



Annex A: GSMA MPI Privacy Design Guidelines for Mobile Application Development: Use cases for illustration only.

Annex B: High Level Privacy Principles

The use cases contained in Annex A are for illustration purposes and were developed to help put into context the 'Guidelines' contained in the GSMA's discussion document, *'Privacy Design Guidelines for Mobile Application Development'*.

Should you wish to comment on these use cases please respond by email to mobileprivacy@gsm.org Please mark the subject of your email, 'GSMA MPI – Use Cases'.

Annex A: GSMA MPI Privacy Design Guidelines for Mobile Application Development: Use cases for illustration only.

Location Privacy - Use Case

Miguel has purchased a new application that accesses Miguel's location as well as his contacts and camera gallery to enable him to geotag photo's, send these to his friends and share his current location with his friends so they can meet up when in the same city or vicinity.



Location: Example of Good Practice

1. As part of the application purchase process Miguel is offered a summary of the application, its features, the data it uses as well as any retention and sharing the application may involve. This may be offered on the portal from which Miguel buys the application or at point of installation. It is not mandatory for this information to be read and accepted by the user due to the scope and volume of data included it is however available to the user throughout the lifecycle of the application and shall be encouraged to be viewed prior to installation. The application includes a link to "Application Data" in the user setting menu which the user may refer to at any time after installation.

Privacy Policies: Purpose and Use, Respect User Rights

2. On installation the application notifies Miguel that it requires access to Miguel's location as well as his contacts and gives Miguel the choice to grant permission for access by the application. In the event Miguel rejects the request the installation fails.

Privacy Policies: Openness, Transparency and Notice

3. The application is signed by a recognized signing authority and as such includes the developer's full name, a link to the developer's web site and an active support email address that must be maintained as part of the signing process. This information is accessible via the application certificate and is re-produced in the application preferences menu for the application.

Privacy Policies: Openness, Transparency and Notice

4. The application offers Miguel privacy settings that may re-set on each launch of the application (session) or for all subsequent application uses (blanket).

Privacy Policies: User Choice and Control

5. On selecting the 'blanket' option the application advises Miguel that he may change his prompting choice at any time by going to the application preferences menu.

Privacy Policies: [User Choice and Control, Respect User Rights](#)

6. At installation the application notifies Miguel that his location data shall be shared with his social networking "friends" and shall be stored for a period of 3 months and provides Miguel with the choice to accept this or not. In the event Miguel rejects the request the installation fails.

Privacy Policies: [Openness, Transparency and Notice](#)

- 6.a The application/service provider has confirmed via their privacy policy statement that all data stored, held or shared shall be retained for no longer than 3 months unless explicitly required by law or within the context of the applications use case. In the event retention is greater than 3 months the declaration in 6 shall reflect the period. They also assure that data older than this shall be deleted within a further period of 1 month. **Privacy**

Policies: [Data Minimisation and Retention](#)

- 6.b Miguel is provided with a link to the service providers privacy policy via a link in the Application Preferences menu which outlines to the user that their data is a) stored in encrypted form, b) transferred and shared using encrypted bearers, c) anonymised wherever this is possible within the context of the application. The user may also be able to utilise automated privacy profile functionality (P3P) if available.

Privacy Policies: [Security; User Choice and Control](#)

7. The application/service provider provides a link to their website which contains a comprehensive list of the 3rd parties the information will be shared with and a link to that 3rd party's privacy policy (if available).

Privacy Policies: [Accountability and Enforcement](#)

NOTE: In the application used by Miguel a single link is provided in the Application Preferences for privacy information. This provides a menu driven option range for the user to aid readability and reduce unnecessary data utilisation. In the case of Miguel's application the menu choices offered are:

