Mobile privacy: a better practice guide for mobile app developers

Submission by the Australian Communications Consumer Action Network to the Office of the Australian Information Commissioner

10 May 2013

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government on behalf of consumers to ensure availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact

Steven Robertson,
Policy officer

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: steven.robertson@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Contents

1. Executive Summary

ACCAN appreciates the opportunity to comment on the OAIC's draft privacy guidelines for app developers. By assisting app developers in meeting their requirements under privacy law and privacy best practice, the OAIC guidelines provide valuable flow-on benefits to consumers, in an industry which is gaining notoriety for undermining consumers' rights.

Our submission makes a number of recommendations, both specific and thematic, which would enhance the consumer benefit of these guidelines:

Recommendation 1: the OAIC guidelines should advise developers against making use of third-party data processes, storage, etc.

Recommendation 2: the OAIC guidelines should discourage opt-out third-party analytics.

Recommendation 3: where third-party analytics are used on an opt-out basis, the OAIC guidelines should encourage developers to make the opt-out process as simple as possible.

Recommendation 4: the OAIC guidelines should provide advice on protecting users' privacy when making use of advertising systems.

Recommendation 5: the OAIC guidelines should include stronger encouragement for app developers to carry out, publish, and seek public consultation on privacy impact assessments.

Recommendation 6: the OAIC guidelines should actively discourage developers from offering in-app benefits in exchange for personal information.

Recommendation 7: the OAIC guidelines should include a recommendation that privacy policies inform users of how any personal information will be stored.

Recommendation 8: the OAIC guidelines should include a recommendation that users be prompted to accept or reject any privacy-impacting changes to an app or its privacy policy.

Recommendation 9: the OAIC guidelines should provide specific guidance on the collection, use and disclosure of location data by app developers.

Recommendation 10: the OAIC guidelines should recommend that developers provide a clear and easy way for a user to revoke permission to access their personal information.

Recommendation 11: the OAIC guidelines should contain specific recommendations on the use of third-party services such as cloud storage services, including recommendations around transparency and limitation of access.

Recommendation 12: the OAIC guidelines should encourage developers to be open and transparent about the range of information they can, or do, access from users' social media profiles.

Recommendation 13: the OAIC guidelines should strongly encourage developers to make their apps functional without access to a user's social media accounts where possible.

Recommendation 14: the OAIC guidelines should caution developers against circumventing users' settings through other apps or similar methods.

Recommendation 15: the OAIC guidelines should include an explanation, in general terms, of the need to secure personal information.

Recommendation 16: the OAIC guidelines should set out the key responsibilities of the individual within an organisation who is responsible for security.

Recommendation 17: the OAIC guidelines should elaborate on the requirements of "due diligence" of third-party code.

Recommendation 18: the OAIC guidelines give some indication of what an acceptable delay in deleting a user's information might be.

Recommendation 19: in the context of deleting user information, the OAIC guidelines should distinguish between information that is held on the mobile device or on a remote system.

Recommendation 20: in the context of deleting user information, the OAIC guidelines should distinguish between information that is used by a single app and information that may be used by multiple apps.

Recommendation 21: the OAIC guidelines should not require that a user's information be deleted when an app is deleted in cases where this may result in detriment to the end user, including:

— when user information is stored in a collection that is used by multiple apps (such as photo albums, contact databases and messages); and
— when user information is stored on a remote system and may remain useful to the user despite the app being deleted (such as account details and online purchase histories).

Recommendation 22: the OAIC guidelines should draw attention to the special considerations that may arise when considering the privacy of children and young people.

Recommendation 23: the OAIC guidelines should encourage developers to consider the particular requirements that users may have when attempting to obtain consent to the collection of personal information.

Recommendation 24: the OAIC guidelines should be amended to note the importance of maintaining accessibility when presenting simplified descriptions of privacy policies.

Recommendation 25: the OAIC guidelines should recommend including a simplified text-based description of the privacy policy in addition to any visual or auditory devices.

Recommendation 26: the OAIC guidelines should be amended to advise developers to make privacy information available to consumers before any purchase or download begins.

Recommendation 27: the OAIC guidelines should set out suitable constraints on any "creative" presentations of privacy policies to ensure that privacy information remains clear and accessible to users.

Recommendation 28: greater detail should be provided about the resources contained in the appendix.

2. Responses to the OAIC's draft guidelines

2.1. App privacy essentials

2.1.1. Your privacy responsibilities

Transfer to third parties

This section suggests that developers "[h]ave controls in place … 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."

