



Applying the legislation

Guideline *Information Privacy Act 2009*

Privacy and Mobile Apps

This guideline¹ provides information about the mobile app environment and its potential impact on the privacy of users. It also sets out some key considerations for Queensland Government agencies which develop mobile apps to ensure compliance with the privacy principles in the *Information Privacy Act 2009* (Qld) (**IP Act**).

What are mobile apps?

A mobile application or 'mobile app' is a software program designed to run on a smartphone, tablet computer or other mobile device. Mobile apps are increasingly being used as part of the government's delivery of services to the community.

Does the IP Act apply to mobile apps?

Any system which involves the collection, storage, use or disclosure of personal information by a Queensland government agency (or its bound contracted service providers) is subject to the requirements of the IP Act, including the Information Privacy Principles (**IPPs**) for non-health agencies and the National Privacy Principles (**NPPs**) for health agencies. Because mobile apps potentially capture information about their users the privacy principles must be taken into account in both the app's design and the information provided to users.

Although the IP Act only applies to Queensland government agencies and bound their contracted service providers, app developers outside of government may find this resource useful.

Privacy challenges for mobile apps

Mobile app capabilities present unique challenges for privacy protection. Mobile apps have the potential to collect significant amounts of personal information about users, often without them being aware of the collection. Mobile apps may be able to access:

- the user's phone and email contacts
- call logs
- internet data
- calendar data

¹ In developing this information sheet OIC acknowledges the Canadian resource - 'Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps' developed jointly by the Office of the Privacy Commissioner Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia.



Office of the Information Commissioner
Queensland

- data about the device’s location²
- the device’s unique IDs³; and
- information about how the user uses the app.

The scope of personal information which can potentially be collected, combined with the speed at which apps are developed and distributed, could result in the personal information of hundreds of thousands of users being collected in a short space of time.

Privacy considerations when developing mobile apps

Like any other project involving personal information privacy should be included in the planning phase of an app’s development. It will also be an important consideration for the entire life cycle of the app.

Some key privacy considerations are set out in the table below.

Action	Relevant legislation
<p>Complete a Privacy Impact Assessment as part of project planning.</p> <p>Consider and map the flow of personal information. This will help to identify privacy vulnerabilities in a systematic way.</p>	
<p>Consider what personal information is essential for the app.</p> <p>Consider whether the app needs to collect and use personal information at all to function. If it does, collect only as much personal information as you need. Do not collect personal information just because it may be useful or valuable in the future.</p>	<p>IPPs 1-3</p> <p>NPP 1</p>
<p>Tell people how the app will use personal information.</p> <p>During the installation, tell users what personal information the app is collecting, what it will be used for, and who it will be shared with. It can be difficult to communicate this information effectively in the small screen environment. Consider strategies for giving an effective notice, such as layering information and putting important information up front, or using graphics, colour or sound to draw attention to notices.</p>	<p>IPP 2</p> <p>NPP 1</p>

² Which will generally be the location of the device’s user.

³ Each mobile device can have a number of unique identifiers, including the International Mobile Station Equipment Identity number (IMEI), Wi-fi Media Access Control (MAC) address, Internet Protocol (IP) address and Bluetooth address.



Office of the Information Commissioner
Queensland

<p>Consider how personal information will be stored and secured.</p> <p>The IP Act requires that personal information is protected against unauthorised access, loss or misuse. Ensure that the storage and security of any personal information collected through the mobile app is well planned, and that appropriate controls are in place on both the mobile device and backend systems that will store personal information. Security safeguards should be appropriate to the sensitivity of the information.</p>	<p>IPP 4 NPP 4</p>
<p>Have a clear and accessible privacy policy.</p> <p>Ensure you have a clear and accessible policy which enables users to evaluate what you propose to do with their personal information. Users should be able to access this information before deciding whether to download the app.</p> <p>Make sure your policy lets users know how they can access or amend their personal information, how they can delete the app or their subscription to the app, and what will happen to personal information already collected and stored.</p>	<p>IPP 5 NPP 5</p>
<p>Only use personal information for the purpose it was collected; only disclose personal information in permitted circumstances.</p> <p>Agencies may need to use and disclose personal information for an app to function. For example, location data may be required to deliver certain functions in a navigation or public transport app. Agencies may need to share personal information with another entity to provide the services offered by the app. Apps should generally only use personal information for the purpose it was collected, and only disclose to the individual it is about, except in limited circumstances. Agencies should monitor apps to ensure personal information is only used and disclosed in ways that are permitted by the IP Act and in accordance with their privacy policy.</p>	<p>IPP 10-11 NPP 2</p>
<p>Will personal information be transferred out of Australia?</p> <p>The IP Act sets out additional requirements when personal information is transferred outside of Australia. If the development or delivery of the app will involve the transfer of personal information outside of Australia you will need to consider the obligations in section 33 of the IP Act.</p>	<p>Section 33 IP Act</p>



Office of the Information Commissioner
Queensland

<p>Consider whether contractors will be engaged to perform any services which involve the transfer of personal information.</p> <p>If an agency plans to engage a contracted service provider to perform services connected with the development or delivery of an app, compliance with the rules about contracted service providers in the IP Act may be required.</p> <p>See the OIC Guideline Agency obligations when entering into contracts and other agreements⁴.</p>	<p>Chapter 2, Part 4 IP Act</p>
<p>Consider the end of life of personal information</p> <p>Ensure that a plan exists for when the app is deleted, or subscription ends, taking into account public records and other legal obligations.</p>	<p><i>Public Records Act 2002 (Qld)</i></p> <p>NPP 4(2)</p>
<p>Plan for breaches and complaints.</p> <p>Agencies should develop specific procedures for dealing with privacy breaches and complaints associated with their mobile apps.</p>	<p>Chapter 5 IP Act</p>

For additional information and assistance on handling personal information under the IP Act please refer to the OIC's guidelines or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au

Published 29 April 2013 and last updated 31 July 2017

Changes to legislation after the update date are not included in this document

⁴<https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers/overview-of-agency-privacy-obligations-when-entering-into-contracts-and-other-agreements>