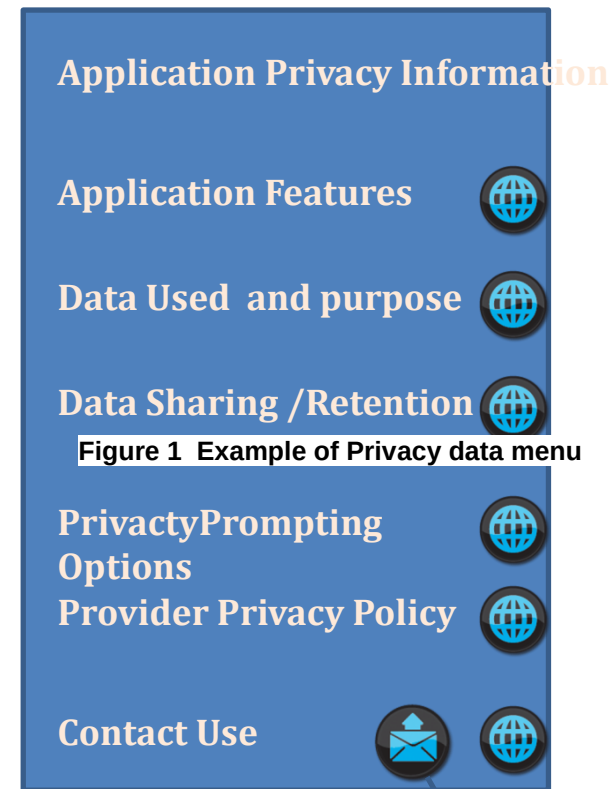


Figure 1 Example of Privacy data menu

mailto:
Coolapps@coolapps.com

8. During installation Miguel is provided with the option to choose whether he provides permission for each instantiation of the application (session) or once with no further need to make future requests (blanket). A single prompt is provided to cover all data categories to be accessed and Miguel is able to provide explicit acceptance of access permission for all with a single consent. In the event Miguel rejects this choice the application defaults to request permission every time the data is requested by the application.

Privacy Policies: User Choice and Control; Respect User Rights

9. The application privacy settings default to session based prompting but offers Miguel the option to use blanket prompting should he wish.

Privacy Policies: User Choice and Control; Respect User Rights

10. The phone Miguel uses' differentiates between trusted and un-trusted applications. Un-trusted applications prompt the user warning that the application is un-trusted, may contain malware and is not recommended by the operator or service provider. It does however offer Miguel prompting options that default to prompting every access with a session based option which Miguel may choose to select.

Privacy Policies: User Choice and Control

11. Though the application is un-trusted (un-signed) the developer has used context sensitive prompting to reduce the impact of prompts on the user experience i.e. when the application asks the user to enter a phone number to make a call or send an SMS/MMS and provides a send button to be used the user is not given a prompt as the context within which the application is working is clear to the user.

Privacy Policies: Openness, Transparency and Notice – context sensitive user experience

12. Whilst Trusted application may not prompt based on the fact they have been signed by a recognized signing authority they shall permit the user to revoke this “blanket” option and select a more informative prompting option such as, prompting on a session basis.

Privacy Policies: User Choice and Control

13. The developer provides the means within the application framework to enable prompts based on the user’s privacy preferences even though this is a trusted application and enables the user to alter these choices at any time via a preferences menu option.

Privacy Policies: User Choice and Control

14. Miguel has become confident in the value of the application but now wants to cut down on the number of times he is being prompted. He therefore decides to revisit the prompting regime he initially adopted when installing the application and is able to access the prompting options via his user settings menu within the application.

Privacy Policies: User Choice and Control

15. All parties providing, using sharing or otherwise benefiting, supporting or delivering the services used by the application have agreed to abide by and support the “Privacy by Design” principle. Data shall be tagged at each phase of the service delivery process to enable privacy breaches to be isolated and dealt with quickly.

Privacy Policies: Accountability and Enforcement



Location: Example of Bad Practice

1. As part of the application purchase process Miguel is offered an application with no supporting information on the features, the data used or whether information will be stored or shared.

Privacy Policies: Purpose and Use, Respect User Rights

2. On installation the application provides no notification to Miguel to indicate that it requires access to Miguel’s location and contacts.

Privacy Policies: Openness, Transparency and Notice

3. The application is signed by the developer and has no independent validation or verification mark. Whilst this is not an issue in itself there is no way to validate or confirm that the developer contact information provided is valid without first installing the application and trying the links.

Privacy Policies: Openness, Transparency and Notice {Risk}

4. Miguel is offered no access to privacy settings that may enable him to alter the privacy defaults of the application.

Privacy Policies: User Choice and Control

5. The application adopts a default 'blanket' option but does not offer Miguel the option to change this to a more stringent permissioning policy such as session or single shot.

Privacy Policies: User Choice and Control, Respect User Rights

6. The application installs and provides Miguel with no indication (or only a partial indication - shared: no indication with whom) his location data shall be shared with his social networking "friends" and shall be stored for a period of 3 months. Miguel is offered no choice other than to halt the application if he does not want the application to do this.