While this is certainly a useful suggestion to developers, we believe the guidelines should recommend against disclosing personal information to third parties in the first place. While it may often be impractical for a developer to process data entirely in-house, it is important that the guidelines treat third-party disclosure for the purposes of data processing as something that should only be done when necessary, rather than a standard channel of information flow in mobile apps.

> Recommendation 1: the OAIC guidelines should advise developers against making use of third-party data processes, storage, etc.

A more insidious disclosure of users' personal information to third parties is the automatic disclosure for the purposes of tracking usage and performing analytics on an app's user base. Some apps automatically disclose information to third parties for such purposes, with little prior warning given to the end user. For example, the privacy policy of Rovio[1] notes that:

> Rovio may use Flurry analytics tool in order to develop and analyze use of the Services. If you wish to opt-out from Flurry analytics, please follow this link: http://www.flurry.com/resources/privacy.html.

In order to opt out from Flurry analytics, users of Rovio apps must visit the Flurry website[2] and provide their mobile device's identifier to Flurry. Such an arrangement is unacceptable: in order to opt out from these analytics the user is required to disclose further information to the third party. If third-party analytics are to be used, they should ideally be used in an opt-in basis; where they are used on an opt-out basis the opt-out process should be made as simple as possible.

> Recommendation 2: the OAIC guidelines should discourage opt-out third-party analytics.

[1] <http://www.rovio.com/Privacy>

[2] <http://www.flurry.com/user-opt-out.html>

> Recommendation 3: where third-party analytics are used on an opt-out basis, the OAIC guidelines should encourage developers to make the opt-out process as simple as possible.

There appears to be little recognition in the Guidelines of the role of third-party advertising in mobile platforms. Since the use of mobile advertising systems raises the possibility of targeted marketing, data mining, user profiling and so forth, it may be useful to provide guidance to developers on managing the privacy risk of using third party advertising in their apps.

> Recommendation 4: the OAIC guidelines should provide advice on protecting users' privacy when making use of advertising systems.

Privacy impact assessments (PIAs)

The guidelines note that a developer "may choose to publish [their] PIA" and that developers "might even wish to encourage privacy organisations or members of the public to consult on [their] draft PIA". We suggest that this language should be strengthened; rather than publication of and consultation on PIAs being something that developers might consider, it should be actively encouraged as best practice. Privacy policies and FAQs that accompany apps rarely give a clear description of how personal information will be collected, used and disclosed, and a PIA presents an opportunity for developers to set such information out in greater detail.

> Recommendation 5: the OAIC guidelines should include stronger encouragement for app developers to carry out, publish, and seek public consultation on privacy impact assessments.

2.1.2. Be open and transparent about your privacy practices

Bartering for personal information

The guidelines advise developers to be open and transparent about their privacy practices "even if [they] choose to offer benefits—such as convenience or free downloads—to [their] customers in exchange for access to their personal information." ACCAN is concerned that the guidelines do not take a stronger stance against this practice.

The practice of bartering for personal information in this way raises particular concerns if the functionality of the app is restricted until the user provides their personal information. ACCAN has previously argued against apps that offer restricted functionality until the user purchases in-game credits or features,[3] and we similarly believe that limiting the functionality of an app until the user provides personal information is a practice that should be discouraged.

[3] ACCAN, *App purchases by Australian consumers*, submission to the Commonwealth Consumer Affairs Advisory Council, February 2013, <http://accan.org.au/files/App_purchases_by_Australian_consumers.pdf>.

While it is ultimately the choice of an individual consumer to trade their personal information for in-app benefits, this practice cannot be considered best privacy practice, and should be actively discouraged by the OAIC.

> Recommendation 6: the OAIC guidelines should actively discourage developers from offering in-app benefits in exchange for personal information.

Storage of personal information

In addition to recommending that privacy policies tell users what information will be stored, where it will be stored, for how long it will be stored and with whom it will be shared, consideration should also be given to recommending that privacy policies tell users how the information will be stored. In particular, users should be informed whether their information will be stored in plain text rather than in an encrypted form or other secure form.

> Recommendation 7: the OAIC guidelines should include a recommendation that privacy policies inform users of how any personal information will be stored.

