Australian Government
Office of the Australian Information Commissioner

Mobile privacy

A better practice guide for mobile app developers

September 2014

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Office of the Australian Information Commissioner Act 2010*.

All OAIC publications can be made available in a range of accessible formats for people with disability. If you require assistance, please contact the OAIC.

Date of initial publication: September 2013, revised September 2014

Office of the Australian Information Commissioner
GPO Box 2999
CANBERRA ACT 2601
Tel: 02 9284 9800
TTY: 1800 620 241 (no voice calls)
Email: enquiries@oaic.gov.au

This guide is based on *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, published by the following privacy regulators:

Office of the Privacy Commissioner of Canada
Information and Privacy Commissioner of Alberta
Information and Privacy Commissioner for British Columbia

Contents

Introduction

The purpose of this guide

The Office of the Australian Information Commissioner (OAIC) has developed this guide to help mobile device application (app) developers embed better privacy practices in their products and services, and help developers that are operating in the Australian market to comply with Australian privacy law and best practice.[1]

Many of the practices outlined in this guide may also assist other businesses involved in the app ecosystem, such as:

- advertising networks
- advertisers
- mobile platform providers
- app developer trade associations
- developers of other (non-mobile) applications.

This document is a better practice guide. It is designed to provide suggestions for both privacy compliance and better practice. Your business may or may not be covered by the *Privacy Act 1988* (Cth) (Privacy Act). Whether it is or not, this guide will help you make your apps more privacy-friendly.

There is a checklist to help you ensure your app is privacy friendly at Appendix A. The checklist is a summary of this guide. You can follow the checklist to help build privacy protections into your apps. There is also a list of resources at Appendix B if you need more information.

Background

People are increasingly using mobile devices for their computing needs, including to access the internet. In a 2012 Australian study:

- 76 per cent of respondents said that they owned a smartphone, compared with 67 per cent in 2011
- 84 per cent of respondents said that they would own a smartphone in 2013
- 69 per cent of the mobile phone users – and 87 per cent of smartphone users – had installed an app on their phone
- 38 per cent said that they owned a 'tablet' device

[1] Section 5B of the Privacy Act provides that the Act may apply to the acts or practices of an organisation that occur outside of Australian jurisdiction in certain circumstances.

- 92 per cent of tablet owners said that they used apps on their device.[2]

The Australian community puts a high level of trust in the mobile apps they use and their expectation for privacy protection is equally high. Apps which fail to protect user privacy lose user confidence and gain negative publicity.

Failing to protect privacy could also result in a breach of the Privacy Act (see *Application of the Privacy Act*, below). Individuals can complain to the OAIC if they believe that their privacy has been breached by a business or government agency covered by the Act. Alternatively, the Information Commissioner can choose to investigate the way in which your app handles personal information, even if no-one has complained. The consequences of an investigation could include having to change the way your app handles personal information or having to pay compensation to affected users. Where a breach of privacy is very serious, the Commissioner may seek a civil penalty.[3]

Privacy by design

The mobile environment, along with the new app economy it has generated, presents both potential and risks for how personal information is handled. If you are a mobile app developer, whether you work on your own, or for a business or government agency, you should adopt a 'privacy by design' (PBD) approach. PBD aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.[4]

You can build PBD into your apps by applying privacy-enhancing practices throughout the life cycle of the personal information that you handle – that is, its collection, use (including data matching, targeted advertising and analytics), disclosure, storage and destruction.[5] Given the growing popularity of apps, app developers can expect increased scrutiny of the privacy practices in the app industry in the years ahead – by both regulators and the market itself, driven by increasingly informed, discerning and influential consumers. Implementing a PBD approach will help you make sure you are privacy-friendly, whether or not your business is covered by the Privacy Act.

> If your business must comply with the Privacy Act, implementing better privacy practice can also reduce your compliance costs.

2 MM Mackay, *Australian Mobile Phone Lifestyle Index*, 8th edition, September 2012, www.aimia.com.au/ampli and personal correspondence from MM Mackay

3 See www.oaic.gov.au/privacy/what-happens-to-your-privacy-complaint.

4 Definition of 'Privacy by Design'; www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/84.

5 See www.privacybydesign.ca/index.php/about-pbd/.

How does the Privacy Act apply to apps and app developers?

