Australian Government

Office of the Australian Information Commissioner

# App purchases by Australian consumers on mobile and handheld devices

## Submission to the Commonwealth Consumer Affairs Advisory Council

**March 2013**

**Timothy Pilgrim**
**Australian Privacy Commissioner**

# Contents

# Introduction

The Office of the Australian Information Commissioner (the OAIC) welcomes the opportunity to respond to the Issues Paper *App purchases by Australian consumers on mobile and handheld devices*.[1]

Our submission aims to broadly outline to the Commonwealth Consumer Affairs Advisory Council and the Treasury, the regulatory environment in which applications (apps) and app businesses operate, and some issues that can arise in the design, implementation and use of mobile apps.

# About the OAIC

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.

[1] http://issues.ccaac.gov.au/2012/12/12/app-purchases-by-australian-consumers-on-mobile-and-handheld-devices/

# The Privacy Act

## Personal information

The Privacy Act regulates the way in which 'personal information' is handled by most Australian Government agencies and some private sector businesses. 'Personal information' is any information about an individual whose identity is apparent, or can reasonably be ascertained, from the information.[2] 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
- contact lists, which reveal details about a user's social connections and the contacts themselves
- voice print and facial recognition biometrics, because they identify and collect unique characteristics of an individual's voice or face
- location information, because it can reveal user activity patterns and habits and, as a consequence, identity.

Mobile devices often generate and store large amounts of information which can potentially be linked to the identity of their users. In this context, most mobile devices would be holding personal information.

## Application of the Privacy Act

### *The National Privacy Principles*

The National Privacy Principles (the NPPs, set out in Schedule 3 to the Privacy Act) regulate the way that private sector organisations (organisations) handle personal information. The NPPs impose the collection, storage, security, use, disclosure and access and correction obligations of organisations covered by the Privacy Act. In general, the NPPs apply to all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers, and a limited range of small businesses.[3]

Those small businesses covered by the Privacy Act include those which collect or disclose personal information for a benefit, service or advantage. This distinction is relevant in the case of app businesses, as many may have an annual turnover of $3 million or less (which would otherwise mean they would be exempt under the small business exemption in the Privacy Act).

---

2 See *Privacy Act 1988* (Cth), s 6(1) at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249829

3 Available at www.privacy.gov.au/materials/types/infosheets/view/6583

In this context, the business model for each app business would need to be considered to determine if it is regulated by the Privacy Act.[4] For example, where an app business's mobile device apps collect, use or disclose personal information for the purposes of gaining advertising revenue, that business may be covered by the Privacy Act.

***Extra-territorial application of the Privacy Act***

Section 5B of the Privacy Act relevantly provides that the Act may apply to the acts and practices of organisations that occur outside Australia or its external territories. In particular, s 5B(3) provides that where an organisation:

- 'carries on business in Australia or an external Territory'
- collects personal information in Australia or an external Territory (ie from an individual or individuals physically located in Australia),[5] either before or at the time of the act or practice, or
- holds personal information in Australia or an external Territory, either before or at the time of the act or practice

the Privacy Act will apply to the act or practice.

Any organisation that runs an app which involves the collection, use and disclosure of personal information of Australian residents or citizens and that has an organisational link with Australia may be covered by the Privacy Act.[6]

As such, even where a business develops an app outside of Australia, and administers and/or hosts the app outside of Australia, that business may still be covered by the Privacy Act.

The question of the extra-terrestrial application of the Privacy Act has been further clarified as part of the Privacy Act reforms.

***Privacy enforcement***

If an organisation is covered by the Privacy Act, and its app breaches the Privacy Act, the OAIC can act against the organisation, either in response to a complaint from an individual or as part of an investigation initiated by the Commissioner of his or her own volition; these are referred to as Own Motion Investigations (OMIs).[7]

Conciliation is attempted to resolve all investigations. Possible resolutions include:

- an apology

[4] See Privacy Act s 6D(4)(c) and s 6D(4)(d) at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249834

[5] See the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 at www.comlaw.gov.au/Details/C2012B00077/Explanatory%20Memorandum/Text

[6] See Privacy Act s 5B at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249828

[7] See Privacy Act Part V Division 1 at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249927

- a change to the respondent's practices or procedures
- staff counselling
- taking steps to address the matter, for example providing access to personal information, or amending records
- compensation for financial or non-financial loss
- other non-financial options, for example a complimentary subscription to a service.[8]

In the case of a complaint brought by an individual, the Commissioner can make a determination where conciliation does not resolve the matter. Determinations can be enforced, if necessary, in the Federal Court or Federal Magistrates Court.[9]

In the case of OMIs, the OAIC publishes reports of these investigations where there is a public interest in doing so. While currently there are no remedy powers available to the Commissioner in relation to OMIs, additional powers will be available upon the commencement of the privacy reforms in March 2014 (see *Privacy reform*).

