



Office of the Information Commissioner Queensland

Privacy and Mobile Apps

How three Queensland government agencies meet their obligations under the *Information Privacy Act 2009* (Qld) when developing and operating mobile apps

We thank the staff of the audited agencies for their support and co-operation.



The Office of the Information Commissioner licenses this report under a Creative Commons – Attribution License. People reading or using this report may do so in accordance with the following conditions: Attribution (BY), requiring attribution to the original author.

© The State of Queensland. (Office of the Information Commissioner) 2017

This report is available on our website at www.oic.qld.gov.au. You can request further copies from us at:

Office of the Information Commissioner
Level 8, 160 Mary Street, Brisbane, Qld 4000
PO Box 10143, Adelaide Street, Brisbane, Qld 4000
Phone 07 3405 1111
Fax 07 3405 1122
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-9953725-4-2

August 2017

The Honourable Peter Wellington MP
Speaker of the Legislative Assembly
Parliament House
George Street
Brisbane QLD 4000

Dear Mister Speaker

I am pleased to present *Privacy and Mobile Apps: How three Queensland government agencies meet their obligations under the Information Privacy Act 2009 (Qld) when developing and operating mobile apps*. This report is prepared under section 135 of the *Information Privacy Act 2009 (Qld)*.

The report outlines agencies' practices in handling personal information, in particular their compliance with the privacy principles and the Act, when planning, developing and operating mobile apps. It identifies examples of good practice and makes recommendations to all government agencies.

In accordance with subsection 193(5) of the Act, I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Rachael Rangihaeata'.

Rachael Rangihaeata
Information Commissioner

Table of contents

1	Summary	1
	Conclusions	2
	Privacy in planning and development.....	3
	Privacy when collecting personal information.....	4
	Privacy when storing, using or disclosing personal information.....	5
	Recommendations.....	5
	Agency responses	6
2	Context	7
	Audit objectives, scope and method	9
	Report structure	12
3	Privacy when planning and developing mobile apps.....	13
	Conclusion.....	14
	Detailed findings	15
	Recommendations.....	19
4	Privacy when collecting personal information	21
	Conclusion.....	21
	Detailed findings	22
	Recommendations.....	25
5	Privacy when handling personal information	27
	Conclusion.....	28
	Detailed findings	29
	Recommendations.....	31
	Appendix A – Agency responses	35
	Appendix B – Methodology.....	51
	Appendix C – Commonly used terms and acronyms	53
	Appendix D – References.....	55
	Appendix E – Overview of Privacy Impact Assessment (PIA) process.....	57

1 Summary

Government agencies are increasingly using mobile apps to connect with the community, for example through social media apps. They are also developing and deploying their own apps to deliver services and offer another way for Queenslanders to interact with government.

Australians are becoming more discerning about privacy, and want to be able to choose the personal information they provide and its use, including in mobile apps. This means government agencies need to design mobile apps with privacy in mind.

Unlike traditional programs for desktop computers, mobile apps can seek permission to access information stored on hand-held devices. This includes location, contacts and pictures. Mobile apps can also seek permission to access and use a device's features such as the camera, microphone and GPS.

Government agencies must give sufficient information to individuals so they understand about the personal information the agencies collect, use and usually disclose.

Governments around the world recognise the importance of data security. In Queensland, government agencies have to comply with the requirements in the *Information Privacy Act 2009* (Qld) and, where applicable, in the Queensland Government Enterprise Architecture, which guides information and communications technology. This includes protecting personal information against loss, unauthorised access and other misuse.

Users who are confident that a government agency handles their personal information appropriately are more likely to maintain trust in the agency, use an agency's app and benefit from it.

We selected three mobile apps for detailed review:

QParents – operated by the Department of Education and Training (DET)

MyTransLink – operated by the Department of Transport and Main Roads (TMR)

Policelink – operated by the Queensland Police Service (QPS)

The objective of the audit was to assess whether agencies effectively apply the privacy principles when developing and operating mobile apps for the community.

We considered the nature of the personal information the agencies collect, use and disclose. In particular, we examined whether agencies:

- adequately considered the privacy principles when planning and developing mobile apps
- applied the privacy principles when collecting personal information through mobile apps
- adequately managed the security, access and use of personal information collected through mobile apps.

Conclusions

The three audited agencies adopted different approaches to deal with their privacy obligations when developing and operating the mobile apps.

It is more efficient to design an information system with privacy in mind from the outset, rather than trying to add privacy protections once the system is operational. QParents is a good example of the benefits of the privacy by design approach. DET considered the privacy aspects of the QParents app in detail at the development stage. The department also built appropriate security measures to protect personal information handled through the app. As a result, the privacy protections in QParents support user confidence in the app and trust in government agencies.

TMR adopted another approach, minimising the personal information its MyTransLink mobile app collects. The department has also set up a regular technical testing regime. These are effective ways to manage an agency's privacy obligations and reduce privacy risk.

QPS focused on getting the Policelink mobile app up and running. It did not consider the privacy aspects of the app when developing it in 2012 because of poor project governance. QPS developed an initial Privacy Impact Assessment in July 2017 at the conclusion of this audit. While this is a first step in incorporating privacy into the app, there is more work to do. The delay in considering the privacy aspects of the mobile app means that QPS cannot demonstrate how it ensured the app met the privacy principles, the legislative requirements or its own policies about privacy.

The three agencies inform the users about the personal information they collect through their respective mobile apps. The apps have multiple links to privacy statements and other privacy information. There is a mix of generic privacy information and information tailored to a particular app. While this enables individuals to understand how the agencies will use and disclose the personal information they collect through the apps, it can also be confusing.

There is less information on why the apps seek permission to access specific features on the device.

DET and TMR have designed the apps to protect information during collection, transfer and storage. They have implemented security controls and testing practices, supported by strong information governance frameworks. As a result, they can demonstrate they adequately manage the security, access and use of personal information collected through the apps.

QPS did not test the app before deploying it and has not set up a testing regime. Weak governance means that QPS operates the app in isolation from its strategic information governance and its information and communication technologies (ICT) management and policies. Thus, QPS is unable to demonstrate how it manages the security, access and use of personal information collected through the Policelink app.

Privacy in planning and development

Considering the privacy implications of an app when developing it is a good way to make sure the agency meets its privacy obligations. Visible privacy protections such as data encryption increase consumer confidence and trust, and hence increase the likelihood that consumers will use the app.

A Privacy Impact Assessment (PIA) enables agencies to identify the personal information they intend to collect and consider how they will manage it. The principles underpinning a PIA apply to any government agency.

DET conducted a comprehensive PIA for QParents to assess possible privacy impacts. This is appropriate given the sensitivity of the personal information QParents collects and uses.

TMR chose not to conduct a PIA because it decided that the MyTransLink mobile app would not collect personal information, unless a user elects to receive a response to their feedback.

The Policelink mobile app collects personal information. However, QPS did not conduct a PIA before launching the app even though its policies support the conduct of a PIA or equivalent.

The lack of a PIA means QPS cannot demonstrate how it ensured, at the development stage, that the app met the privacy principles. QPS was not able to identify and manage privacy risks related to the Policelink app, for example explaining the specific purpose for which it collects demographic information.

QPS completed a PIA in July 2017. It is a good first step to incorporate privacy considerations into the existing mobile app, but QPS needs to do more work. For example, the PIA does not explain why noncompliance with five specific Information Privacy Principles is necessary for law enforcement activities for all or any of the personal information collected through the

Policelink mobile app. Similarly, the PIA does not explain the technological and procedural security measures QPS is applying to protect personal information.

A PIA is a living document, and it loses relevance when agencies do not keep it up to date. Agencies need to reassess the privacy impacts of the app regularly, for example, when they update the app or release new features, to identify vulnerabilities and manage their privacy obligations.