What is personal information?

The Privacy Act regulates the way in which individuals' personal information is handled. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.[6] What constitutes personal information will vary, depending on whether an individual is reasonably identifiable in a particular circumstance, but may include:

- photographs
- Internet Protocol (IP) addresses, Unique Device Identifiers (UDIDs) and other unique identifiers in specific circumstances
- contact lists, which reveal details about the contacts themselves and also a user's social connections
- voice print and facial recognition biometrics, because they collect characteristics that make an individual's voice or face unique
- location information, because it can reveal user activity patterns and habits.

Application of the Privacy Act

The Australian Privacy Principles (APPs) in the Privacy Act set out how personal information should be handled. The APPs apply to most Australian and Norfolk Island Government agencies and some private sector organisations – collectively referred to as APP entities.

All businesses and not-for-profit organisations with an annual turnover greater than $3 million have responsibilities under the Privacy Act subject to some exceptions.

As well some small business operators (organisations with a turnover of $3 million or less) are covered by the Privacy Act including:

- private sector health service providers
- businesses that sell or purchase personal information
- credit reporting bodies.[7]

> You are likely to be covered by the Privacy Act if you use personal information to sell advertising, including through an app.

The APPs cover the collection, use, disclosure and storage of personal information. They allow individuals to access their personal information and have it corrected if it is incorrect. There are also specific APPs that deal with the use and disclosure of personal

[6] Privacy Act s (6)(1). For a more detailed explanation, see the APP guidelines - Chapter B, Key Concepts available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-b-key-concepts.

[7] For more information about the kinds of organisations that are covered by the Privacy Act, see www.oaic.gov.au/privacy/privacy-topics/business-and-small-business/small-business.

information for the purpose of direct marketing (APP 7) and cross-border disclosure of personal information (APP 8).[8] Implementing the steps in this guide will help you to comply with the APPs.

If your business is covered by the Privacy Act, it is important that you understand whether your app is used for **direct marketing** and make sure it complies with the direct marketing requirements of the APP 7.[9]

Make user privacy your competitive advantage

Whether or not you are covered by the Privacy Act, as an app developer, it's ultimately in your best interests to build strong privacy protections into your apps. The mobile apps that take privacy seriously will be the ones that stand out from the crowd and gain user trust and loyalty:

- The 2013 OAIC Community Attitudes to Privacy study found that 62 per cent of Australians opt not to use smartphone apps because of concerns about the way personal information would be used.[10]
- A 2013 survey by the Pew Research Centre found that 51 per cent of teenage app users had avoided certain apps over privacy concerns, and 26 per cent had uninstalled an app because it was collecting personal information that they did not wish to share.[11]
- A 2012 Australian study found that 56 per cent of Australians do not approve of websites showing specific advertising based on information that the websites have collected in the background about their interests. Further, 69 per cent of respondents reported they had refused to use an application or website because it collected too much personal information. 75 per cent of the respondents said they needed to know more about the ways in which companies collected personal information.[12]

8 For a summary of the APPs, see the APP quick reference tool www.oaic.gov.au/privacy/privacy-resources/privacy-guides/app-quick-reference-tool. For more detail, see the full text of the APPs www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles.

9 See Chapter 7 of the APP guidelines, available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-7-app-7-direct-marketing.

10 See www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013#_Toc368300728.

11 See www.pewinternet.org/~/media//Files/Reports/2013/PIP_Teens%20and%20Mobile%20Apps%20Privacy.pdf.

12 C. Arnott and M. Andrejevic, *Internet privacy research: report*, prepared for the Centre for Critical and Cultural Studies University of Queensland, February 2012, http://cccs.uq.edu.au/personal-information-project.

App privacy essentials

This section covers the essential information you need to know when designing, implementing and managing your app. There is a checklist to help you ensure your app is privacy friendly at Appendix A. Remember – think 'privacy by design'!

1. Your privacy responsibilities

It is important to integrate good privacy protections into your day-to-day business practice. You should also ensure that your business arrangements and contracts protect privacy and comply with your obligations under the Privacy Act.

APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that enable compliance with the APPs, and will enable them to deal with privacy enquiries or complaints.