Opting out of changes

If a privacy policy is changed, users should have a chance not only to provide feedback (which will in most cases fall on deaf ears) but also to (i) stop using the app, and (ii) have their information deleted from any systems operated by the app developers/third parties. The fact that a user agreed to one version of the policy should not be taken to mean that they have consented to a modified version of the policy.

> Recommendation 8: the OAIC guidelines should include a recommendation that users be prompted to accept or reject any privacy-impacting changes to an app or its privacy policy.

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

Location information

Consideration should be given to including guidance on the collection of location information, since mobile devices provide a straightforward means of gathering users' locations. As the OAIC is no doubt aware, location information can potentially reveal personal or sensitive information about individuals, and it may therefore warrant specific guidance in this section.

> Recommendation 9: the OAIC guidelines should provide specific guidance on the collection, use and disclosure of location data by app developers.

Revocation of permission

While the guidelines note the importance of an app obtaining a user's permission before accessing personal information, consideration should also be given to the importance of a user being able to revoke that permission at any time. Developers should at a minimum provide a clear and straightforward way for users to revoke permission for specific types of information, including, for example, location information, access to a user's photos, and address book/contact information.

> Recommendation 10: the OAIC guidelines should recommend that developers provide a clear and easy way for a user to revoke permission to access their personal information.

Collection of personal information from other apps and social media services

It is useful that the guidelines recommend that developers "[a]void associating data across apps unless it is obvious to the use and necessary to do so." We suggest, however, that more could be said on this point. For example, a number of apps (such as Dropbox[4] and Google Drive[5]) provide frontends to cloud storage services, and these apps and services can often be accessed from third party apps.[6] This requires the user to put a great deal of trust in the third-party developer not to access any information stored in the cloud service beyond what the user expects will be accessed. The guidelines should be expanded here to require greater transparency and limiting access when using such services.

> Recommendation 11: the OAIC guidelines should contain specific recommendations on the use of third-party services such as cloud storage services, including recommendations around transparency and limitation of access.

Other apps make use of social media services for the purposes of, for example, comparing a user's game scores against their Facebook friends' scores, or playing directly against friends.[7] While this is a function that some users may appreciate, it also represents a privacy and security risk, since these apps gain full access to the information in a user's social media account. It is important that users are (i) aware of the extent of access that such an app may have to their social media accounts, and (ii) free to use an app without granting it access to their social media accounts, so long as such access is not required for the app to function.

---

[4] <https://www.dropbox.com/>

[5] <https://drive.google.com/>

[6] For example, the Goodreader app from Good.iWare allows the user to nominate either of these services for storage; see <http://www.goodiware.com/goodreader.html>.

[7] For some examples of apps that can request access to Facebook accounts, see Collapse! Blast <https://play.google.com/store/apps/details?id=com.realarcade.CLB&feature=search_result> and Zynga Poker <https://play.google.com/store/apps/details?id=com.zynga.livepoker&feature=search_result>.

> Recommendation 12: the OAIC guidelines should encourage developers to be open and transparent about the range of information they can, or do, access from users' social media profiles.
>
> Recommendation 13: the OAIC guidelines should strongly encourage developers to make their apps functional without access to a user's social media accounts where possible.

The guidelines could also be expanded to recommend against using third-party apps to bypass the user's privacy and security settings. If a user restricts access to location data to a weather app, for instance, other apps should not indirectly obtain location data from the weather app.[8] Such behaviour directly contradicts a user's consent and expectations.

> Recommendation 14: the OAIC guidelines should caution developers against circumventing users' settings through other apps or similar methods.

2.1.4. Secure what you collect

Context

As this section stands, there is little context for the security guidance given. Providing some broad exposition of the legislative requirements for, and best practices in, securing personal information (e.g. under NPP 2 and APP 11) would assist developers in understanding their obligations and assist end users in understanding their rights.

> Recommendation 15: the OAIC guidelines should include an explanation, in general terms, of the need to secure personal information.

Organisational responsibility

It may be unclear to a reader of these guidelines what being "responsible for security" involves. Some elaboration on the role and responsibilities of such a person would be useful.

> Recommendation 16: the OAIC guidelines should set out the key responsibilities of the individual within an organisation who is responsible for security.