Privacy Policies: Openness, Transparency and Notice

- 6.a The application/service provides no information on its privacy policy and Miguel is unable to decide whether their privacy policies align with his own. Miguel is unable to ascertain if the provider meets national laws in Spain or even to ascertain if the source is a valid provider.

Privacy Policies: Data Minimisation and Retention

7. The application/service provider provides no link to their website.

Privacy Policies: Accountability and Enforcement

8. During installation Miguel is provided with no option to choose whether he provides permission for each instantiation of the application (session) or once with no further need to make future requests (blanket). The application defaults to blanket.

Privacy Policies: User Choice and Control; Respect User Rights

9. The application is untrusted (un-signed) and the developer has not used a context sensitive approach to prompting to reduce the impact of prompts on the user experience i.e. when the application asks the user to enter a phone number to make a call or send an SMS/MMS and provides a send button to be used the user is given a prompt asking them to permission the call even though they have pressed the applications send button.

Privacy Policies: Openness, Transparency and Notice – context sensitive user experience

10. The application is a trusted application and does not prompt based on the fact it has been signed by a recognized signing authority however it does not offer Miguel the ability to revoke this default blanket state when he realises that his data charges are higher than expected.

Privacy Policies: User Choice and Control

11. The developer does not provide the means within the application framework to enable prompts based on the user's privacy preferences.

Privacy Policies: User Choice and Control

12. Miguel is concerned that his network charges are rather higher than they should be and wants to cut the applications access to data without his explicit permission. He therefore decides to revisit the prompting regime he initially adopted when installing the application but finds he is unable to change this.

Privacy Policies: User Choice and Control

13. Miguel can find no indication or supporting information that indicates that all parties providing, using sharing or otherwise benefiting, supporting or delivering his service have agreed to abide by and support "Privacy by Design" principles and he is unable ascertain the level of protection his data will be provided with throughout the applications life cycle.

Privacy Policies: Accountability and Enforcement

Children's Privacy: Use case



Child Privacy: Example of Good Practice

1. Ayshah wants to use the application store client provided by her service provider on her new phone. In particular she would like to download the social networking application her friends use. Because Ayshah has never used this feature before and she is under 18 she is presented with a prompt indicating she must be over 18 to download or use the application.

Privacy Policies: Children and Adolescents, Purpose and Use, Openness, Transparency and Notice

2. Ayshah's service provider sets all privacy and content access to Blocked as a default for applications restricted to persons over 18 years of age .They require explicit 'opt in' by the bill payer before they will activate services and adult content.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

3. When Ayshah gets home she asks her mother if she can download the application. Ayshah's mother calls the service provider and indicates she is happy for Ayshah to have access to the app store and advises the service provider that Ayshah is 10 years old. The service provider activates their 'age banded' content system and provides Ayshah with access to the app store.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

3a The banded content system on the application store presents content based on privacy and age profiles defined by the bill owner and the users age.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

4. Next day at school Ayshah accesses the application store. She is presented with content that is suitable for 12 years and under due to the content banding system used by her service provider.

Privacy Policies: Children and Adolescents

5. Ayshah locates the social networking application her friends are using and downloads it to her phone. The application store has made it clear that this application will share Ayshah's personal information and explicitly states what information will be shared.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice

6. The application store sends the bill payer (Ayshah's mother in this case) an email/SMS to confirm there has been a transaction. They also include a unique transaction identifier.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement, Purpose and Use, Openness, Transparency and Notice

7. The application indicates that it may share Ayshah's location data. Since Ayshah is not the bill payer and is under 18 years of age her location information may only be shared if the bill payer grants permission.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice

8. When Ayshah gets home she asks her mother to enable her location information to be shared with her friends. Ayshah's mother confirms the location information is shared only with members of her 'buddy list' and these may be selected or de-selected individually via the application interface.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

9. Ayshah's mother calls their service provider and grants permission for Ayshah's location to be shared using the unique transaction identifier to confirm she is the bill payer.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

10. The service provider activates provision of location for Ayshah and in addition sends an email/SMS to Ayshah's number to ensure she is aware this has happened. In addition the service provider also sends an SMS to the bill payers mobile to confirm this has taken place.

Privacy Policies: Children and Adolescents, Security, Accountability and Enforcement

11. Ayshah launches her application and selects those friends on her buddy list with whom she wants to share her location. Only those friends she actively selects are provided with her location information.

Privacy Policies: User Choice and Control

12. Ayshah's application includes a small cartoon icon in the lower right hand corner which Ayshah may use at any time to report concerns.