Putting in place a privacy management program for your business will help you manage risks up front. Given the potentially high number of users of your app, it can also help you to respond to requests for access to their personal information and complaints in an organised manner.

Developing and managing your privacy management program

Managing privacy doesn't need to be complicated or difficult. Anyone, from a one-person operation to a large company, can build a privacy management program.

- Identify someone within your business to be responsible for privacy protection and dealing with privacy complaints, even if you only have a small team.
- When you are in the planning stages for an app, conduct a Privacy Impact Assessment (PIA) to help ensure you have considered all the relevant privacy issues (see below for more information).
- Have controls in place (such as contracts) to ensure that third parties process personal information in accordance with their obligations under privacy law and facilitate your compliance with your own obligations, and make sure the controls are aligned with user expectations. Be cautious when using third party code or software development kits — such as those from advertising networks or analytics providers – which could contain code you aren't aware of, such as aggressive adware or malware. A PIA can help establish what kind of controls may be appropriate.

Privacy Impact Assessments

You should consider carrying out a PIA for each app you develop, whether or not your business is covered by the Privacy Act.

A PIA is a tool that 'tells the story' of a project from a privacy perspective. A PIA:

- describes how personal information 'flows' in a project – how it is collected, used, disclosed, accessed, stored and deleted

- analyses the possible privacy impacts of the project on individual privacy
- through that analysis, helps find potential ways to manage, minimise, or avoid privacy impacts while achieving or enhancing project goals
- encourages good privacy practice and underpins good risk management.

You may choose to publish your PIA so that members of the public are aware of your commitment to privacy. You might even wish to encourage privacy organisations or members of the public to consult on your draft PIA. Both actions will help build user trust in your app.

The OAIC has published a *Guide to undertaking privacy impact assessments* which you may find useful.[13] Additional resources and tools can be found in Appendix B.

2. Be open and transparent about your privacy practices

APP 1 requires APP entities to have a clearly expressed and up-to-date APP Privacy Policy about how they manage personal information.

The process of developing a privacy policy will help you to inspect your own practices in a systematic way. Users increasingly expect transparency about how their personal information is handled; businesses which clearly explain this are rewarded with user trust and loyalty.[14] You should tell users what your app does with their personal information, why it does it, and what their choices are. This is the case even if you choose to offer benefits – such as convenience or free downloads – to your customers in return for access to their personal information.

For suggestions about how to implement these ideas, see the OAIC's *Guide to developing an APP privacy policy*[15] and the resources found under the heading *Communicating privacy rules on small screens* in Appendix B.

---

13 Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy.

14 For example, a study in Europe found that a consumer's trust of and loyalty to a website are particularly influenced by whether the consumer feels comfortable with how their personal information is handled. (C. Flavián & M. Guinalíu, 'Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site' (abstract), in *Industrial Management and Data Systems*, vol. 106, issue 5, 2006, at www.emeraldinsight.com/journals.htm?issn=0263-5577&volume=106&issue=5&articleid=1550797&show=abstract). A US study found that 'customers have higher loyalty to sites that request the least information (and) lower loyalty to sites that request the most information.' (JP Lawler, *A study of customer loyalty and privacy on the Web* (abstract), ETD Collection for Pace University, Paper AAI3126207, 2002, at http://digitalcommons.pace.edu/dissertations/AAI3126207

15 Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy.

Your privacy policy

Make your app's privacy policy easy to find; users should not have to search for it. It's best to make the privacy policy (or at least a summary of it, easy to access through your app; see *3. Obtain meaningful consent – the small screen challenge* below).

If you want the collection of personal information by your app to be covered by the same privacy policy as your other activities (such as your website), make sure that the privacy policy adequately covers your app and its functions.

