Australian Government

Office of the Australian Information Commissioner

Mobile privacy

A better practice guide for mobile app developers

Consultation draft - April 2013

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

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

ISBN XXX-X-XXXXXX-XX-X

This publication should be attributed as: Office of the Australian Information Commissioner, *Mobile Privacy: A better practice guide for mobile app developers (2013)*.

Enquiries regarding the licence and any use of this report are welcome.

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

The Office of the Australian Information Commissioner 1

Introduction 2

The purpose of this guide 2

How does the Privacy Act apply to apps and app developers? 3

Make user privacy your competitive advantage 4

App privacy essentials 5

1. Your privacy responsibilities 5

2. Be open and transparent about your privacy practices. 6

3. Only collect personal information that your app needs to function 8

4. Secure what you collect 9

5. Obtain meaningful consent – the small screen challenge 9

6. Timing of user notice and consent is critical 10

Privacy and mobile apps: a checklist for app developers 11

Resources 13

The Office of the Australian Information Commissioner

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

The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner.

The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982* (Cth), and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the *Privacy Act 1988* (Cth) (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Introduction

The purpose of this guide

The OAIC has developed this guide to help mobile device application (app) developers embed better privacy practices in their products and services.

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 to 67 per cent in 2011
- 84 per cent of respondents said that they would own a smartphone in 2013
- 69 per cent of respondents said they had installed an app on their smartphone
- 38 per cent said that they owned a 'tablet' computer
- 93 per cent of tablet owners and 92 per cent of smartphone owners said that they used apps on their device.[1]

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 interfered with by an entity covered by the Act, including interferences by or in connection with an app. Alternatively, the 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 making changes to the way your app handles personal information, having to pay compensation to affected users, or (after 12 March 2014) a civil penalty.[2]

It is clear that the mobile environment, along with the new app economy it has generated, presents risks as well as potential. 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' approach, where privacy-enhancing practices are applied throughout the life cycle of the personal information – that is, its collection, use (including data matching and analytics), disclosure, storage and destruction.[3]

1 MM Mackay, *Australian Mobile Phone Lifestyle Index*, 8th edition, September 2012, www.digital-tsunami.com/2012/09/27/australian-mobile-device-usage-report/

2 See www.privacy.gov.au/complaints/outcomes and www.privacy.gov.au/materials/types/infosheets/view/6545; for information about civil penalties after 12 March 2014, see www.oaic.gov.au/privacy-portal/resources_privacy/Privacy_law_reform.html#whats_changed

3 www.privacybydesign.ca/index.php/about-pbd/

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.

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

What is 'personal information'?

The Privacy Act regulates the way in which 'personal information' is handled by most private sector businesses and Australian, ACT and Norfolk Island government agencies.[4]

'Personal information' is any information about an individual whose identity is apparent, or can reasonably be ascertained, from the information.[5] What constitutes personal information will vary, depending on what can reasonably be ascertained 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.

Mobile devices often contain large amounts of personal information, and have the potential to be linked to the identity of their users.

Application of the Privacy Act

The Privacy Act covers:

- any business that:
    - collects or discloses personal information for a benefit, service or advantage
    - handles health information[6], or
    - has an annual turnover of more than $3 million[7]
- credit providers and credit reporting agencies
- most Australian, ACT and Norfolk Island Government agencies (Government agencies).

[4] Privacy Act s (6)(1) re definition of 'agency', s 6C, 6D.
[5] Privacy Act s (6)(1).
[6] Privacy Act s 6C. See also the OAIC information sheet at www.privacy.gov.au/materials/types/infosheets/view/6558
[7] Privacy Act s6D(1).

Your app is likely to be covered by the Privacy Act if your business model relies on using personal information to sell advertising.

In most cases, businesses covered by the Privacy Act must comply with the National Privacy Principles (NPPs).[8]
Government agencies covered by the Privacy Act must comply with the Information Privacy Principles (IPPs).[9] If you are a business working for a Government agency as a contracted service provider, you will need to comply with the IPPs too.

The Privacy Act has been amended. From 12 March 2014, the NPPs and IPPs will be replaced by the Australian Privacy Principles (APPs) which will apply to both businesses and Government agencies.[10] If your business has to comply with the NPPs and/or IPPs, then it will need to comply with the APPs. The APPs contain new obligations – for example, about privacy policies, direct marketing and sharing information with overseas businesses. For more information about the APPs, see the OAIC's law reform page.[11]

If your business must comply with the NPPs and/or IPPs (or, in the future, the APPs), implementing better privacy practice can reduce your compliance costs.