Privacy Policies: Children and Adolescents

13. Ayshah's device enables the application to run in the background without closing down. If the application is active for a period of more than 36 hours the application provides Ayshah with a reminder that she is still sharing her location.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice, Respect User Rights

14. Ayshah closes the application after school and then re-opens it the next morning. The application provides Ayshah with a prompt reminding her that she is sharing her location every time she launches the application and provides a simple icon to enable her to stop providing location.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice, Respect User Rights



Child Privacy: Example of Bad Practice

1. Ayshah wants to use her service provider's application store client on her new phone to access the application store to download the social networking application her friends use. She is able to access the application store immediately.
Privacy Policies: Children and Adolescents, Purpose and Use, Openness, Transparency and Notice
2. Ayshah accesses the application store. Ayshah locates the social networking application her friends are using and downloads it to her phone. The application store has not made it clear that the application will share Ayshah's personal information.
Privacy Policies: Children and Adolescents, Purpose and Use, Openness, Transparency and Notice
3. The application allows Ayshah to share her location immediately without the need for her to have this activated by the bill payer, her parent or guardian.
Privacy Policies: Children and Adolescents, Respect Users Rights, Openness, Transparency and Notice
4. Ayshah launches her application; the application shares her location with everyone in her buddy list.
Privacy Policies: Openness, Transparency and Notice, Respect Users Rights
5. Ayshah's device enables the application to run in the background without closing down. The application may run for months without being re-set or re-started. During this time the application provides no additional prompts to remind Ayshah she is sharing her location.
Privacy Policies: Respect Users Rights, Openness, Transparency and Notice
6. Ayshah closes the application after school and then re-opens it the next morning. The application provides Ayshah with no launch time prompts to remind her she is still sharing her location.
Privacy Policies: Purpose and Use, Openness, Transparency and Notice, Respect User Rights



Advertising Privacy: Example of Good Practice

1. Ulrich accesses one of his favourite application stores and finds a suitable application.
2. The app store provides a summary of the application, its features, the data it uses as well as any retention and sharing the application may involve. The app store description also explicitly flags the fact that the application provides purchase discounts provided Ulrich is happy to have targeted advertising sent to him based on his current location.

Privacy Policies: Purpose and Use, Respect User Rights

- a. The application store makes it clear that the application and the targeted advertising need to have bill payer's permission.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice

- b. Users who are not bill payers have similar content Blocked defaults set as outlined above. They require explicit 'opt in' by the bill payer before these capabilities may be activated.

Privacy Policies: Security, Purpose and Use, Children and Adolescents

3. Ulrich reads the application store description and also looks at the application providers 'Privacy Policy' for the application which is included as a link on the application store description.

Privacy Policies: Purpose and Use, Openness, Transparency and Notice

4. Having read the information Ulrich decides to download the application.

5. The application has not been tested or signed by a recognized signing authority or review process. At installation the platform warns Ulrich that this is an untrusted application and indicates what functions and features need to be permissioned. A single prompt is provided asking Ulrich if he wants to install the untrusted application. This default to NO, Ulrich must select YES to install. A second prompt indicates what permissions are needed and provides Ulrich with the choice to accept or reject. Here again the default is REJECT, Ulrich must explicitly select ACCEPT. In the event Ulrich accepts the application installs. If Ulrich rejects the application does not install.

Privacy Policies: User Choice and Control, Purpose and Use, Openness, Transparency and Notice