Your privacy policy should, at a minimum, clearly and accessibly[16] notify potential users:

- who you are and how to contact you
- what kinds of personal information your app collects and stores
- how your apps collects personal information, and where it will be stored (on the device or elsewhere)
- the purposes for which your app collects the personal information
- how personal information will be used and disclosed
- how users may access their personal information, and correct it or seek to have it corrected
- how users may complain about a breach of the APPs, and how you will deal with such a complaint
- whether you are likely to disclose the information outside Australia and, if it is practicable, which countries you are likely to disclose the information to.[17]

Sending information overseas

APP 8 imposes specific obligations about sending personal information outside of Australia and you may remain accountable for what happens to that information. If your app sends your customers' personal information overseas, you should make sure that the personal information is still handled in a way which protects your customers' privacy.[18]

As a matter of best practice, you may also want to tell users

- how long you will keep the personal information that your app collects

[16] If your policy may need to be accessed by individuals with special needs, such as an individual with a vision impairment you should put appropriate accessibility measures in place to enable that access. Australian Government agencies are also required to comply with any applicable government accessibility requirements – see, for example http://webguide.gov.au/accessibility-usability/accessibility

[17] APP 1.4 contains a non-exhaustive list of information that you must include in your privacy policy. For more information, see the APP guidelines.

[18] For more information about sending personal information overseas, see APP guidelines – Chapter 8 available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

- whether the users will be 'trading' access to their personal information for benefits such as convenience or free downloads, and
- any other issues that will affect user privacy.

You should have a monitoring process in place to make sure that you and your app handles personal information as described in your privacy policy.

Making changes to your privacy policy, or to how you collect, use or disclose personal information

- Inform users in advance about updates to your app's privacy policy.
- Give users reasonable time to provide feedback before you implement changes.
- Tell users exactly what rules you are changing so they don't have to compare the new and old policies to understand what's happening.
- If you are including new features, especially features that involve disclosing information to third parties, make the changes easy to find and understand through the update process.
- Wherever possible, seek express consent from users to any changes that could impact on their privacy.
- *Never* make silent app updates that will diminish the user's privacy.

Sensitive information

If your app collects sensitive information, you are likely to have additional privacy obligations under the APPs. 'Sensitive information' includes an individual's health information, their membership of a trade union or political association, their sexual orientation or practices, and more.[19]

3. Obtain meaningful consent – the small screen challenge

Your customers need to know about your privacy practices to be able to provide you with *informed* consent to handle their personal information[20] – but it can be difficult and unpleasant to read a lengthy privacy notice on a small screen. Getting the balance right between providing information and avoiding 'notice fatigue' (where people ignore notices or warnings because of over-exposure) is critical. We list some suggestions below.

- **Use short form notices**

[19] For example, see APPs 3, 6 and 7. 'Sensitive information' is discussed in more detail in the APP guidelines – see Chapter B, Key Concepts at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-b-key-concepts.

[20] APP 5 requires that you notify individuals of certain matters when you collect their personal information. See APP guidelines – Chapter 5 at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information.

- These are notices that are no longer than a single screen (if possible) and that explain what data will be collected from users, and any third party data sharing practices - they also link to the full privacy policy and/or terms of use.
- Provide specific, targeted notices to users when they need to make a decision about whether to consent to the collection of their personal information.[21] These notices should contain details about the specific collection so that users can make an informed decision.
- Make sure that the short form notice draws user attention particularly to any collection, use or disclosure of information that they would not otherwise reasonably expect.

- **Provide a privacy dashboard**
  - Display user privacy settings with a tool that allows users to tighten their settings. The tool should be easy and straightforward to use.
  - Instead of just using an on/off button, explain the consequences of making a choice to provide data so users can make an informed decision.

- **Adapt existing mobile privacy policy template language or generators**
  - See *Resources* in Appendix B – but make sure the result meets any obligations you have in Australia under the Privacy Act.

Give users a way to modify their information, opt out of any tracking and delete their profile entirely if they wish. Rather than just using text, your privacy policy can make more of an impact by using the techniques listed below.

- **Graphics**
  - The first layer of your mobile privacy policy could primarily be icons, labels or images, as long they are linked to text that provides more detail.
  - You could also make use of graphics in the app at the moment when sensitive information is about to be transmitted and user consent is required. For example, if your app is about to access the user's location data, you could activate a symbol or icon to raise user awareness of what is happening and the reason for it, as well as the user's choices.

- **Colour**
  - You can alert the user by using colour and altering its intensity. The intensity of the colour could be scaled to the importance of the decision or sensitivity of the information.