Make user privacy your competitive advantage

Irrespective of whether 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:

- A 2012 survey by the Pew Research Center found that that 57 per cent of app users in the United States have either uninstalled an app over concerns about having to share their personal information or declined to install an app in the first place for similar reasons.[12]
- A 2012 UK study found that 27 per cent of consumers were more concerned about their privacy on smartphones than on their computer, and that 68 per cent of people choose not to download an app that they didn't trust.[13]
- A 2012 Australian study found that 56 per cent of Australians do not approve of having advertising targeted to them based on personal information. Further, 69 per cent of respondents reported they had refused to use an application or

8 Available at www.privacy.gov.au/materials/types/infosheets/view/6583
9 Available at www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=infosheets&fullsummary=6541&Itemid=1021
10 See Schedule 1, www.comlaw.gov.au/Details/C2012A00197
11 Available at www.oaic.gov.au/privacy-portal/resources_privacy/Privacy_law_reform.html
12 See http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf
13 TrustE, *Consumer Privacy Attitudes and Business Implications*, July 2012, available at www.truste.com/window.php?url=http://download.truste.com/TVarsTf=7EDO6P8Z-187

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.[14]

App privacy essentials

This section covers the essential information you need to know when designing, implementing and managing your app. A checklist to help you ensure your app is privacy friendly is available at Appendix A.

1. Your privacy responsibilities

Integrate good privacy protections into your day-to-day business practice. Implement a comprehensive privacy policy, and ensure that your business arrangements and contracts protect privacy and comply with your obligations under the Privacy Act.

The process of developing a privacy policy will help you to inspect your own practices in a systematic way. Putting in place privacy rules for your business will help you manage risks in a timely manner. 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, even if you only have a small team.
- When you are in the planning stages for an app, identify the data collection, use and flows, along with the privacy and security policies under which the data is being collected, used, accessed, stored and deleted.
- 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 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.

[14] 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

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
- analyses the possible privacy impacts on individuals' privacy
- identifies and recommends options for managing, minimising or eradicating these impacts
- analyses the project's effect on individual privacy
- helps find potential solutions and manage privacy impact through this analysis
- can make a significant difference to the project's privacy impact and still achieve or enhance the project's goals, and
- 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 PIA guide which you may find useful.[15] Additional resources and tools can be found in Appendix B.

2. Be open and transparent about your privacy practices.

Users increasingly expect transparency about how their personal information is handled; businesses which clearly explain this are rewarded with user trust and loyalty.[16] 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.

[15] Available at www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=guidelines&fullsummary=6590&Itemid=1021

[16] 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

For suggestions about how to implement these ideas, see *Communicating privacy rules on small screens* in Appendix B.

Your privacy policy

Make your app's privacy policy easy to find; users should not have to search for it. Wherever the app is being made available for download, clearly and accessibly tell potential users:

- whether they can opt in to (or opt out of) the collection or use of their personal information - if they can't, explain why
- what personal information your app will be collecting, and why
- where it will be stored (on the device or elsewhere)
- who it will be shared with and why
- how long the app will keep it
- whether the user can 'trade' access to their personal information with you for benefits such as convenience or free downloads, and
- any other issues that will affect user privacy.[17]

Protecting your users' privacy throughout the 'information life cycle'

- Have a monitoring process in place to make sure that the app handles personal information as described in your privacy policy.
- 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 transfers of information to third parties, make the changes easy to find and understand through the update process.
- *Never* make silent app updates that will diminish the user's privacy.
- Provide specific, targeted notifications to users when they need to make a decision about whether to consent to the collection of their personal information. These notifications should contain the same sorts of information listed in your privacy policy (see above) so that users can make an informed decision.

[17] The Privacy Act requires that you notify individuals of certain matters when you collect their personal information See NPP 1.3 at www.privacy.gov.au/materials/types/infosheets/view/6583#npp1 and IPP 2 at www.privacy.gov.au/materials/types/infosheets/view/6541#a

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

The Privacy Act requires that you only collect the personal information that is necessary.[18] Consider whether you need to collect personal information at all.

- 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 data just because you believe it may be useful in the future.
- Delete personal information that you no longer need for a lawful purpose.[19]
- 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 (such as a person's ethnicity, political opinions, sexual preferences or health information) at all, unless the person has expressly consented.[20]
- 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 modify or delete the data used by 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.
- Never 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 device-unique identifiers if it is not essential to the functioning of the app.
- Avoid associating data across apps 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.

[18] See IPP 1 at www.privacy.gov.au/materials/types/download/8685/6524 and NPP 1 at www.privacy.gov.au/materials/types/guidelines/view/6582

[19] For exceptions to this, see NPP 2.1 at www.privacy.gov.au/materials/types/guidelines/view/6582

[20] See the definition of 'sensitive information' in the Privacy Act s6(1): www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249829

- If you have to keep a copy of the information, secure it and delete it as soon as possible.