Privacy when collecting personal information

Under the *Information Privacy Act 2009* (Qld), agencies collecting personal information must take all reasonable steps to make people generally aware of why they are collecting the information and how they will use it. When a mobile app seeks permission to access personal information through specific features on the device, for example the camera, microphone or location tracker, agencies should provide a collection notice to the user at the earliest opportunity.

DET tailored the privacy information to QParents. The collection notice is clear and detailed, and the policies are comprehensive, except about the current permissions. However, depending on the starting point, the user can access up to six different sources of information about privacy practices relevant to QParents. The terms and conditions for QParents list the permissions required, but not the reasons for seeking these permissions. For example, they state that the Google Analytics cookies collect location information, but do not explain why the app needs to access location information.

TMR does not collect personal information for the operational functions of the app. Even so, there are links from the MyTransLink app to three sources of information about privacy, including privacy policies tailored to TransLink and generic information.

Originally, the privacy information associated with individual Policelink forms was overly generic. As we were finalising the audit, QPS rationalised the collection notices for 20 forms and upgraded its privacy statement. The landing pages for these forms include an appropriate collection notice and a link to the service's upgraded privacy statement. However, the reasons for collecting, and seeking permission to use, personal information are unclear for specific collections. For example, QPS does not explain how it will use information about a user's aboriginality when the user is reporting graffiti. Similarly, it is unclear how QPS will use access to recording audio through the microphone.

Agencies controlling documents containing personal information must ensure that the documents are protected against: loss; unauthorised access, use, modification or disclosure; and any other misuse. There are also broader requirements for information security. Security testing before deploying a mobile app, an upgrade to an existing app or new feature, should be standard practice for all agencies.

DET and TMR have considered the technical aspects of data protection, and the information governance, strategic information management and day-to-day operation of the QParents and MyTransLink mobile apps. Both departments tested their mobile apps before deploying them.

DET and TMR have rigorous, ongoing testing regimes to identify vulnerabilities and to ensure cyber-security protections are in place. This includes identifying and mitigating the risks of the app being a means of accessing or penetrating wider departmental systems.

QPS did not consider cyber-security aspects of the Policelink app before deploying it, or progressively as it released new functions, or in anticipation of new releases. The app developers assumed that other business units within QPS were responsible for information governance. They focussed on the immediate task of achieving functionality.

QPS has not advised how it is managing the security, access and use of personal information collected through the Policelink mobile app.

Recommendations

We recommend that:

1. DET updates its privacy impact assessment for QParents to address expanded permissions
2. QPS enhances its privacy impact assessment for the Policelink mobile app, and documents in detail how it will ensure the app meets the requirements of the *Information Privacy Act 2009* (Qld) and of the Queensland Government Enterprise Architecture
3. DET, TMR and QPS ensure the sources of information about privacy accessible from the app are consistent and complete, to give users enough information about the agency's practices in handling personal information in the context of the app
4. DET, TMR and QPS explain to the users the reasons for the permissions to access a device's features
5. TMR includes information, on the TransLink website, about how to provide feedback or make a privacy complaint

6. QPS updates the collection notices within forms about specific collections or specific questions
7. QPS sets up a regime of cyber security testing for the Policelink mobile app, including vulnerability assessments and penetration testing

We also recommend that all agencies:

- a. assess the privacy impacts of mobile apps at the development stage to identify and plan how they will meet the requirements of the *Information Privacy Act 2009* (Qld)
- b. document how they consider privacy at key stages of developing and operating their mobile apps
- c. reassess the privacy impacts of mobile apps regularly, for example when rolling out new features and updates, to identify vulnerabilities and manage their privacy obligations
- d. give users a clear, specific and complete collection notice, tailored to the mobile app
- e. outline the device's features the app requests access to and explain the reasons for seeking these permissions
- f. ensure they protect the personal information collected through mobile apps against: loss; unauthorised access, use, modification or disclosure; and any other misuse. This includes testing each app for vulnerabilities before deploying it and at key stages of its life.

Note: All agencies means all government agencies subject to the *Information Privacy Act 2009* (Qld) including Queensland government departments, statutory bodies, local governments, public universities, Hospitals and Health Services, and other public authorities.

[Agency responses](#)

We provided a copy of this report to the audited agencies for their comments. We considered their views in reaching our conclusions.

The agencies' responses are in Appendix A.

2 Context

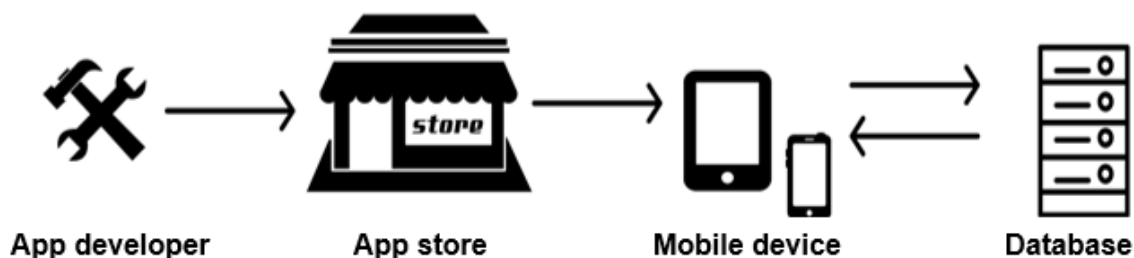
A mobile app is a software application developed for use on small, wireless computing devices, such as smartphones and tablets, rather than desktop or laptop computers.

The most commonly used mobile apps are social networking apps or games. However, Australians also use mobile apps to obtain services, including government services. Users report higher levels of satisfaction with government e-services compared with any other service delivery method, other than face-to-face service delivery.



Mobile apps provide another pathway to government services, which increases the efficiency of their delivery. Apps are effective if members of the community are willing to use them and confident that their personal information is protected.

We chose mobile apps for review that an app developer had designed for release through the two largest app stores. Once downloaded from the app store onto the mobile device, the app interacts with the agency's systems to provide government services to the community.



Australians are becoming more discerning about privacy, and want to be able to choose the personal information they provide and its use, including in mobile apps. About half (44%) of Australians will choose not to use an app on a mobile device to protect their personal information.

94% of consumers consider 'trust' more important than the 'ease of use of a website', app or device.



The community rates trust highly. Most Australian consumers believe that trust is more important than convenience. Convenience includes the ease of use of a website, app or device.

In 2017, a survey of Australians' attitudes to privacy found that the community trusted health service providers the most (79%), followed by financial institutions (59%) and state and federal government departments (58%).

In maintaining community trust, government agencies need to design mobile apps with privacy in mind. Unlike traditional programs for desktop computers, mobile apps can seek permission to access information stored on the hand-held devices. This includes location, contacts and pictures. Mobile apps can also seek permission to access and use a device's features such as the camera, microphone and GPS.

A hand-held device is inherently different to a desktop computer. Mobile apps have additional security and privacy concerns. For example, data transmitted through a mobile app using Wi-Fi transmission is susceptible to interception.

Cyber security is a key concern for both federal and state levels of government. The Queensland government recognises the importance of data security. All agencies have to comply with the requirements in the *Information Privacy Act 2009* (Qld) and departments and statutory bodies have additional obligations under the Queensland Government Enterprise Architecture which guides information and communications technology. App developers building mobile apps for government must also satisfy the requirements of the app stores before the app is available to the public.

It is more efficient to design an information system with privacy in mind from the outset, rather than trying to add privacy protections once the system is operational. Visible privacy protections increase consumer confidence and trust, and hence increase the likelihood that consumers will use the app. If a mobile app has vulnerabilities or breaches users' privacy, agencies may end up with time-consuming procedures and/or expensive payouts to resolve issues or privacy breaches.