Password storage

It would be useful to provide guidance on how passwords should be stored, rather than simply stating that they should not be stored in plaintext. While it may not be appropriate to specify a

[8] Chan C, *Penn State study: Cellphone apps pose hidden threats*, 2 April 2013, <http://current.it.psu.edu/article/penn-state-study-cellphone-apps-pose-hidden-threats>.

particular method of password storage in these guidelines, it would be useful to provide developers with some indication of what best practice password storage requires. Note, for instance, that during the ABC's recent security breach,[9] many users' passwords were able to be determined—despite the passwords not being stored in plaintext—because inadequate password security was in place.[10]

Due diligence on third party code

It would be useful to elaborate on what "due diligence" on libraries and third-party source code might require—for example, only using code from trusted third parties, or auditing any third party code to ensure that it meets the standards set out in these guidelines. "Due diligence", by itself, is a relatively imprecise term, and further detail should be provided to ensure that end users are protected.

> Recommendation 17: the OAIC guidelines should elaborate on the requirements of "due diligence" of third-party code.

Time to deletion and deletion triggers

Rather than simply recommending that developers are transparent about the time taken to delete users' personal information, these guidelines could usefully suggest a reasonable timeframe for deletion.

> Recommendation 18: the OAIC guidelines give some indication of what an acceptable delay in deleting a user's information might be.

The guidelines recommend that "[w]hen users delete an app the data that you hold about them should also be deleted". ACCAN suggests that this recommendation requires clarification. A mobile app user's information can be stored in (at least) two places—on the user's mobile device, and on the developer's systems (or "in the cloud"). In each case, deleting a user's information simply because an app is deleted is problematic.

In many cases, it may be appropriate to delete a user's information that is stored on a mobile device when the user deletes the relevant app. Care is needed, however, that no other app makes use of that data. For instance, multiple apps may add data to the contacts database, text message history, or photo album on a user's mobile device, and much of this data may be personal information. It would be inappropriate, however, to delete this information simply because the user deletes the app that creates it—the data may remain useful to the user through other apps, or remain an important record for the user in the future. On the other hand, information that is specific to the app in question—such as login details for a remote server—should generally be deleted when the app is deleted.

---

[9] Sydney Morning Herald, *Fifty thousand exposed in ABC website hack*, 27 February 2013, <http://www.smh.com.au/it-pro/security-it/fifty-thousand-exposed-in-abc-website-hack-20130227-2f5j9.html>.

[10] Hunt T, *Lousy ABC cryptography cracked in seconds as Aussie passwords are exposed*, 27 February 2013, <http://www.troyhunt.com/2013/02/lousy-abc-cryptography-cracked-in.html>.

When a user's information is stored remotely—on a developer's servers, "in the cloud" or on the user's home computer—the situation is again more complicated than the guidelines appear to allow. First, it is not clear that developers can satisfy this requirement. They may be unaware that a user has deleted an app from a mobile device and, even if a user deletes an app from every mobile device they own, the app will typically remain associated with that user's account in the relevant app store. Under these conditions, it is not clear how an app developer could be expected to delete a user's information simply because the user has deleted an app from their mobile device.

More importantly, deleting a user's information because the user deletes an app from one mobile device may be detrimental to the user. If a user operates multiple mobile devices with a copy of a particular app on each device, deleting the user's information when one of those copies is deleted will result in the user losing their account entirely, despite the fact that they may wish to continue using the app on their other devices. A user who deletes the Facebook app from a tablet device, for instance, may wish to continue using the Facebook service on their mobile phone or computer. Deleting the user's Facebook information simply because they deleted the app from their tablet would cause enormous inconvenience to the user.

ACCAN therefore suggests that deletion of a mobile app will generally be an inappropriate trigger for an app operator to delete the user's information. The relation between apps and user data will often be complex, and we suggest that the guidelines should be amended to reflect this complexity.

Recommendation 19: in the context of deleting user information, the OAIC guidelines should distinguish between information that is held on the mobile device or on a remote system.

Recommendation 20: in the context of deleting user information, the OAIC guidelines should distinguish between information that is used by a single app and information that may be used by multiple apps.

Recommendation 21: the OAIC guidelines should not require that a user's information be deleted when an app is deleted in cases where this may result in detriment to the end user, including:

— when user information is stored in a collection that is used by multiple apps (such as photo albums, contact databases and messages); and
— when user information is stored on a remote system and may remain useful to the user despite the app being deleted (such as account details and online purchase histories).

Of course, it may be appropriate for a user's account to be automatically closed—and their personal information automatically deleted—after a certain period of inactivity, and there should be transparency about this timing. The point remains, however, that deleting an app from a mobile handset in itself is not a suitable trigger for deleting a user's information.