Jurisdictional complexities can limit the effectiveness of regulatory oversight. Many apps used by Australians are administered by businesses located outside Australia and/or hosted on foreign servers. In such circumstances, it can be difficult for Australian regulators to determine and enforce their jurisdiction. However, the OAIC is working with its international counterparts through organisations such as the OECD and APEC to establish cross-border enforcement processes.

***Privacy reform***

*The Australian Privacy Principles*

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Reform Act) received royal assent on 12 December 2012.[10] The Reform Act will make substantial changes to the Privacy Act, the majority of which will come into force on 12 March 2014. Among other changes, the NPPs (and their public sector equivalent, the Information Privacy Principles)[11] will be replaced by a single set of harmonised privacy principles, the Australian Privacy Principles (APPs).[12]

Organisations currently regulated by the NPPs will be covered by the APPs. The OAIC is developing guidance on the application and operation of the APPs.



8 See www.privacy.gov.au/complaints/outcomes

9 See Privacy Act s 55A at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249956

10 See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* at www.comlaw.gov.au/Details/C2012A00197

11 See Privacy Act, s 14 at www.comlaw.gov.au/Details/C2012C00903/Html/Text#_Toc343249862

12 See *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, Schedule 1 at www.comlaw.gov.au/Details/C2012A00197

*Privacy codes*

Organisations covered by the NPPs (or a body or association representing them) can develop written codes of practice for the handling of personal information. These codes set out how one or more of the NPPs are to be applied or complied with, and the NPP organisations that are bound by the code.

Part IIIB of the reformed Privacy Act, which replaces the current Part IIIAA, changes the process for the development of privacy codes, which will become known as APP codes.[13] Part IIIB allows for the Commissioner to approve and register enforceable codes which are developed by agencies and organisations ('entities'), on their own initiative or on request from the Commissioner, or by the Commissioner directly.

The OAIC is currently consulting on guidelines for developing codes.[14] It may be that the mobile app industry chooses to develop a privacy code or codes, or that the Commissioner requests this of the industry.

*Privacy reform – enforcement implications*

From 12 March 2014, the Commissioner will have enhanced enforcement powers, including the ability to:

- make a determination in the case of OMIs
- accept enforceable undertakings
- seek civil penalties in the case of serious or repeated breaches of privacy
- conduct assessments of privacy performance for businesses and Australian Government agencies.

# Measures to protect privacy

To be privacy-enhancing, apps and apps businesses should:

- only collect the personal information that they need to function (NPP 1)
- keep any personal information that they collect secure (NPP 4)
- obtain meaningful consent from users, which requires that consumers – that is, users and potential users – are adequately informed of privacy practices (NPP 2, NPP 5 and NPP 10) (see *Notices and consent*).[15]

The OAIC is currently drafting better practice privacy guidance for developers of mobile apps. The guidance will educate app developers about best privacy practice and the

[13] See *Privacy Amendment (Enhancing Privacy Protection) Act 2012* at www.comlaw.gov.au/Details/C2012A00197

[14] See www.oaic.gov.au/news/consultations.html#current_consultations

[15] See the National Privacy Principles at www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-factsheet2_NPPs_online.pdf and the *Guidelines to the National Privacy Principles* at www.privacy.gov.au/materials/types/guidelines/view/6582

commercial benefits of being privacy-friendly.[16] The document will recommend that developers adopt a 'privacy by design'[17] approach, under which:

- developers carry out a Privacy Impact Assessment (PIA) to help ensure they have identified and addressed all the relevant privacy issues
- privacy-enhancing practices are incorporated through the design, implementation and management stages of the app
- 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.