Government agencies achieve better outcomes and meet community expectations when they incorporate privacy considerations in the design of mobile apps.

The objective of the audit was to assess whether agencies effectively apply the privacy principles when developing and operating mobile apps. We examined whether agencies:

- adequately consider privacy principles when planning and developing mobile apps
- apply the privacy principles when collecting personal information through mobile apps
- adequately manage the security, access and use of personal information collected through mobile apps.

We considered the nature of the personal information the agencies collect, use and disclose. We can only provide limited assurance on the findings about the technical aspects discussed in Chapter 5. This is because we relied on agencies' self-assessments and we do not have the technical expertise to test these.

Scope

The audit examined three government agencies' mobile apps available to the community:

QParents – operated by the Department of Education and Training (DET)

MyTransLink – operated by the Department of Transport and Main Roads (TMR)

Policelink – operated by the Queensland Police Service (QPS)

These apps are web-based apps in the sense that they access information over a network connection, rather than existing information within a device's memory. We examined the apps available on the Australian Android/Google Play and iOS/Apple apps stores. We define the mobile app from the users' perspective, for example when they access a web-interface from a portable device and submit online forms or receive alerts and notifications.

This audit did not assess the platforms (Apple app store or Google Play store) distributing the apps, their operating systems, the security or privacy aspects of the platforms, or their collection of personal information. Similarly, any vulnerabilities of the devices themselves and their operating systems were not within scope. This includes overseas transfer or backup of information by the apps' operating systems.

QParents is a portal to online information in OneSchool, which is a system that supports teachers, administrators, parents and students in:

- student management
- curriculum and learning management
- finance and asset management
- resource management
- performance, reporting and analysis.



QParents provides parents of Queensland state school students with secure online access to their child's information. It works on an 'opt in' model, where schools must first express interest in using the portal. Once DET rolls out QParents to the school, the school can invite parents to register for the portal.

Registered parents gain direct access to the student's information the school has decided to make available, for example student timetable, attendance records, report cards, invoices and payments. Parents can also use QParents to communicate with the school, for example about their child's absences.

DET launched the app on 30 May 2016 after a pilot program. The department reported that, as at November 2016, it had released QParents to 544 schools with 322 schools having started inviting parents. Approximately 30,000 parents had registered, covering approximately 43,000 students.

MyTransLink**Department of Transport and Main Roads**

MyTransLink is an app that provides timetables and other information about bus, train, ferry



and tram services in south east Queensland, Cairns and Mackay. The app allows customers to set their favourite services or stops, plan their journey and receive notifications and service alerts. In south east Queensland, customers can also access the trip announcer feature to track their journey in real-time.

Mobile app users have downloaded the MyTransLink app 573,346 times between its launch in December 2014 to the end of September 2016. MyTransLink has 80,349 weekly active users.

Policelink is a division of QPS. It provides a multi-channel point of contact for members of the community wishing to make non-urgent contact with Queensland Police.

The Policelink mobile app is one option for reporting non-urgent incidents, including wilful damage and graffiti, lost property and fare evasion.



The Policelink phone number, 131 444, is another way to contact police for non-urgent assistance.

In October 2012, QPS launched a set of online forms on its website and the Policelink app on Australian app store platforms (Android/Google Play and iOS/Apple). The app is also available on the Windows app store.

Between 2012 and 2015, QPS added forms to the Policelink webpage. The mobile app enables some, but not all, of the webpage functions.

For example, a member of the community cannot use the Policelink mobile app to report cold call investment fraud. Similarly, an individual without a passport or a driver's licence can only report wilful damage and graffiti over the phone or in person.

QPS advised that, across all platforms, the app was downloaded over 65,000 times in the four years preceding 2017, compared with 180,000 downloads in the three years preceding 2015.

Method

We conducted this audit under section 135 of the *Information Privacy Act 2009* (Qld). It provides for a broad audit scope and allows the Information Commissioner to review entities' personal information handling practices, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally.

Details of the audit methodology are provided in Appendix B.

The report is structured as follows:

Section	Contents
Chapter 3	examines privacy when planning and developing mobile apps
Chapter 4	examines privacy when collecting personal information
Chapter 5	examines privacy when storing, using or disclosing personal information
Appendix A	contains the responses received from the audited agencies
Appendix B	outlines the audit methodology
Appendix C	lists the terms and acronyms used in this report
Appendix D	contains references
Appendix E	overview of privacy impact assessment process

3 Privacy when planning and developing mobile apps

Privacy should be built in, not bolted on.¹

Agencies should consider the privacy implications of any proposal from the outset. This is often more efficient than retrofitting systems, policies, services or products with privacy protections.

Privacy Impact Assessments (PIAs) support good governance and encourage designing systems with privacy in mind. Agencies can use a PIA to identify, and plan for, how they will meet the requirements of the *Information Privacy Act 2009* (Qld).



Different projects will require different PIAs depending on the risk, the sensitivity and the volume of the personal information handled. The principles are scalable and applicable to any government agency. At a minimum, agencies should perform, and keep a record of, a threshold privacy assessment. The threshold assessment enables agencies to determine whether they need to undertake a full PIA process. Generally, if an app involves personal information, some form of PIA is necessary. We have published a guideline on PIAs on our website, and provide an overview at Appendix E.

When agencies are developing a mobile app, a PIA enables them to identify the personal information they intend to collect and consider:

- who to collect the personal information from and how to collect it
- what legislation authorises or requires to collect the personal information
- how to store the personal information, security precautions to ensure compliance with the privacy principles
- who has access to the data
- what they will use the personal information for

¹ *Putting the Privacy into Service Delivery Reform*, speech by Karen Curtis, Australian Privacy Commissioner, 2010.

- whether they will disclose the personal information and if so, to whom and for what purpose
- whether they will share the personal information with any other entities
- whether they will transfer the personal information outside Australia.

In addition to complying with the *Information Privacy Act 2009* (Qld) and the privacy principles, departments and statutory bodies must meet the requirements of the Queensland Government Enterprise Architecture. The Queensland Government Enterprise Architecture is the collection of ICT policies and associated documents that guides agency ICT initiatives and investments to improve the compatibility and cost-effectiveness of ICT across government. It supports the privacy principles and PIAs.

A critical part of the Queensland Government Enterprise Architecture is the Information Standards, including Information Standard 18 which sets out required data and system security obligations. The implementation guideline for Information Standard 18 (IS18) states:

Agencies should refer to IS18 for further information regarding the monitoring of communications including email and the Information Privacy Act 2009 for obligations regarding the protection of personal information.

Considering the privacy implications of an app is a good way to make sure it meets the privacy obligations. Agencies should review the PIA and privacy risk before deploying the app and at key stages of its life cycle, for example when updating the app.

We assessed whether the agencies adequately considered privacy principles when planning and developing the mobile apps. In particular, we examined whether they completed a PIA or equivalent.

Conclusion

The three agencies approached the development of their respective apps differently. DET adopted a privacy by design approach. The European Data Protection Supervisor defines privacy by design as:

'...building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.'

DET conducted a comprehensive PIA for QParents to assess possible privacy impacts, given the sensitivity of the personal information QParents collects and uses.

TMR did not conduct a PIA. This is because it determined that the MyTransLink mobile app would not collect personal information, unless a user elects to receive a response to their feedback.

Limiting the personal information collected is consistent with the privacy principles. While it is an effective way to manage an agency's privacy obligations, we strongly support performing, and documenting, a threshold privacy assessment.