2.1.5. Obtain meaningful consent—the small screen challenge

Informed consent

The draft guidelines should explicitly recognise the additional sensitivity of personal information for children and young people, the complexity of establishing the informed consent of a child or young person, the differences in decision-making by children and young people, and similar factors affecting the ability of a child or young person to provide informed consent.[11] A child may be less likely to fully consider the privacy implications of providing their personal information, particularly if this information is requested in exchange for unlocking features or levels in a game, for instance. In light of such considerations, it may not be reasonable to infer consent from a child who taps any button that stands between them and playing a new game.

> Recommendation 22: the OAIC guidelines should draw attention to the special considerations that may arise when considering the privacy of children and young people.

ACCAN understands that Apple's "App Store Review Guidelines" include a clause to the effect that an app targeting minors for data collection will generally be rejected from the Apple iTunes store. We believe that this is a laudable position for Apple to take, and encourage the OAIC to strengthen its guidelines in this respect.

There are a number of additional categories of consumers for whom it may be difficult to establish informed consent. Consumers from culturally and linguistically diverse (CALD) communities and consumers with cognitive impairments, for instance, may have particular requirements that a developer should take into consideration when attempting to obtain consent.[12] It would be useful, both for developers and for vulnerable end users, for the OAIC guidelines to set out some of the considerations of capacity that may arise when the user of an app is less able to provide informed consent.

> Recommendation 23: the OAIC guidelines should encourage developers to consider the particular requirements that users may have when attempting to obtain consent to the collection of personal information.

Presentation of simplified privacy policy information for users with accessibility requirements

We support the suggestions in these guidelines that privacy policies should be presented to users in a straightforward way. We caution, however, that some of the suggestions given— in particular, the use of visual and auditory cues to present important information—may present difficulties for users with particular accessibility requirements. Although the guidelines suggest linking the graphics to more detailed text descriptions, this approach would remove the benefit of the simplified presentation of a privacy policy for users with accessibility issues. A preferable

[11] These issues are discussed, for example, in the Australian Law Reform Commission's *For your information: Australian privacy law and practice*, report 108, August 2008, chapters 67–69.

[12] ACCAN, *Informed consent research report*, 2009, <http://accan.org.au/files/Reports/ACCAN_Informed_Consent.pdf>.

approach would be to include a simplified text-based explanation of key aspects of the privacy policy, in addition to any visual or auditory devices.

> Recommendation 24: the OAIC guidelines should be amended to note the importance of maintaining accessibility when presenting simplified descriptions of privacy policies.
>
> Recommendation 25: the OAIC guidelines should recommend including a simplified text-based description of the privacy policy in addition to any visual or auditory devices.

2.1.6. Timing of user notice and consent is critical

Presentation of privacy policies practices prior to purchase

The guidelines note that privacy information should be presented to users "during the download/purchase process and also upon first use". In practice, it may not be open to app developers to present information to users during the purchase process, which is largely handled by app store operators, and once download/purchase process is complete it may be difficult for users to obtain a refund if they disagree with the policy or practices. Users need to have this information made available *before* the download/purchase process. Developers could, for example, provide a link to a webpage with this information in their in-store app page.

> Recommendation 26: the OAIC guidelines should be amended to advise developers to make privacy information available to consumers before any purchase or download begins.

Creativity of presentation

ACCAN agrees with the OAIC's suggestion in these guidelines that developers should consider novel ways to present privacy information to users, and that more creative approaches to presenting privacy information may encourage consumers to read privacy policies and make it simpler for them to do so.

We suggest, however, that a degree of predictability is also important. Excessively "creative" presentations may have the effect of making privacy information more difficult for users to access or understand. For example, privacy information that is presented in a primarily graphical format may lack detail, and waiting for privacy policy information that is presented in a video form may be so time-consuming as to be a disincentive for users to familiarise themselves with the policy.

Developers' creativity needs to be constrained by suitable principles that ensure that privacy information remains clear and accessible. Ideally, any creative presentation should be thoroughly tested to ensure that the information remains useful to end users.

Recommendation 27: the OAIC guidelines should set out suitable constraints on any "creative" presentations of privacy policies to ensure that privacy information remains clear and accessible to users.

2.2. Resources

Descriptions of further resources

The names of the resources listed in this appendix are in many cases insufficient to explain the content of the resources. In order to make this appendix more useful to developers, short descriptions of the resources should be provided.

Recommendation 28: greater detail should be provided about the resources contained in the appendix.