The guidance will recognise that app developers face a number of challenges in communicating their privacy policies with consumers:

- The small screens of many mobile devices make it difficult to read large amounts of text, such as a detailed privacy policy.
- 'Privacy fatigue' – while a majority of users are concerned about app privacy,[18] users are presented with many privacy policies, and these policies are often lengthy and difficult to read. As such, few users read privacy policies in depth.[19]



[16] For example, a 2012 survey found that that 57% of app users in the US 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 (http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf); a 2012 UK study found that 27% of consumers were more concerned about their privacy on smartphones than on their computer, and that 68% choose not to download an app that they didn't trust (www.truste.com/window.php?url=http://download.truste.com/TVarsTf=7EDO6P8Z-187); and a 2012 study found that 56% of Australian respondents do not approve of having advertising targeted to them based on personal information, 69% had refused to use an application or website because it collected too much personal information and 75% said they needed to know more about the ways in which companies collected personal information (http://cccs.uq.edu.au/personal-information-project).

[17] www.privacybydesign.ca/index.php/about-pbd/

[18] For example, 57% of app users 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 (http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf); 27% of consumers are more concerned about their privacy on smartphones than on their computer, and 68% choose not to download an app that they don't trust (www.truste.com/window.php?url=http://download.truste.com/TVarsTf=7EDO6P8Z-187); 69% of consumers reported they had refused to use an application or web site because it collected too much personal information, and 75% said they needed to know more about the ways in which companies collected personal information (http://cccs.uq.edu.au/personal-information-project)

[19] For example, a 2001 US study found that only 3% of respondents carefully read website privacy policies 'most of the time', with the remainder of respondents split evenly between the following answers: 'I have spent little or no time looking at websites' privacy policies', 'I have glanced through websites' privacy policies, but I have rarely read them in depth' and 'It has depended on the circumstances. Sometimes, I have reviewed websites' privacy policies carefully. Other times, I have reviewed the privacy policies little, if at all.' (Privacy Leadership Initiative, Privacy Notices Research Final Results, conducted by Harris Interactive, Inc. December 2001).

# Key privacy issues

## Notices and consent

The large and growing numbers of Australians who use mobile device apps place a high level of trust in those apps, and their expectations of privacy when using these apps are equally high. Apps which fail to protect users' privacy may find themselves the subject of negative attention. Media reports of apps gaining unauthorised access to user information – including address books, photos and location data – lead to a loss of public confidence in the product.

The OAIC has an interest in ensuring that:

- app privacy practices conform to the NPPs and meet the privacy standards expected by the Australian community
- app users are adequately informed of potential privacy implications when they download and use an app, with:
    - the app's privacy policy presented in an accessible and simple way, and
    - privacy policies fully and accurately reflecting the app's privacy practices.[20]

In particular, the OAIC is aware that many app privacy notices may not conform to the requirements of NPP 1.3, which requires organisations that collect personal information about an individual to take reasonable steps to ensure that the individual is aware of:

- the identity of the organisation and how to contact it
- the fact that he or she is able to gain access to the information
- the purposes for which the information is collected
- the organisations (or the types of organisations) to which the organisation usually discloses information of that kind
- any law that requires the particular information to be collected
- the main consequences (if any) for the individual if all or part of the information is not provided.

In order to effectively inform users, app privacy policies should be:

- honest, accurate and specific
- easy to understand
- prominently positioned
- accessible for consumers with disability
- updated when necessary.

[20] See business openness obligations at www.privacy.gov.au/materials/types/infosheets/view/6583#npp5

The OAIC's forthcoming guidance for mobile app developers will contain more detailed information on these issues, including links to suggested symbols to easily convey privacy information.

### Consumer awareness

One strategy to address consumer concerns is promoting consumer education on apps, such as the advice provided by the Department of Broadband, Communications and the Digital Economy[21] and the Australian Communications Consumer Action Network.[22] We also understand that similar guidance is being developed by the Information and Privacy Commission of NSW.

One way that the OAIC invests in consumer awareness is through its participation in Privacy Awareness Week (PAW), which is held each year by the Asia Pacific Privacy Authorities Forum, of which the OAIC is a member, to promote greater privacy awareness and the importance of protecting personal information.[23]

The theme for PAW 2013, held from 28 April to 4 May, is privacy law reform. The OAIC expects to launch a number of useful resources for consumers, as it has done in previous PAWs.

For example, in PAW 2012, the OAIC launched a fact sheet with tips on how consumers can protect their personal information.[24] Many of these tips are adaptable for consumers of mobile apps, who can take steps such as:

- reading privacy notices before installing new apps
- deleting apps which do not provide enough privacy information, or which appear to be privacy-invasive
- using passwords where possible (different passwords for different apps)
- not allowing apps to use or store the consumer's contacts without permission from those contacts.

It is important to note, however, that many of these actions are currently difficult for consumers; the app industry needs to make sure that its practices are not only privacy-enhancing – and compliant with the Privacy Act – but also that they are comprehensible to consumers.