The Policelink mobile app collects personal information. However QPS did not conduct a PIA before launching the app, even though its policies support the conduct of a PIA or equivalent. We observed a disconnect between policy and practice when QPS was developing the app. This is because the project governance was weak and the focus was on releasing the app.

The lack of PIA means, at the development stage, QPS was not able to identify and manage privacy risks related to the Policelink app, for example to make sure it uses or discloses personal information appropriately.

QPS cannot demonstrate how it ensured the app met the privacy principles, for example that there is a specific purpose for which it collects demographic information. An agency should not collect personal information just because it thinks the personal information may be useful at some time in the future. Users who are not confident that a government agency handles their personal information appropriately may lose trust in the agency and may be less likely to seek contact with the agency.

QPS completed a PIA in July 2017. It is a good first step to gradually incorporating privacy considerations into the existing mobile app.

A PIA is a living document, and it loses relevance when agencies do not keep it up to date. When agencies reassess the privacy impacts of the app, for example when they deploy app updates or release new features, they are better able to identify vulnerabilities and manage their privacy obligations.

[Detailed findings](#)

DET commissioned Crown Law to complete a thorough and extensive PIA before releasing QParents. The app collects, and gives access to, personal information such as reasons for a student's absence. The PIA identifies that the collection of personal information is for a purpose directly related to schools' functions and activities under the *Education (General Provisions) Act 2006* (Qld). This is consistent with Information Privacy Principle 1.

The PIA describes QParents, the information collected and the flow of information, and the privacy requirements for the app. It also describes and assesses the app's functions against

each privacy requirement. The PIA identifies privacy risks, their likelihood and impact and recommends actions the department should take to comply with the requirements, or prevent or mitigate privacy risks. Crown Law used the methodology described in our guideline.

However, the current version of QParents accesses personal information that the original PIA did not consider, for example, data about the device's location. The department plans to assess the privacy impacts of further app development, and will consider these permissions.

DET has strategies to identify and manage privacy impacts as part of continuous improvement:

- An information governance committee ensures mobile app development considers relevant legislation, the department's policy and strategic direction, and its strategic business and technical environment.
- A stakeholder reference group evaluates updates and discusses proposals.
- Up to date policies and procedures reflect the department's privacy obligations.
- Staff operating the app, including contractors, receive annual training covering privacy obligations.

TMR decided to minimise collecting personal information when developing MyTransLink, but did not document this decision. The app only collects a user's name and contact details when the user requests a response to their feedback. This approach is effective in minimising privacy risks and intrusion into the personal affairs of an individual. As a result, TMR felt it was not necessary to conduct a PIA but did not document its considerations.

During this review, TMR created a new position within TransLink to ensure project managers use the department's project management tools and templates, and document key facts. The department advises that it will conduct PIAs, information security classifications and other key governance initiatives as required for future major updates to the MyTransLink app.

When TMR collects personal information to respond to a customer's feedback, it stores it on the Customer Engagement Team's database, which is separate from the operating database for MyTransLink.

In its contracts with public transport service providers, TMR requires all parties involved to use and disclose the information appropriately. This includes when using personal information to respond to user feedback. The department has tailored privacy clauses in its contracts with service providers. It also notifies users in its privacy policy, accessible from within the app, that it might disclose information to contracted service providers.

When developing the Policelink mobile app, QPS did not complete a PIA or equivalent despite the app collecting personal information such as name, date of birth and gender. Depending on

the type of online report, the app also collects identification details, such as a driver's licence or passport number, and cultural details, such as whether or not a person identifies as Aboriginal or Torres Strait Islander.

QPS's policy position on privacy is positive, strong and firm. The policies and procedures about technology and privacy are detailed and rigorous, except for privacy complaints. We have not described the issues around privacy complaints as they are not the focus of this audit. It is clear that QPS expects its staff to follow the policies, including about privacy. The Operational Procedures Manual and Management Support Manual outline the privacy principles and describe how QPS staff must adopt the principles in daily operations.

The project documentation is limited. The information about the origin of the project mostly relies on the recollection of people involved at that time.

The project documentation does not explain how the app deals with personal information and privacy, for example:

- the reasons for collecting the personal information through the Policelink app
- the ways in which QPS will use or disclose this personal information
- the nature of any statistical or other reports generated from the personal information collected
- the notifications to the community about the personal information collected, stored, used and disclosed
- the impact of collecting personal information on a user's experience, particularly how it affects users' attitudes to reporting incidents.

We identified two factors contributing to QPS not applying the relevant privacy policies when developing the mobile app:

- unclear responsibility for project management oversight
- limited project scope.

It is not clear who was ultimately responsible for overseeing the project. This means that, at the design and development stage, QPS did not ensure that the app met the legislative requirements for privacy and/or its own policies about privacy.

The project acquittal dated October 2015 stands alone as formal, signed project documentation. While it shows the chain of responsibility for project reporting, it is incomplete. It does not provide evidence as to whether and how executive management was involved in planning, overseeing or evaluating the development of the mobile app. The acquittal contains inconsistencies and

some key sections are blank. For example, there is minimal information in the section on 'Alignment to agency/program strategies and objectives'. A final section on 'Project Closure Acceptance' is blank and unsigned.

In developing the Policelink mobile app, QPS acted on assumptions about the use or disclosure of information, for example:

- If police officers collected the information originally, they must use it for something, for example, 'investigative purposes'.
- If statistical information is collected, some part of government must have demanded the statistics.
- Someone must use the information collected through the website.
- It was not the project team's role to ask questions about the practices of another business unit within QPS.
- The existing online tools (for example links to privacy policies on the QPS website) covered policy requirements.

QPS has not documented these assumptions which the project team put forward during our interviews. The team believed that its job was to achieve functionality – quickly, responsively and within budget – which it did. This view was consistent with executive management recognition of these achievements.

During the review, QPS identified an executive manager responsible for the Policelink mobile app. QPS has shown commitment to addressing the privacy considerations for persons using the app. In July 2017, it completed a PIA for the app. The PIA touches on most of the elements in our guideline, except for identifying and consulting with stakeholders. We note that QPS is still finalising details that will inform the PIA, for example, how it will test the app for vulnerabilities.

This is a first step but QPS needs to do further work in the following areas:

- The map of personal information flow does not describe security classifications for information in accordance with the Queensland Government Enterprise Architecture.
- The PIA does not explain the audit checks QPS has undertaken or will undertake.
- There is little or no discussion on access rights and processes, disclosure of personal information to third parties, or the potential for transfer of information outside Australia.
- It does not map the flow of information through to a final conclusion.

- QPS cites section 29 of the *Information Privacy Act 2009* (Qld) as being a blanket exemption from five Information Privacy Principles. Section 29 states that a law enforcement agency is not subject to these principles if QPS is:

‘satisfied on reasonable grounds that noncompliance is necessary for activities related to the enforcement of laws.’

The PIA does not explain why noncompliance is necessary for all or any of the personal information collected through the Policelink mobile app.

- The PIA does not explain the technological and procedural security measures it is applying to protect personal information.
- QPS sets out a limited capacity to make privacy complaints about the app when the *Information Privacy Act 2009* (Qld) provides for a more comprehensive complaints process.
- The PIA does not adequately cover the privacy implications of using a contracted service provider.

QPS is continuing to develop the Policelink mobile app and releasing new features. Every time it changes the app, QPS will need to re-assess the privacy considerations and update the PIA accordingly.