6. Ulrich accepts the application installation. On installation completion the application defaults to no targeted advertising being pushed to Ulrich.
Privacy Policies: Respect User Rights, User Choice and Control, Openness, Transparency and Notice
7. Ulrich has to explicitly request that the targeted advertising be sent via the application configuration menu. The application may wish to prompt Ulrich on start up for the first time asking whether Ulrich wishes to accept advertising. If Ulrich rejects the request, the application may provide Ulrich with a reminder. Reminders should not be sent too frequently so as to cause annoyance. **Privacy Policies: Openness, Transparency and Notice**
8. Ulrich decides to activate the push advertising option and does so via the application settings menu.
Privacy Policies: Respect User Rights, User Choice and Control, Openness, Transparency and Notice
9. Having accepted the provision of the targeted advertising via the application settings menu Ulrich is able to **disable provision at any time by changing settings** on the application settings menu.
Privacy Policies: User Choice and Control
10. The application automatically switches push advertisements OFF when Ulrich is roaming. Should Ulrich want to have the service whilst roaming he is able to activate 'While Roaming' via the application settings menu.
Privacy Policies: Security, Data Minimisation, Openness Transparency and Notice
11. The 'While Roaming' setting is reset once the application runs on Ulrich's home network. Ulrich is required to explicitly re-activate 'While Roaming' after the application resets.
Privacy Policies: Security, Data Minimisation, Openness Transparency and Notice
12. Ulrich is happy to accept advertising whilst roaming and the related charges that will incur. He sets 'While Roaming' to 'Accept'. The application will continue to provide advertising either in the Home or Roaming networks until such time as Ulrich disables it.
Privacy Policies: User Choice and Control
13. Ulrich is generally happy with the content being pushed to him. It is generally well targeted and has proven useful. One advertiser however sends adult content which Ulrich is unhappy with as he has a young family.
Privacy Policies: Respect User Rights, User Choice and Control, Openness, Transparency and Notice, Accountability and Enforcement.
14. Ulrich uses the advertisers preferences ('Opt in') option via a link in the applications settings menu and deactivates content from this advertiser.
Privacy Policies: User Choice and Control

15. Ulrich finds the information continues to be delivered. He uses the link in the application set up menu to contact the developer/service provider and reports that his request has not been actioned.

Privacy Policies: **Respect User Rights, User Choice and Control, Accountability and Enforcement.**

16. The Developer/Service Provider sends Ulrich an SMS confirming they have his request and have actioned it.

Privacy Policies: **Respect User Rights, Accountability and Enforcement.**



Advertising: Example of Bad Practice

1. Ulrich accesses one of his favourite application stores and finds a suitable application.

2. The app store provides a summary of the application, its features, the data it uses as well as any retention and sharing the application may involve. The app store description does not explicitly highlight the fact the application will push targeted advertising to Ulrich.

Privacy Policies: **Openness, Transparency and Notice, Purpose and Use, Respect User Rights**

3. Ulrich reads the application store description but is unable to see links to a developer portal or contact email address. Neither is Ulrich able to find a link to the developers/distributors 'privacy policy.

Privacy Policies: **Openness, Transparency and Notice, Purpose and Use, Respect User Rights**

4. Ulrich decides to go ahead with the download.

5. The application has not been tested or signed by a recognized signing authority or review process. At installation the platform does not advise Ulrich that this is the case.

Privacy Policies: **Openness, Transparency and Notice, Purpose and Use, Respect User Rights, Security, User Choice and Control**

6. Ulrich is not provided with any prompts relating to the functionality the application needs or seeking permission to access his person data including his location.

Privacy Policies: **User Choice and Control**

7. On installation the application starts pushing targeted advertising to Ulrich.

Privacy Policies: User Choice and Control

8. Ulrich is unable to deactivate this from the application interface and no link is provided to enable Ulrich to ask the service provider/distributor to deactivate it.

Privacy Policies: Respect User Rights, User Choice and Control

9. The application provides no ability to switch push advertisements OFF when Ulrich is roaming.

Privacy Policies: Respect User Rights, User Choice and Control

10. Ulrich is not happy with the content being pushed to him. It is often poorly targeted and includes adult material.

Privacy Policies: Accountability and Enforcement

11. Ulrich is unable to deselect specific advertisers or to switch off the targeted advertising without uninstalling his beloved coffee application.

Privacy Policies: Respect User Rights, User Choice and Control

Annex B: High Level Privacy Principles

“Privacy by Design”

The high-level Principles set out below broadly describe the privacy outcomes mobile users should experience. They are not intended to replace or supersede applicable law but to foster business practices and standards that deliver meaningful transparency, notice, choice and control for users with regards their personal information and the safeguarding of their privacy.

Openness, Transparency and Notice –

Responsible persons shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices. Users shall be provided with information about persons collecting personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users’ personal information, including to whom their personal information may be disclosed, enabling users to make informed decisions about whether to use a mobile application or service.

Purpose & Use –

The access, collection, sharing, disclosure and further use of a users' personal information shall be limited to meeting legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.

User Choice and Control –

Users shall be given opportunities to exercise meaningful choice, and control over their personal information

Data Minimization and Retention –

Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected and otherwise accessed and used. Personal Information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations, and should subsequently be deleted or rendered anonymous.

Respect User Rights –

Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.

Security –

Personal Information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.

Education –

Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.

Children & Adolescents –

An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and compatible with national law.

Accountability & Enforcement –

All Responsible Persons are accountable for ensuring these principles are met.