4. Secure what you collect

- 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. Users' information should be encrypted when it is stored and when it is transmitted over the internet.
- Adapt your code to allow for differences in mobile platforms.
- Generate credentials securely.
- Use due diligence on libraries and other third-party code.
- Don't store passwords in plain text on your server.
- Give users a clear and easy way to refuse an update, and to deactivate and delete the app. When users delete an app, the data that you hold about them should also be deleted.
- Give users the ability to delete or request the deletion of all of the data that your app has collected about them.
- Be transparent (for example, in your privacy policy) about how long it will take to delete personal information once a user deletes your app.

5. Obtain meaningful consent – the small screen challenge

No one wants to read a 20-page privacy policy on a small screen. Consider the right information strategy to reach app users without causing 'notice fatigue' where people ignore notices or warnings that they see too often. You might be able to adapt existing mobile privacy policy template language and generators (see *Resources* in Appendix B) but make sure the result meets any obligations you have in Australia under the Privacy Act.

Here are some options for visual cues that may be helpful.

- **Use short form notices**
  - 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.
  - 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. Approach this display in a way that encourages user action, such as with the use of radio buttons rather than web links.

  - Instead of just using an on/off button, explain the consequences of making a choice to provide data so they can make an informed decision.

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 following techniques:

- **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**
  - 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 of this document.

6. 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. 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, clearly state whether your app will tag the images with location data and allow the user to opt out of this feature at the time of taking the photo or video.
- Depending on the purpose of your app, you can give users control over repeated prompting to avoid notice fatigue, but the user should ideally be able to set a period of time after which the consent should be renewed.

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.
- ☑ 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.
- ☑ Map out where the information is going and identify potential privacy risks.
- ☑ Use a Privacy Impact Assessment[21] to assist with privacy planning.

☑ Be open and transparent about your privacy practices

- ☑ Develop a privacy policy that informs users clearly and simply what your app is doing with their personal information.
- ☑ Post the privacy policy where users can easily find it, and where it is readily accessible to potential users who are considering downloading your app.
- ☑ 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 give them an easy way of refusing the update.

☑ 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 data collection outside of what they would reasonably expect is necessary for the functioning of the app.

☑ Secure what you collect.

- ☑ Put in place appropriate safeguards to protect the personal information you are handling. Use encryption when storing and transmitting data.

[21] See www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html.

- ☑ 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 deletes your app.

☑ 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, when they first use the app, and throughout their app experience, to ensure that their consent remains meaningful and relevant.
- ☑ Be thoughtful and creative when deciding when to deliver privacy messages to most effectively capture users' attention and achieve the most impact at the right time, without causing notice fatigue. For example, if your app is about to actively tag photos with the user's location data, you could activate a symbol as a cue to the user, providing them with a choice to refuse.

[Find out more about privacy and apps, including resources for using icons to represent privacy information, in the OAIC's *Mobile privacy: a better practice guide for mobile app developers* [Link]]

Appendix B - Resources

Being privacy-aware

OAIC resources

10 steps to protect other people's personal information

Taking reasonable steps to make individuals aware that personal information about them is being collected

Other Information sheets explaining the National Privacy Principles in depth

Privacy Impact Assessment Guide

Privacy quiz for organisations

A guide to handling personal information security breaches

International regulatory resources

Mobile App Developers: Start with Security

Mobile Privacy Disclosures: Building Trust Through Transparency

Securing Personal Information: A Self-Assessment Tool for Organizations

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.'

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.'

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.

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.

Association for Data-driven Marketing and Advertising (Australian)

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

Australian Web Industry Association

'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.'

Selected privacy-related guidance for app developers

The Association for Competitive Technology, Act4Apps Education Initiative (news release), January 2013

Berkeley Center for Law & Technology, Mobile Phones and Privacy, July 10, 2012

Calo, M. Ryan. Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame Law Review 1027 (2012)

California Auditor General and mobile application platforms' joint statement on privacy, February 2012

California Department of Justice, Privacy on the Go: recommendations for the mobile ecosystem, January 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 Draft App Certification Program, July 2012

Lookout Mobile App Advertising Guidelines June 2012

National Telecommunications and Information Administration, Mobile app voluntary transparency screens (draft), January 2013

OASIS Privacy Reference Management Model Version 1.0 Committee Specification Draft, March 26 2012

Offices of the Information and Privacy Commissioners of British Columbia and Alberta, and the Office of the Privacy Commissioner of Canada, Securing Personal Information: A Self-Assessment Tool for Organisations

Pew Research Centre, Privacy and Data Management on Mobile Devices, September 2012

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, August 2012

Communicating privacy rules on small screens

Act4Apps Education Initiative

App Trust Project

Common terms

Know Privacy

Mobile app voluntary transparency screens

Privacy Commons

Privacy Icons (beta)

Privacy Icons (alpha)

Selected mobile app privacy rating tools

Clueful

LBE Privacy Guard

Lookout Premium

MobileScope