Recommendations

We recommend that:

1. the Department of Education and Training updates its privacy impact assessment for QParents to address expanded permissions

2. the Queensland Police Service enhances its privacy impact assessment for the PoliceLink mobile app, and documents in detail how it will ensure the app meets the requirements of the *Information Privacy Act 2009* (Qld) and of the Queensland Government Enterprise Architecture

We also recommend that all agencies subject to the *Information Privacy Act 2009* (Qld):

- a. assess the privacy impacts of mobile apps at the development stage to identify, and plan how they will meet the requirements of the *Information Privacy Act 2009* (Qld)

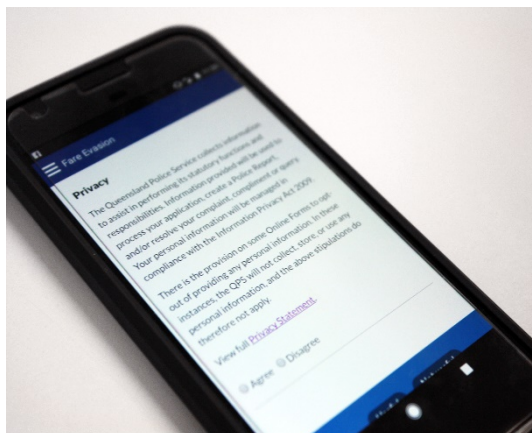
b. document how they consider privacy at key stages of developing and operating their mobile apps

c. reassess the privacy impacts regularly, for example when rolling out new features and updates, to identify vulnerabilities and manage their privacy obligations

4 Privacy when collecting personal information

Under the *Information Privacy Act 2009* (Qld), agencies collecting personal information must take all reasonable steps to make people generally aware of why they are collecting the information and how they will use it.

When an agency gives information to individuals so they understand about the personal information the agency collects, uses and usually discloses, we call this a collection notice.



Agencies should consider how to deliver the collection notice effectively and at the right time. Ideally, users will see the notice before they download the app, or before they start using it. Agencies should also explain why the app seeks permission to access specific features on the device, for example the camera, microphone or location tracker. Where possible, the app should allow users to opt out of the collection of their personal information.

It can be difficult to communicate this information effectively on a small screen. An agency should consider strategies for giving an effective notice, such as using short form notices where possible, putting important information up front with links to more detailed explanations, or using graphics, colour or sound to draw attention to notices.

We assessed whether the three agencies under review apply the privacy principles when collecting personal information through the mobile app. In particular, we examined whether each agency takes all reasonable steps to inform the user generally about the personal information it collects and uses.

Conclusion

The audited agencies inform the users about the personal information they collect through their respective mobile apps. There are links to privacy statements and other privacy information from the apps. This enables individuals to understand how the agencies will use and disclose the personal information they collect through the apps. There is, however, less information on why the apps are seeking permission to access specific features on the device.

DET has excellent privacy information tailored to QParents. Its policies are comprehensive and complete, except about the current permissions. TMR does not collect personal information for the operational functions of the app. Even so, TMR has includes links to privacy policies in its

MyTransLink mobile app. Originally, the privacy information associated with individual Policelink forms was overly generic. As we were finalising the audit, QPS rationalised the collection notices for 20 forms and upgraded a privacy statement. The forms' landing pages include an appropriate collection notice and a link to the service's privacy statement.

The three apps contain multiple links to privacy statements or terms and conditions. These links direct users to multiple sources for information on privacy, including information tailored to the specific app and generic information. This can be confusing at times.

DET, TMR and QPS do not explain to users the reasons why the mobile apps seek permission to access functions on the hand-held device.

[Detailed findings](#)

QParents users have opportunities to consent or withhold consent to DET collecting their personal information. The process of activating QParents goes through a layered and informed series of consents. First, the school must choose to offer QParents and decide what information from OneSchool the parents will be able to access. Then the school invites parents to use the portal. Finally, the parents decide whether or not to register for QParents.

However, there is no 'single point of truth' about privacy practices relevant to QParents. Depending on the starting point, the user can access up to six different sources of information. The QParents mobile app links to different privacy statements prior to download, during registration and from within the app. DET has advised that it will review the privacy statements for consistency.

Prior to download, both the Google Play Store and Apple iTunes Store have a link to the developer website, in this case DET. The Google Play link opens a QParents webpage on the department's website. The Apple link accesses the QParents portal. Both webpages outline the information collected through the app, the reasons for collection and to whom the information might be disclosed. Both provide a clear and detailed collection notice, whereas the whole-of-government privacy statement accessed from the privacy link on the webpage is more general.

Also before download, the Google Play store and Apple iTunes store have a privacy policy link, which opens the privacy statement accessible from the department's website footer. This is generic and not as useful as the QParents webpage.

The privacy statement provided on registration is specific to QParents. In addition to the statement, the terms and conditions explain the use of a student photo, authorisation of delegated viewers and the possibility of information going overseas. Together, the privacy statement and terms and conditions provide a very good collection notice for the personal

information the app collects. It would be improved by explaining the reason for each permission. The terms and conditions list the permissions required, but not the reasons for seeking these permissions. For example, they state that the Google Analytics cookies collect location information, but do not explain why the app needs to access location information.

The department publishes a QParents User Guide accessible from a QParents webpage. The guide informs users about updates to QParents. It states that a 2017 release is live, and the support information reflects the latest changes, including updates to the use, collection or security of information. For example, the 2017 release mentions options for parents to verify identity.

The department provides support to users of the OneSchool system; this includes responding to QParents users about service requests or faults. The department's internal policies do not explicitly refer to privacy or data breaches when considering escalating calls. The information to support staff dealing with questions about QParents does not cover privacy explicitly. For example, the guidance does not highlight the importance of identifying privacy issues and escalating a support call if it involves a possible privacy complaint or a privacy breach. DET advised it might be possible to include this in future versions of the guidance.

TMR does not collect personal information to operate the MyTransLink app. The app seeks permission for push notifications and geolocation data. The permissions are linked to a randomly generated user ID, which is not connected to any personal information. If a user does not give permission for push notifications or access to geolocation data, MyTransLink will work with limited functionality (for example, the app will not be able to alert a user on approach to a particular stop).

The app collects personal information only if:

- a user provides feedback on the operation of the app; and
- the user selects the option on the feedback screen to request a response (name, address, phone, and/or email).

Even so, the department provides information about its privacy practices, for example in the app's conditions of use. The app contains a link to TransLink's privacy policy on the entry screen, and on other screens throughout the app.

The MyTransLink app links to three sources of information about privacy, including privacy policies tailored to TransLink and generic information.

The 'MyTransLink app' webpage states

'MyTransLink doesn't collect or store any of your private information. The app will save your favourite services ('My services') and stops ('My stops')—it won't collect any other information about you or your phone.'

This statement is incomplete. It does not mention that the app collects contact information when the user requests a response to their inquiry or feedback.

At the bottom of the webpage there is a link to 'MyTransLink conditions of use'. The conditions of use mention the collection of contact details for surveys, and to improve the app and TransLink's services.

The global footer on the webpage links to a TransLink privacy statement. While the statement refers throughout to TMR, it is distinctly a TransLink statement. It differs from the department's 'Privacy and security statement' accessible from TMR's website. The two privacy statements align but are tailored to the different products and services. For example, the TransLink's statement excludes content about drivers' licences but includes information about go cards.

TransLink's 'Privacy' webpage does not explain how TMR informs users of any changes that affect collection, use or security of their personal information.

TMR's contact details for any questions about privacy and security practices are available on the website. The department could improve this information and explain how to provide feedback or make a privacy complaint.

QPS informs the users of its Policelink mobile app about the collection, use and disclosure of personal information.

During our review, we found two issues with the app's collection notices:

- At times, the app relied on generic information, which was insufficient because it was not specific enough for a person to understand the purpose of the collection.
- QPS provided multiple sources of privacy information which were not always accurate or consistent.

QPS addressed these issues as we were finalising the review. It changed online forms to reduce the collection of personal information and upgraded its privacy information. Now, when users access one of 20 forms through the app, they see a short collection notice on the landing page for the form. There is also a link to an updated privacy statement, that contains a newly tailored and comprehensive collection notice. Users must 'agree' to this privacy information, in nearly all cases, before they can complete the form. Additionally, seven forms are in a new format and QPS advised it will continue to upgrade the forms in this way.

QPS has not yet amended the notices within forms about specific collections or specific questions. The match of collection/permission to use is unclear for specific collections. For example, QPS does not explain how it will use information about a user's aboriginality when the user is reporting graffiti. Similarly, it is unclear how QPS will use access to recording audio through the microphone.

Originally, QPS directed users of the Policelink app to multiple generic information sources, which were inconsistent with each other. The privacy link within the app accessed multiple privacy statements depending on the form a user completed, for example reporting fare evasion or registering a party. The app relied on the whole-of-government privacy statement and the privacy statement available on QPS's website. These statements were generic, and not tailored to the mobile app context.

The Policelink mobile app seeks a wide range of permissions, including location information, access to contact lists, access to the device's audio, video or camera recordings and to USB storage of data.

The Android/Google Play app store requires that the description lists the permissions sought. The descriptions on the app stores are not consistent with other descriptions. For example, the description accessible from the device differs from the description on the app store's website.

Recommendations

We recommend that:

3. the Department of Education and Training, the Department of Transport and Main Roads, and the Queensland Police Service ensure the sources of information about privacy accessible from the app are consistent and complete to give users enough information about the agency's practices in handling personal information in the context of the app

4. the Department of Education and Training, the Department of Transport and Main Roads, and the Queensland Police Service explain to the users the reasons for the permissions to access a device's features

5. the Department of Transport and Main Roads includes information, on the TransLink website, about how to provide feedback or make a privacy complaint

6. the Queensland Police Service updates the collection notices within forms about specific collections or specific questions

We also recommend that all agencies subject to the *Information Privacy Act 2009* (Qld):

- d. give users a clear, specific, and complete collection notice, tailored to the mobile app

- e. outline the device's features the app requests access to and explain the reasons for seeking these permissions

5 Privacy when handling personal information

Cyber security is a critical risk to privacy and personal information. Under the privacy principles, an agency having control of a document containing personal information must ensure that the document is protected, for example, against loss or misuse.

The *Information Privacy Act 2009* (Qld) also describes requirements for the use, disclosure and handling of information, and transfer of personal information outside Australia.



Under Information Standard 18 about information security, departments and statutory bodies must implement information security to protect information assets, and any ICT assets which create, process, store, view or transmit information, against unauthorised use or accidental modification, loss or release. This includes developing, documenting, implementing, maintaining and reviewing appropriate security controls to protect the information agencies hold by:

- establishing appropriate information security policy, planning and governance within the agency in line with the standard, including adopting all specified frameworks, standards and reporting requirements
- implementing appropriate security controls, as detailed by the standard and its supporting documents.

Security testing before deploying a mobile app should be standard practice for all agencies. They should repeat the testing before rolling out an upgrade or new feature.

The *Information Privacy Act 2009* (Qld) requires agencies to take all reasonable steps to ensure contracted service providers comply with the privacy principles. For ICT contractors, the Queensland Government Information Technology Contracting Framework supports agencies to achieve legislative compliance. It provides a standard form of contract which includes as standard a clause binding contractors to the privacy principles.

In seeking to test cyber security for the mobile apps, we worked with the Queensland Government Chief Information Office to develop a questionnaire, based on the ISACA *Mobile Apps Audit Testing Framework*. We requested agencies self-assess their cyber-security for the mobile apps subject to this audit. As a result, we provide limited assurance only on the findings about the technical aspects.

We considered whether the three audited agencies are adequately managing the security, access and use of personal information collected through mobile apps.

We examined whether the agencies:

- test the security of the mobile app before deployment or updates
- ensure the personal information is stored securely, or if applicable, is transferred overseas appropriately
- ensure any external contracted service providers operate in accordance with the *Information Privacy Act 2009* (Qld).

Conclusion

DET and TMR have considered not only the technical aspects of data protection, but also the information governance, strategic information management and day-to-day operation of the QParents and MyTransLink mobile apps. As a result, they can demonstrate they adequately manage the security, access and use of personal information collected through the apps.

DET and TMR tested their mobile apps before deploying them. They have designed the apps to protect information during collection, transfer and storage.

Both departments have rigorous, ongoing testing regimes to identify vulnerabilities and to ensure cyber-security protections are in place. This includes identifying and mitigating the risks of the app being a means of accessing or penetrating wider departmental systems.

QPS did not test the Policelink mobile app before deploying it and has not set up a testing regime. Weak governance means that QPS operates the app in isolation from its strategic information governance and ICT management and policies. The app developers assumed that other business units within QPS were responsible for information governance. They focussed on the immediate task of achieving functionality.

As a result, QPS cannot demonstrate how it is managing the security, access and use of personal information collected through the Policelink app.

QPS is considering establishing a cycle of vulnerability assessments and penetration testing, but has not given details about the proposed testing cycle, what it will address or the timing of its implementation and frequency.

The three agencies advised that they do not transfer overseas the personal information they collect through the apps. They also use standard government contracts to engage ICT service providers to develop, update or operate the apps. The standard contracts bind the providers to the privacy principles.

DET has a detailed and comprehensive approach to cyber security for QParents, incorporating privacy by design principles, security controls, penetration testing, regular vulnerability testing, encryption of data in transit and at rest, and authentication practices. This approach governed the design of the app before the department deployed it, and continues to govern the operation and development of the app.

The department ensures the personal information it collects through QParents is stored securely. It has a strong governance framework with internal controls, including information management controls.

There is also an organisational structure with clear lines of responsibility and reporting for QParents. At the most senior level, the Innovation and Information Steering Committee is responsible for information management, supported by a suite of tools, including an enterprise assurance framework and risk management software.

Reporting to the Innovation and Information Steering Committee, the OneSchool Board has decision authority for QParents. The OneSchool Board includes the Assistant Director-General, Information and Technologies Branch, the Chief Information Officer, and the Executive Director, One School.

DET analysed the information environment and designed safeguards to protect the information it stores appropriately. For example, the department categorises student data as 'protected' and encrypts it during a connection between the user and the server, using SSL Certificates.

The mobile app requires proof of identity to register, and supports two-factor authentication while it is used. The registration process verifies each parent's identity, and ultimately provides a code or password for the parents to use. These steps are designed to prevent unauthorised access to personal information.

Three out of five of DET's contracted service providers are bound to the privacy principles in their contracts. Of the other two providers, one has passed a stringent independent privacy assessment and the other is not handling personal information and does not need to be contractually bound to the privacy principles. The department advised it does not transfer overseas the personal information collected through the QParents mobile app.

TMR tested the MyTransLink app before deployment. The department conducts regular data security testing. It uses external testing companies to verify that updates of, and changes to, the app work properly, and to check data security. TMR conducts vulnerability scanning on a monthly basis and penetration testing as needed to identify risks, including to the department's

information holdings. The department reviews the testing results for technical aspects of projects and addresses any risks.

The MyTransLink app does not collect or store personal information, other than to respond to feedback. If TMR decides to expand the app's scope so that it collects further personal information, this will be a trigger point for the department to reconsider the privacy implications.

TMR has built technical aspects of data protection into the operation of the MyTransLink app. The app randomly generates a unique User ID in a standalone TransLink database, and stores information about favourite stops or services with the User ID locally on the user's device. This is not personal information, as the app matches the user account number to the device, and not to the person or to personally identifying information.

TransLink has a good information governance framework, which it strengthened during our review. Originally, the Digital Solutions team within TransLink would prepare a briefing note on potential projects for endorsement by the Technology Change Management Committee, Customer Evolution Advisory Group and then for approval by the Customer Evolution Board. If approved, developers would prepare a project plan for approval, in most cases. TMR's sample project briefing mentioned risks and issues, and the *Information Privacy Act 2009* (Qld).

TransLink has since adopted a more formal and structured approach to project governance. It has created a project governance position within the Digital Solutions team, to ensure all ICT projects meet project management and information governance requirements.

In general, all TransLink's ICT contractors are accredited under the Government Information Technology Contracting Framework. The standard terms and conditions of the contract bind the contractors to the privacy principles.

TMR advised that it does not send TransLink customer information offshore.

QPS has not considered cyber-security aspects of the Policelink app before deploying it, or progressively as it released new functions, or in anticipation of new releases.

At the time of our audit, QPS has not conducted technical testing of the Policelink mobile app, penetration testing or vulnerability testing, with one exception. The Public Service Business Agency, which provides ICT support to QPS, was examining certificate issuance across a number of applications in early 2015, and came across a security issue with the Policelink mobile app. QPS fixed the problem within a week. It has not taken other testing action.

QPS has not advised how it is storing the personal information collected through the Policelink mobile app securely.

The app developer advised that the app does not transfer information overseas.

QPS used a whole-of-government procurement contract to engage the app developer. This contract binds the developer to the privacy principles.

Recommendations

We recommend that:

7. the Queensland Police Service sets up a regime of cyber security testing for the Policelink mobile app, including vulnerability assessments and penetration testing

We also recommend that all agencies subject to the *Information Privacy Act 2009* (Qld):

- f. ensure they protect the personal information collected through mobile apps against: loss; unauthorised access, use, modification or disclosure; and any other misuse. This includes testing each app for vulnerabilities before deploying it and at key stages of its life.

Appendices

Appendix A – Agency responses

Appendix B – Methodology

Appendix C – Commonly used acronyms

Appendix D – References

Appendix A – Agency responses



Office of the
Director-General

Department of
**Education and
Training**

10 AUG 2017

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
Email: sandra.heidrich@oic.qld.gov.au

Dear Ms Rangihaeata

Thank you for your letter dated 26 July 2017 regarding your recent audit into privacy and mobile apps across three Government agencies, including the Department of Education and Training's QParents app.

The Department accepts all three recommendations from the report and the proposed implementation actions are enclosed.

I was pleased to note the QParents app was considered by your office as a good example of the benefits of the privacy by design approach to app development.

Should your officers have any further questions, I invite them to contact Mr Michael O'Leary, Assistant Director-General, Information and Technologies Branch, on telephone 3034 4420 or by email at michael.oleary@det.qld.gov.au.

Thank you for the opportunity to respond to the report and its recommendations.

Yours sincerely

A blue ink signature of Dr Jim Watterston, written in a cursive style.

DR JIM WATTERSTON
Director-General

Ref: 17/400551

Enc

Level 37 1WS
1 William Street Brisbane
Queensland 4000 Australia
PO Box 15033 City East
Queensland 4002 Australia
Telephone +61 7 3034 4754
Facsimile +61 7 3034 4769
Website www.det.qld.gov.au
ABN 76 337 613 647

Privacy and Mobile Apps - Department of Education and Training, QParents

OIC recommends :-		Agency response and any proposed management action	Agency nominated owner	Agency nominated completion date
#	Recommendation			
1	DET updates its privacy impact assessment for QParents to address expanded permissions.	DET will update its privacy impact assessment for QParents to address expanded permissions.	Assistant Director-General, Information and Technologies	December 2017
3	DET ensures the sources of information about privacy accessible from the app are consistent and complete to give users enough information about the agency's practices in handling personal information in the context of the app.	DET will reduce the links to privacy within the QParents app to the single QParents Privacy information.	Assistant Director-General, Information and Technologies	December 2017
4	DET explains to the users the reasons for the permissions to access a device's features.	DET will update the privacy statement to explain to users reasons for permissions to access a device's features.	Assistant Director-General, Information and Technologies	December 2017



Office of the
Director-General

Department of
Transport and Main Roads

Our ref: DG34054

11 AUG 2017

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner Queensland
PO Box 10143
Adelaide Street
BRISBANE QLD 4000

Dear Ms Rangihaeata

Thank you for your letter of 26 July 2017 enclosing a copy of your proposed report to the Speaker of Parliament in relation to the Information Privacy and Mobile Apps Audit – My TransLink App.

Thank you for providing the Department of Transport and Main Roads (TMR) with an opportunity to respond to your proposed report and recommendations. I have enclosed a table with TMR's responses to the proposed report that is to be tabled in the Queensland Parliament.

I also thank you for offering to meet with TMR representatives to discuss the audit. TMR will contact your office in the coming days to organise this meeting.

In the meantime, if you require further information about this matter, I encourage you to contact Ms Anastasia Armstrong, Manager (Digital Solutions), TransLink Division, TMR, by email at anastasia.armstrong@translink.com.au or telephone on 3338 4271.

Yours sincerely

Neil Scales
Director-General
Department of Transport and Main Roads

Enc (1)

1 William Street, Brisbane
GPO Box 1549 Brisbane
Queensland 4001 Australia

Telephone +61 7 3066 7316
Facsimile +61 7 3066 7122
Website www.tmr.qld.gov.au
ABN 39 407 690 291

OIC recommends-		Agency response and any proposed management action	Agency nominated owner	Agency nominated completion date
#	Recommendation			
3	TMR ensures the sources of information about privacy accessible from the app are consistent and complete to give users enough information about the agency's practices in handling personal information in the context of the app	<p>TMR agrees with this recommendation.</p> <p>While the My TransLink app "windows in" or "iframes" the "feedback and enquiries" form on the webpage (see further clarification below), from an app user perspective it would be assumed that the app is collecting personal information as the form is accessible through the app. Given this, TMR accepts the OIC's comments on page 24 of the draft report that the statement on the 'My TransLink app' webpage is "incomplete". TMR has therefore amended the webpage to clarify personal information may be collected if an app user wishes to provide personal information when submitting feedback or enquiry. TMR also proposes to update the app conditions of use to clarify this.</p>	TransLink Digital Solutions and TMR Privacy Unit	31 August 2017
		TMR will review its privacy statements, links and website footers in relation to the app to ensure that all are consistent and complete.		
4	TMR explains to the users the reasons for the permissions to access a device's features	<p>TMR partially agrees with this recommendation.</p> <p>In section 4 of the draft report, the OIC recognises that TMR does not collect personal information to operate the MyTranslink app. However the app does seek permission for push notifications which is recognised by the OIC and is explained in the current conditions of use for the app. Permission to use push notifications for surveys is not included in the TransLink privacy webpage at https://translink.com.au/legal/privacy (the webpage) as those terms are web specific terms (much like there is no reference to cookies for example in the app conditions of use).</p> <p>The app "feedback and enquiries" form is "windowed in" to the app as it is captured as an "iframe" on the app however it is a form that is actually</p>	TransLink Digital Solutions and TMR Privacy Unit	31 August 2017

		located on the webpage. This would however not be known or visible to an app user. The form does not explain why a person's personal information is being collected however it does include a link to the privacy policy at https://translink.com.au/legal/privacy . The webpage will be amended and live by 31 August 2017 with a header to make the purposes of collection clear at the top of the form. Once the webpage is amended then this amendment will also appear through use of the form on the app.		
5	TMR includes information, on the TransLink website, about how to provide feedback or make a privacy complaint.	<p>TMR agrees with this recommendation.</p> <p>The TransLink privacy webpage at https://translink.com.au/legal/privacy (the webpage) has been updated with privacy complaints details.</p> <p>Translink general feedback and enquiries contact details were already included in the webpage and continue to apply for privacy feedback and enquiries. TransLink</p>	TransLink Digital Solutions and TMR Privacy Unit	Completed
		contact details apply to all TransLink enquiries and feedback. TransLink will continue to re-direct any privacy specific feedback and enquiries to the Privacy Contact Officer in the TMR Privacy Unit.		