- **Sound**

[21] APP 5 requires entities that collect personal information to take reasonable steps either to notify the individual of certain matters or to ensure that they are aware of those matters. See Chapter 5 of the APP guidelines for more information.

- Selective use of sounds, and scaling the device's volume, can draw attention to a privacy-related decision that needs to be made in a timely way.

For further information, including on the use of symbols and icons, see *Communicating privacy rules on small screens* in Appendix B .

Users with disability

Almost 20% of the Australian population has a disability.[22] Your privacy policy and notices need to be accessible to people with disability, such as people who are blind and use screen readers,[23] people who are colour blind, and people who are Deaf or hard of hearing. If you use tools (such as graphics or sound, like those listed below) which are not accessible to people with disability, make sure you offer an alternative way for these users to get the information. For information on ensuring that your app – including your privacy processes – is accessible to people with disability, see *Making your privacy practices accessible to customers with disability* in Appendix B .

4. Timing of user notice and consent is critical

When people use mobile devices, their attention can be intermittent and limited. So it's important to be thoughtful and creative about the timing of user notice and consent.[24] To get the most impact, consider the following:

- Highlight privacy practices during the download/purchase process and also upon first use.
- Obtain consent at the point of download.
- Tell users what will happen with their information in real time – this is sometimes known as providing 'in-context notices'. Users must be able to make timely and meaningful choices. For example, if your app takes photos or video, the first time that the user activates the photo or video function, clearly state if your app will tag the images with location data and allow the user to opt out of this feature.

5. Only collect personal information that your app needs to function

The APPs require that you only collect the personal information that is necessary.[25] Consider whether you need to collect personal information at all.

---

[22] According to the Australian Bureau of Statistics study *Disability, Ageing and Carers, Australia*: Summary of Findings, 2009, available at www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4430.0Main%20Features22009?opendocument&tabname=Summary&prodno=4430.0&issue=2009&num=&view=

[23] A screen reader is text-to-speech software that interprets the content of a screen and reads aloud what is displayed on the screen (such as email, documents or spreadsheets) to enable people with visual impairment to access textual information.

[24] The APP 5 notification statement must be provided at or before the time of collection, or if this is not practicable, as soon as practicable after. See APP guidelines – Chapter 5 for more information.

[25] See APP 3 and the APP guidelines – Chapter 3 at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information.

- If you cannot explain how a piece of personal information is related to the functions or activities of your app, then you probably should not be collecting it. Don't collect personal information just because you believe it may be useful in the future.
- Delete or de-identify personal information that you no longer need for a lawful purpose.[26]
- As best practice, allow users to opt in to the collection or use of their personal information. If that is not practicable, allow users to opt out of data collection. If you cannot enable users to opt in or out, explain this to users first so they can make an informed decision about whether to install your app.
- Don't collect sensitive information about a user at all, unless the user has expressly consented.[27]
- If you are sharing behavioural information or device identifiers with third parties (such as an ad network), your privacy policy should identify those third parties and link to information about how users can contact those parties. Ideally, users should be able to opt out of sharing their personal information with third parties.
- Avoid collecting information about a user's movements and activities through the use of integrated location and movement sensors unless it relates directly to the app and you have the user's informed consent.
- Don't collect sound or activate the device camera without the specific permission of the user.
- It is best privacy practice not to collect and store personal information about third parties from a user's device unless you can obtain the consent of those parties. For example, do not collect and store your user's address book.
- Apps should be designed in a way that does not require you to collect any persistent identifiers if it is not essential to the functioning of the app.
- Avoid associating personal information across apps, or between your app and a user's social media account, unless it is obvious to the user and necessary to do so. If you must make links, ensure that personal information is not linked to a user's identifier for longer than it needs to be. For example, if your app transmits personal information, you should not keep a copy of it unless it is necessary.
- Allow users to change their minds about giving you access to their personal information. If this means that they have to uninstall the app, explain this clearly and simply.

[26] For exceptions to this see APP 11.2 and, for further detail, *Privacy business resource 4: De-identification of data and information* available at www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information.

[27] For exceptions to this, see APP 3.4 and APP guidelines – Chapter 3.