## Mobile app privacy internationally

The OAIC continues to work with its counterparts in Australian and international jurisdictions. It is useful to note that government and industry can work together – as has

[21] For example, www.staysmartonline.gov.au/home_users/protect_yourself2/protect_your_identity

[22] For example, http://accan.org.au/index.php?option=com_content&view=article&id=468:national-childrens-and-youth-law-centre-ncylc&catid=124:current-grants&Itemid=203

[23] See www.privacyawarenessweek.org/

[24] See www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet8_10steps_protect_your_information.html

occurred in the United States, particularly in California – to improve privacy outcomes for consumers and limit compliance risks for industry.

Below is a brief summary of relevant international developments.

## United States

A discussion draft of the Application Privacy, Protection, and Security Act of 2013, which would regulate how apps collect personal information, has recently been released.[25] The Act, if passed, would be the first US Federal Act to specifically target mobile app privacy.

The Federal Trade Commission has released an advisory document for app developers,[26] a report on mobile privacy disclosures[27] and a report specifically on privacy disclosure in apps for children.[28] A number of other US organisations – government, non-government and industry – are working on guidance documents and symbols for use by app developers. Links to these will be included in the OAIC guidance for app developers.

### *California*

The *California Online Privacy Protection Act (Business and Professions Code section 22575)* is potentially a very valuable means of improving apps' posted privacy policies. It requires 'an operator of a[n] online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its … online service' to 'conspicuously post its privacy policy.'[29] A number of high-profile app platform providers (including Apple, Google and Microsoft) have agreed to begin asking app developers who collect personal information to include privacy policies. It may also be the case that app developers, in the process of ensuring that their products are compliant in California (and wishing to avoid fines of up to US$2,500 every time a non-compliant app is downloaded)[30] develop apps that comply with California law, but are released for global consumption.

The California Department of Justice has also released a guidance document which includes recommendations for app developers, app platform providers and advertising networks.[31]



---

25 See http://apprights-hankjohnson.house.gov/2013/01/apps-act.shtml

26 Federal Trade Commission 2012, *Marketing your mobile app: get it right from the start*, http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

27 Federal Trade Commission 2013, *Mobile privacy disclosures: building trust through transparency*, www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

28 Federal Trade Commission 2012, *Staff Report*, *Mobile apps for kids: current privacy disclosures are disappointing*, www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

29 www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

30 State of California Department of Justice Office of the Attorney General 2012, *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law* (media release), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance

31 California Department of Justice 2013, *Privacy on the Go,* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

## Canada

Several of Canada's privacy regulators have published a joint guidance document aimed at app developers. It makes recommendations on how to ensure best privacy practice, and reminds app developers of their obligations under Canada's *Personal Information Protection and Electronic Documents Act* and similar provincial laws, which set 'ground rules for how organizations may collect, use or disclose information about individuals in the course of commercial activities [and] gives individuals the right to see and ask for corrections to information an organization may have collected about them.'[32]

## Europe

The *European Data Protection Directive* (Directive) regulates the processing of personal data within the European Union (but does not specifically mention online privacy issues).[33] A draft European General Data Protection Regulation to supersede the Directive is currently being considered. The Regulation would comprise 'one, single, technologically neutral and future-proof set of rules across the EU [so that] regardless of how technology and the digital environment develop in the future, the personal information of individuals in the EU will be secure, and their fundamental right to data protection respected … These proposals will help build trust in the online environment ... [to] enable consumers to engage with innovative technologies and purchase online in full confidence that their data will be protected.'[34]

Further, the European Parliament's Article 29 Data Protection Working Party, which provides advice on the processing and movement of personal data, has recently published an opinion on mobile apps, aimed at app developers and other parties in the app ecosystem. The opinion clarifies the European legal framework regarding 'the processing of personal data in the development, distribution and usage of apps on smart devices, with a focus on the consent requirement, the principles of purpose limitation and data minimisation, the need to take adequate security measures, the obligation to correctly inform end users, their rights, reasonable retention periods and specifically, fair processing of data collected from and about children'.[35]



[32] Privacy Commissioners of Canada, Alberta and British Columbia 2012, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, www.priv.gc.ca/information/pub/gd_app_201210_e.asp#toc3

[33] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[34] European Commission, *How will the EU's reform adapt data protection rules to new technological developments?* Date unknown, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf

[35] Article 29 Data Protection Working Party 2013, *Opinion on apps on smart devices*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf