled in the last year. This is a high percentage given the very busy lives of individual Australians.

APF contends that a key part of the individual's control of their personal information is to ensure that the interpretation of secondary purposes must be very narrow. This is critical to protect the erosion of the "purpose" test, at the heart of the Privacy Principles model, in the face of relentless attempts by government and business to constantly extend the uses of data for purposes, which are neither essential nor reasonably incidental to the original transaction. Big Data tools in particular (when used for personal information rather than the unproblematic non-personal data for which they are well suited) are based on the fundamentally anti-privacy assumption that once collected, the presumption should be that personal information is fair game, available for any new use or purpose. Every weakening of the primary purpose focus potentially represents a weakening of personal information security and privacy, in favour of exploitation by the collector and others in circumstances where typically the individual carries the extra risk but is unaware of the details of those unrelated uses and purposes.

We acknowledge the complexity of the primary versus secondary purpose distinction and its implications when APP 6 is applied. However, we don't think the Guideline provides adequate guidance and in some respects is contradictory. In some areas it encourages a broad definition of primary purpose to avoid subsequent difficulties, while in others it supports a narrow view of both primary and secondary purposes. We suggest that the core issue is 'reasonable expectations' (of the individuals), and examples can and should be provided of where that test might support broad definitions, and where in other circumstances it may suggest a narrower interpretation.

<u>Hold, Use, disclose and purpose</u>

The Guideline does not adequately address the issue of whether there can be more than one "primary purpose".

The Guidelines need to make it very clear how primary purposes and secondary purposes are determined and give clear examples. In addition, examples should never be hidden in block paragraph text but instead should be highlighted.

Use or disclosure for a secondary purpose

As stated above this is a key concern for individuals. A key privacy right is for an individual to control their personal information. The Report found that 97% of the surveyed participants objected to information being used for a purpose other than the reason it was given. This is a resounding objection by individuals to the use and disclosure of personal information for a secondary purpose.

It is also noted that a secondary purpose can often in practice translate into more than one secondary purpose, with new secondary purposes, if accepted, as a routine extension or erosion of the primary purpose, being added to indefinitely, thus negating the benefit of the primary purpose test. The history of privacy law in Australia is too often characterised by this invisible incremental erosion of the effectiveness of originally clear protective principles, so it is important to remove the foundation for built-in incremental scope creep from the APPs.

Using or disclosing sensitive information with the individual's consent

We reiterate our comments on Chapter B and consent. In summary, the principles of meaningful consent must be stated in the Guidelines:

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

If the above issues are not addressed adequately in the Guidelines then the problems with consent will continue. In particular, the standards of consent must be very strict and high for the APP entity to use the personal information for a secondary purpose. This is a purpose the individual would not expect or anticipate. We argue that where consent is the basis for use and disclosure, the consent must be:

1. Express not implied
2. Informed
3. Revocable at any time with written confirmation of the revocation
4. Before use
5. Not bundled in any way and completely separate

A key test of whether consent is "informed" is whether, if the information is distributed to other third parties, the individual must be in a position to tell who all those other parties are (including 4th or subsequent steps, if the third parties on-forward the information further), prior to giving consent. At present, the expectation of "informed" consent is too often treated in practice as satisfied if the Disclosure describes merely the general class or category of recipients -- as if subsequent transmission to say a large number of unidentified 'partners', in unspecified jurisdictions, for unspecified or generic purposes, and with potential for further transmission onwards, were a 'trustworthy' business model.

For transparency, security and a reciprocal relationship with such third parties, it is important that if an individual's information will fall into the hands of a particular entity as a result of giving consent, especially if they are in another jurisdiction or if they may on-forward it to others, the person should know who the entities will be. It must become the exception rather than the rule for the Disclosure on which Consent is ostensibly founded to say in effect "we can't tell you which third parties it will go to because our practices are so sloppy we don't know, and we don't know who they will send it to because we don't know or care".

Using or disclosing information where reasonably expected by the individual

The third example at the top of page 7 seems to be a recipe on how to use personal information for a secondary purpose by:

1. Burying the secondary purpose in a fine print privacy policy using lots of technical jargon; and then
2. Notifying somewhere in a bundled notification

If the above scenario is not the intention (and it should not be the intention) then this example needs to be deleted. The examples used need to be a lot more specific about how the "reasonably expect" requirement would work in practice. In our view, the standard of "reasonably expect" must be a high standard. Individuals do not think about secondary purposes and as such do not read privacy policies looking for potential secondary purposes. The individual never reasonably expects a secondary purpose except in the examples 1 and 2 outlined in the Guideline. In fact, for an individual any use for a secondary purpose (apart from example 1 and 2 being an obvious right of reply) is just trickery unless the individual meaningfully and consciously consented.