6. Secure what you collect

The APPs require you to take reasonable steps to protect any personal information you hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[28]

- Make someone in your business responsible for security.
- Have appropriate controls in place both on the mobile device and on the backend systems to store personal information securely. For example, you should encrypt user information when it is transferred via the internet or stored.
- Adapt your code to allow for differences in mobile platforms.
- Generate credentials securely.
- Do your due diligence on libraries and other third-party code.
- Don't store passwords in plain text on your server.
- Give users the ability to request the deletion of all of the personal information about them that your app has collected.
- Delete or de-identify personal information that you don't need. Be transparent (for example, in your privacy policy) about how long it will take to delete personal information once a user stops using your app.
- Prepare, implement and regularly update a data breach policy and response plan

See the OAIC's *Guide to information security*[29] and *Data breach notification — A guide to handling personal information security breaches*.[30]

Data breaches

A data breach is when personal information your app holds is lost or subjected to unauthorised access, use, modification, disclosure or other misuse. If you experience a data breach connected with your app, you may need to inform your users.

[28] APP 11 and for more discussion see APP guidelines – Chapter 11 www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information.

[29] Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security.

[30] Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

Appendix A — Privacy and mobile apps: a checklist for app developers

Your privacy responsibilities

Your agency or organisation (which may just be you) is responsible for all personal information collected, used and disclosed by your mobile app.

- ☑ Identify someone to be responsible for privacy protection.
- ☑ Use a Privacy Impact Assessment to map where the information is going, identify potential privacy risks, and assist with privacy planning (including 'privacy by design').
- ☑ Implement practices, procedures and systems that enable compliance with the Australian Privacy Principles, and will enable you to deal with privacy enquiries or complaints.
- ☑ Put in place controls, such as conditions of contract or user agreements, to ensure that third parties accessing personal information through your app respect their privacy obligations.

Be open and transparent about your privacy practices

- ☑ Develop a privacy policy that clearly and simply informs users what your app is doing with their personal information.
- ☑ Make your app's privacy policy easy for users and potential users to find.
- ☑ Put in place a monitoring process to ensure that personal information is being handled in the way described in your privacy policy.
- ☑ When updating an app, inform users of any changes to the way their personal information is handled, and seek express consent to any changes that could impact on their privacy.

Obtain meaningful consent despite the small screen challenge

- ☑ Select the right strategy to convey privacy rules in a way that is meaningful on the small screen. This could include:
  - o 'short form notices', with important points up front and links to more detailed explanations
  - o a privacy dashboard that displays a user's privacy settings and provides a convenient means of changing them
  - o cues such as graphics, colour and sound to draw user attention to what is happening with their personal information, the reasons for it, and choices available to the user.

Timing of user notice and consent is critical

- Obtain consent at the point of download.
- Tell users how their personal information is being handled at the time they download the app and in-context when they use the app to ensure that their consent is meaningful and relevant.
- Consider how best to deliver privacy messages to most effectively capture users' attention and achieve the most impact at the right time, without causing notice fatigue.

Only collect personal information that your app needs to function

- Limit data collection to what is needed to carry out legitimate purposes.
- Do not collect data just because you think it may be useful in the future.
- Allow users to opt out of the collection of their personal information, or if that is not practicable, clearly explain they cannot opt out so they can make an informed decision whether to use the app.
- Delete or de-identify personal information that you no longer need for a lawful purpose.

Secure what you collect

- Put in place appropriate safeguards to protect the personal information you are handling. Use encryption when storing and transmitting data.
- Give users the ability to delete or request the deletion of all of the data that your app has collected about them.
- Publish clear policies about how long it will take to delete personal information once a user stops using your app.
- Delete personal information that you no longer need for a lawful purpose.

Appendix B — Resources

Being privacy-aware

OAIC resources

APP guidelines

Guide to developing an APP privacy policy

10 steps to protect other people's personal information

A guide to handling personal information security breaches

Guide to undertaking privacy impact assessments

Guide to information security

Other resources explaining the APPs in depth.

International regulatory resources

Mobile App Developers: Start with Security (US)

Mobile Privacy Disclosures: Building Trust Through Transparency (US)

Opinion on apps on smart devices (European Commission)

Securing Personal Information: A Self-Assessment Tool for Organizations (Canada)

Summary of US regulations and issues

Tips for mobile apps developers (video) (US)

Industry associations

Please note that the following industry associations are not endorsed by the Office of the Australian Information Commissioner. The service descriptions below were supplied by the organisations listed.

Australian Information Industry Association (AIIA)

'AIIA is Australia's peak ICT industry representative body and advocacy group. [AIIA] advocates, promotes, represents and grows the ICT industry in Australia… [AIIA] members are organisations (not individuals) ranging from SMEs to listed Australian organisations, to multinational or even global corporations.'

For more information, see the AIIA website.

AIMIA – the Digital Industry Association for Australia

'Representing the digital content, services and applications industry in Australia since 1992, AIMIA exists to, encourage and support the growth of AIMIA members and the digital industry at large, act as a medium of education and support for its members and

the industry through a number of services, and represent AIMIA members and the digital industry to the broader business community.'

For more information, see the AIMIA website.

The Application Developers Alliance

'A non-profit industry group founded to serve developers, the people who power and expand the world through software. It works to ensure that developers have the tools, network, and policy environment they need to innovate. It champions the work that developers do through every channel open to it.'

The App Developers Alliance contributed to the Mobile app voluntary transparency screens.

For more information, see the App Developers Alliance website.

The Association for Competitive Technology (ACT)

'An international grassroots advocacy and education organization representing more than 5000 small and mid-size app developers and information technology firms.'

ACT contributed to the Act4Apps Education Initiative and initiated the App Trust Project, which includes privacy-related icons.

For more information, see the ACT website.

Association for Data-driven Marketing and Advertising (ADMA)

'As Australia's largest marketing and advertising association, ADMA protects, supports and champions excellence in data-driven marketing and advertising in Australia and beyond.'

For more information, see the ADMA website.

Australian Web Industry Association (AWIA)

'AWIA is the representative body for the Australian web industry, and was created to bring together like-minded industry professionals to promote learning, interaction and personal development.'

For more information, see the AWIA website.

Network Advertising Initiative (NAI)

'The NAI is the leading self-regulatory association comprised exclusively of third-party digital advertising companies. The NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for online advertising purposes. Our organization also educates and empowers consumers to make meaningful choices about their experience with online advertising through an easy-to-use opt-out mechanism.'

The NAI has released a mobile application code, which focuses on privacy issues.

For more information, see the NAI website.

Selected privacy-related guidance for app developers

The Association for Competitive Technology, Act4Apps – educational events, development and UI tools for app developers

California Department of Justice, Privacy on the Go: recommendations for the mobile ecosystem, January 2013

Digital Advertising Alliance, Application of self-regulatory principles to the mobile environment, July 2013

Electronic Frontier Foundation, Mobile User Privacy Bill of Rights, March 2, 2012

Future of Privacy Forum and the Center for Democracy & Technology, Best Practices for Mobile Applications Developers (July 2012) and the Future of Privacy Forum's site for app developers

GSMA, Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development, February 2012; also see GSMA's other mobile privacy resources

Happtique App Certification Standards for medical, health and fitness apps, July 2012

iUbenda mobile app privacy policy generator

Lookout Mobile App Advertising Guidelines June 2012

MEF AppPrivacy mobile app privacy policy generator, September 2013

Network Advertising Initiative, Mobile application code, July 2013

PrivacyChoice Mobile Resources

TRUSTe Mobile Privacy Solutions

United States Federal Trade Commission, Marketing Your Mobile App: Get It Right from the Start, August 2012

United States Federal Trade Commission Staff Report, Mobile Apps for Kids: Current Privacy Disclosures are DisAPPointing, February 2012

United States National Telecommunications and Information Administration, Privacy Multistakeholder Process: Mobile Application Transparency, ongoing

Communicating privacy rules on small screens

Act4Apps Education Initiative

Act4Apps privacy dashboard

App Trust Project

Common terms

Know Privacy

Lifelock Smartphone App Privacy Icon Study

Mobile app voluntary transparency screens

Privacy Commons

Privacy Icons (alpha)

Making your privacy practices accessible to customers with disability

W3C Web Accessibility Initiative

Guide for developers (Apple)

Guide for developers (Android)

Selected mobile app privacy rating tools

Clueful

LBE Privacy Guard