Again, a claim that someone 'reasonably expects' their information to be used by a third party is best satisfied by actually telling them up front exactly who the third and 4th etc, parties will be. Not revealing the actual identity (company name) of all the other parties - particularly those in other jurisdictions or those who may on-forward your personal information - should be framed in the Guidelines as the basis for a presumption that individuals would not reasonably expect their personal information to go to those un-named third and fourth parties. This reverses the situation at present where it seems to have become routine to both conceal these third party identities behind a vague category description ('our partners'), but then to claim 'you should have known'. Individuals are increasingly left to do their own due diligence as to the trustworthiness of recipients. Meaningful decisions rely on being able to assess the trustworthiness of particular identifiable and researchable entities, not of a vague category to which they belong ('partners'). There is no reasonable basis for granting third and fourth party recipients such anonymity when the individual is claimed to reasonably expect them to be recipients.

Related secondary purpose

The first example used at 6.25 is problematic. The problems are:

1. The debt collector obtains the personal information about the debtor by disclosure to them as an agent or by assignment of the debt. The personal information was actually collected by the original creditor for the purposes of providing a loan or

service. The primary purpose of the collection of the personal information is not collection of the debt.
2. Based on the above observation the secondary purpose (as disclosed in the example) is either not related at all to the primary purpose, or related but outside 'reasonable expectations'.
3. That the secondary purpose may be covered by a bundled privacy consent the consumer signed when they entered into the loan, but as we have suggested above, such bundled consents are unacceptable.

Overall, the example does not make sense as a related secondary purpose and should be deleted. This example also demonstrates how ambiguous the meanings of primary purpose and secondary purpose are.

The second and third examples may demonstrate the related secondary purpose test, but could also be seen as a 'reasonably expected' part of the primary purpose.

A similar comment applies to 6.27 on the issue of "directly related secondary purpose". The individual should provide consent for the disclosure in the example. Unless the clinic manager is part of the same organisation as the health service provider, then consent is required to disclose the information. Again the example is ambiguous and should be either clarified or deleted.

We strongly contend that there needs to be some better examples of common situations (that are non-exhaustive) that set out when personal information cannot be disclosed for a secondary purpose.

Note that a mechanism should be required where the party seeking to rely on Disclosure and the use of examples to bring to notice takes reasonable steps, perhaps using 'User Centered Design' and/or 'Learning Effectiveness Evaluation' techniques, to ascertain whether the disclosure is effective in getting the person to understand what will actually be happening, and who will actually be receiving the information. If Disclosure for informed consent purposes are ineffective in conveying the meaning to the recipient person, this should be discovered and corrected prior to use of the Disclosure form of words, and also, if uncorrected, should cast doubt on the effectiveness of the Disclosure to actually inform. At present an incomprehensible disclosure of secondary purpose or non-specific description of third party recipients works to the benefit of the collector, since it is taken to be effective for legal purposes without consideration of whether it is effective in practice for communication purposes. This gives an incentive to provide such legally useful but practically useless Disclosures; an obligation to check whether the Disclosure actually works, and a negative consequence for those which don't, is a necessary corrective for this perverse incentive.

APP 7 – Direct Marketing

The Report found that 59% of surveyed participants being annoyed by unsolicited marketing activity and it is generally expected that this annoyance will continue to rise. Of particular note is the millions of Australians who have joined the Do Not Call register clearly indicating that they do not want to be contacted by direct marketers.

<u>Using and disclosing personal information for the purpose of direct marketing where reasonably expected by the individual</u>

Our comments on this section:

1. The Report has revealed that direct marketing is often an unwelcome intrusion of privacy. Accordingly, the ‘reasonably expects’ standard needs to be high.

2. The examples of when direct marketing would not be reasonably expected, should be clearly listed and contain more detail.

3. Specific examples need to be used. For example, signing up for a particular regular report does not mean the individual wants to receive every possible offer from the organisation. Many organisations use a bait and switch approach to get consumers interested in specific information only for the individual to end up with an “inbox” full of unrelated direct marketing.

4. The list at 7.16 is not sufficient for an individual to reasonably expect direct marketing. For example, consent by bundled consent, a small print privacy policy, a bundled notification and small print about opt-out does not constitute a reasonable expectation of direct marketing. All of these criteria could be met by burying the individual in information they never read.

Individuals should have confidence that an APP Entity cannot in the vast majority of circumstances rely on the reasonable expectation provisions. To ensure this is implemented the list at 7.16 needs to give very specific examples.

Of particular significance is the non-consensual marketing facilitated by Online Behavioural Advertising (OBA), and the necessity of implementing a Do Not Track law which gives effect to an individual's decision not to be tracked by Third Parties. This will become the dominant form of direct advertising, so APP 7 should clearly cover this.

Existing industry attempts to offer choice and respect consent are an almost total failure, with key industry bodies implementing schemes which, if the individual is saying "I do not trust your trackers, cookies and spyware, I do not want to be tracked by certain or all third parties", in effect respond by saying "you must accept another cookie from us, which many of us ignore". In addition, key online direct marketing providers have a history of attempting to subvert user browser choices. The APP 7 must include language indicating that online Do Not Track choices are legally required to be respected, in the same way as the Spam Act requires Unsubscribe notices to be effectively dealt with in a reasonable time.

It should also be made clear that all forms of tracking, cookies, bugs and spyware which permit insertion of data onto a person's device or enable "fingerprinting" or otherwise identifying their device or communications software should be included in the category of "personal information", since as former Privacy Commissioner Crompton said recently at NICTA, in the age of Big Data, re-identification is to be assumed to be possible; it is clearly the aim of the direct marketer to be creating a psychographic profile of a particular individual, since it is for them that advertisements are being tailored, so there should be no room to insist, as some foreign bodies do, that those OBA programs based on tracking etc. are somehow not dealing in personal information."

It is probably not appropriate to expect an equivalent of a new Spam Act each time a new mode of online direct marketing is developed; it should be governed by APP7.

Our comments above also apply to the section from 7.23 onwards.

Providing a simple means for "opting out".

It is not easy for individuals to opt out. The opt out procedure is difficult to find and often requires a phone call for written contracts. That phone call leaves you on hold for a long time and with no confirmation of success. It would be useful for the OAIC to survey just how difficult it is to opt out for individuals.

At 7.20 the most important point of a simple opt out process is missing, that is, where to find the opt out.

1. In email communications the unsubscribe button is often located in very small print at the bottom of the direct marketing. The print size needs to be compulsorily increased to 12 point and specific words outlined to be used by the APP Entity. This is necessary because there are systemic problems with APP Entities hiding the opt out in fine print. Individuals should expect what the opt out will say and be able to read it.

2. Individuals need to know exactly where to look for an opt out process for APP entities where the contract was formed in writing. Individuals should have a range of options including:

    a. That there will be an opt out in the privacy policy of the APP Entity on its website. The link to the privacy policy must appear on the home page and be a minimum of 12 point font size. The opt out must be the first matter dealt with in the privacy policy and contain a prominent and clear process.
    b. The privacy policy must also include a phone number to call and opt out and an address.
    c. An individual must be able to contact the APP Entity and opt out using any contact method for the APP Entity i.e. calls or emails should be re-routed – entities should not be able to insist on opt-out only being by the advertised channel.

<u>Requests by an individual to stop direct marketing communications</u>

We contend that a request to stop direct marketing communications is just not acted on by APP Entities. It is very easy for an APP Entity to make a "commercial decision" to continue the direct marketing as any breach is unlikely to involve enforcement action as it is difficult for the consumer to prove the opt out. For the opt out system to work, the individual needs to be notified that the opt out was successful.

'Opting in' is of course the preferred approach for all personal information collection (one implemented by the Spam Act), in part because you know who you are dealing with.

'Opting out' requires knowing who is tracking or recording or collecting data about you. There must be a mechanism that requires first party APP entities who facilitate third parties (especially from other jurisdictions, or who on-forward to 4th or other parties) to track, bug, surveil or collate psychographic advertising profiles from the first party's site, to be obliged to also facilitate the individual wanting to opt-out.

This is another reason for the proposal for Informed Consent above to require first party operator Disclosures to list and identify all these third parties, not just to say "we use cookies and allow our partners to do so as well".

Typical OBA tracking schemes involve as many as 40-100 third parties inserting tracking tools from a given online page, often without the knowledge of the primary operator (for instance, the Ghostery ad-industry tool for users is apparently often also used by site operators to find out exactly who is using their page to infect users). This reinforces the requirement that Disclosure statements should identify all the third and subsequent parties whose access to the person's information may be facilitated by the primary collector's site. Opt-out for OBA tracking purposes or the like must requires specific Disclosure of each entity whose tracking, otherwise the individual cannot work out who to opt out from, or to contact. Existing industry schemes are completely ineffective to assist robust and complete exercise of Opt in or Opt out choices.

(Note that it is increasingly the practice for personal, government and public sector web sites to deliberately or inadvertently become host to third party OBA tools, so this is not restricted to commercial sites.)

APP 8 – Cross border disclosure of personal information

The AGS fact sheet < http://www.ags.gov.au/publications/fact-sheets/Fact_sheet_No_29.pdf> notes 'disclosure' does not include "personal information is routed through overseas servers. However, if third parties access that information, this will be a disclosure to which APP 8 applies." The advice in the OAIC draft Guideline is ambiguous about when use of servers located overseas would constitute a use and when a disclosure

In the light of recent revelations of widespread third party access to overseas servers, and concerted efforts to undermine the security tools which are used to exclude unwanted access, it is probably appropriate to require that all hosting on overseas servers be treated as a 'disclosure', as it can no longer be assumed that historically accepted security measures or arrangements will be effective in ensuring that third parties cannot access them.

APP 8.1

Reasonable steps to ensure compliance

This must involve, where a third party such as a Cloud host is involved, explicit contractual or binding obligations, ideally enforceable beneficially by the individual affected, to comply with best practices under the APPs. Where a contract is unilateral, non-negotiable and not supplemented by explicit enforceable undertaking, accessible to the user, about such compliance, it is not possible to conclude that reasonable steps have been taken. This may come into conflict with the practice of some global service providers to behave in just such a manner. (The Swedish Data Inspection Board concluded on 10 June 2013 that the lack of contractual certainty over how personal data may be mined or processed, and lack of knowledge about which subcontractors may be involved, precluded assessment of effective compliance with data protection obligations, and it therefore prohibited the nation's public sector bodies from using an offshore Apps cloud service: http://www.datainspektionen.se/press/nyheter/2013/fortsatt-nej-for-kommun-att-anvanda-molntjanst/ and see also http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/. While the detailed obligations are of course different, the experience of cloud contracts failing to offer any real basis for assessment of reasonableness of compliance steps is directly relevant.)

Another issue is proper identification of all likely and possible third parties with access to the information (the point made above). The agency should require complete and detailed lists of all such entities, and make this available for access by the person."

Exception 1

Another enforceable law that affords substantially similar protections: in the light of recent reconsideration by European agencies of the appropriateness of reliance on 'Safe Harbor' models, there should be no presumption that 'Safe Harbor' type models offer substantially similar protections."

Paragraph 8.24 must include the word ‘binding’ before ‘scheme’ – the Explanatory Memorandum has been misquoted, and this is a very significant omission.

Exception 2

Informed consent: We repeat the point above that Informed Consent must be based on Disclosure of the actual recipient entities, not just the general category of recipients. Only where individual agencies may not be named explicitly by law should they be indicated by general category.

Exception 4

Permitted general situations: "suspected unlawful activity or misconduct in relation to an agency's functions" should be interpreted narrowly, to require specific grounds for suspicion of particular offences, rather than generic, not specifically based suspicion that someone somewhere might be doing something, which would permit almost open-ended breach of

APP 8.1.

Similarly, Exceptions 5 and 6 should be read narrowly and not so as to authorise, on generic grounds, bulk disclosure of personal information for non-specific surveillance purposes, as has been indicated may be tempted to be occurring under the excessively broad interpretation of some offshore surveillance laws. In addition, to enable transparency, providing detailed information for publication about volume, nature, basis of suspicion and effectiveness of audit controls on abuse should be a requirement of taking advantage of these 3 exceptions.

The effect of s6A(4), as explained in paragraphs 8.56 to 8.60, is a major concern. It would appear that any assurances given to individuals about protection of their information overseas will be misleading and worthless, at least in respect of potential access to that information under laws of the overseas jurisdiction. While this may be an unavoidable consequence of s6A(4), at the very least the advice in 8.59 about notifying individuals should be much stronger.

APP 9 – adoption use or disclosure of government related identifiers

This Guideline could make it clearer that APP 9 does not apply to identifiers issued by foreign governments (such as foreign driving licence and passport numbers). Also, the examples given in 9.29 are about collection of identifiers rather than use. Better examples

are needed of uses and disclosures that may or may not be permissible once a government related identifier has been legitimately collected under the collection APPs.

APP 10 – quality of personal information

This Guideline is supported, except that paragraph 10.5 encourages a dismissive attitude to poor quality information, on the basis of a judgment by an APP entity about consequences which they may not be in a position to make. There could be better examples in 10.21 of the 'complete' objective – those given are arguably about accuracy.

APP 11 – security of personal information

This Guideline is supported, but we submit that there should be additional guidance about the need for APP entities not to assume that software or other security 'products' on the market are adequate to meet the requirements of APP 11.

Thank you for your consideration.

Yours sincerely

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