QUEENSLAND POLICE SERVICE

COMMISSIONER'S OFFICE
200 ROMA STREET BRISBANE QLD 4000 AUSTRALIA
GPO BOX 1440 BRISBANE QLD 4001 AUSTRALIA

TELEPHONE 07 3364 6488 FACSIMILE 07 3364 4650



11 August 2017

Our Ref: 17/943008
Your Ref:

Rachael Rangihaeata
Information Commissioner
Level 8 160 Mary Street
Brisbane Qld 4000

Dear Ms Rachael Rangihaeata

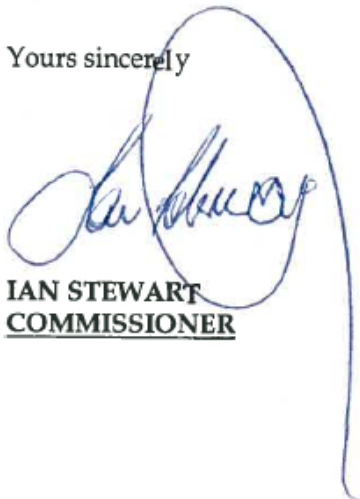
I refer to your letter of dated 26 July 2017 regarding the audit into privacy and mobile apps. Your correspondence was forwarded to the Community Contact Command to Inspector John Van Egmond whom has been providing assistance to your audit team during the audit review.

I can advise that the proposed report and recommendations have been reviewed and we have enclosed a copy of our responses to each of the tabled recommendations and the actions that we have undertaken.

There has been some considerable redesign of the Policelink app with a view to aligning the recommendations by your review team in order to comply to the provisions of the Information Privacy Act.

Should you require any further information please contact Inspector John Van Egmond on ph: 3015 6869 at Policelink or VanEgmond.JohnA@police.gov.au

Yours sincerely



IAN STEWART
COMMISSIONER

QUEENSLAND POLICE SERVICE

OIC recommends		Agency response and any proposed management action	Agency nominated owner	Agency nominated completion date
#	Recommendation			
2	QPS enhances its privacy impact assessment for the Policelink mobile app and documents in detail how it will ensure the app meets the requirements of the <i>Information Privacy Act 2009</i> (Qld) and of the Queensland Government Enterprise Architecture	<p>The QPS accepts that the project documentation is not adequate and recognises deficiencies in the management of the project to date. However, it does not accept the finding of poor project governance.</p> <p>The Policelink App was developed and released in October 2012 as a part of marketing campaign for the introduction of Policelink. Since the initial launch Policelink has moved further into the digital world, with online access and its release of the improved Policelink mobile application (app), launched in August 2014.</p> <p>The initial request was for the development of a suite of applications across key platforms: iPhone (iPad), Android, Blackberry and Windows 7 Mobile. The purpose of the application was simply to provide a conduit for the community tool using these platforms to easily contact Policelink through mobile devices.</p> <p>The app can be downloaded free, through the App Store (iTunes) for Apple devices and Google Play for Android devices.</p> <p>The App was not developed as a single project but evolved over time as new functions were added. The design of the app was based on industry practice for commercial apps, an approach also adopted for the QGOV Smart Service App.</p> <p>The comments in relation to the use of Privacy Impact Assessments are noted. The <i>Information Privacy Act 2009</i> does not mandate the use of PIAs but they can provide a useful risk management and planning tool. The QPS accepts that a Privacy Impact Assessment (PIA) was not completed at the commencement of the Policelink Mobile App deployment project. However, this is not unexpected as the App merely functioned as a public interface to a secure system (the Policelink system) and neither collected nor stored personal information but essentially operated as a gateway to the Policelink webpage. It is accepted, however, that a PIA may have been appropriate as additional functionalities such as hosted forms were added.</p> <p>In the case of the Policelink system itself, the planning for the Policelink system was undertaken prior to the commencement of the <i>Information Privacy Act 2009</i> so a PIA was not included as part of the planning process.</p>	Inspector John VAN EGMOND Policelink	December 2017

	<p>A preliminary PIA has now been completed which covers both the Mobile App and the Policelink System. The PIA is based on a methodology developed in consultation with the former Acting Privacy Commissioner. This methodology was used for the conduct of previous PIAs relating to the deployment of Automatic Number Plate Recognition and Point-to-Point Cameras. These PIAs involved extensive consultation with your office with no concerns of substance expressed. However, the QPS takes on board the issues raised in the Audit Report and will work with your office to address these issues.</p> <p>I note the comments in the report concerning the law enforcement exemption in section 29 of the <i>Information Privacy Act 2009</i>. The QPS has an extremely robust approach to the management of personal and confidential information. The QPS has extensive policies and procedures relating to the collection, security, use and disclosure of information. Under section 10.1 of the <i>Police Service Administration Act 1990</i>, the unauthorised disclosure of confidential information is a criminal offence. The QPS works closely with the Crime and Corruption Commission in dealing with officers who inappropriately access and/or disclose confidential information, and has commenced disciplinary and criminal prosecutions in respect of such access or disclosure.</p> <p>The technical approach of the audit team to the application of the exemption in section 29 raises concerns regarding the practical application of the exemption in a law enforcement and community safety environment. The <i>Information Privacy Act 2009</i> (Qld) is based on the <i>Privacy Act 1988 (Cth)</i> which itself derives from OECD Guidelines on the <i>Protection of Privacy and Transborder flows of Personal Data</i> issued in 1980.</p> <p>Privacy laws both nationally and locally recognise the unique functions and responsibilities of law enforcement and security agencies. Security agencies such as ASIO are simply exempt from the <i>Privacy Act 1988 (Cth)</i>. Law enforcement agencies are dealt with in a different manner through a distinction being drawn between administrative and operational functions. This is commonly done by providing a statutory exemption for operational activities to certain IPPs relating to collection, use and disclosure of personal information. Administrative functions remain the subject of the IPPs. In the case of the Queensland Police Service, the exemption is contained in section 29 of the <i>Information Privacy Act 2009</i>. It is accepted that the section is drafted in narrower terms than its interstate counterparts in that it is limited to enforcement functions. For example, the NSW Police Force has an exemption in respect of all operational functions, Victoria Police has an exemption in respect of both enforcement and community policing, Tasmania Police has an exemption for all of its operational functions and the Northern Territory Police have an exemption which</p>		
--	--	--	--

		<p>encompasses a broad range of operational functions. South Australia and Western Australia do not have privacy legislation and privacy is managed in accordance with administrative schemes. It is also accepted that the exemption is drafted in a technical manner as to require an officer to satisfy themselves that non-compliance with the IPPs is "necessary" before the exemption is engaged. This can create confusion as to what is permissible. For example, in <i>Marigliano v Queensland Police Service</i> [2016] QCAT 110, the Queensland Civil and Administrative Tribunal accepted that the use of Body Worn Video to record the service of a Notice of Appear on a person was lawful; indeed, from an accountability perspective it was desirable. However, an issue before QCAT was whether it was permissible under the <i>Information Privacy Act 2009</i> to film the person as they were being served with Notice. Ultimately, the Tribunal adopted a broad view of the section 29 exemption and found that the recording was lawful. The view of the Tribunal would appear inconsistent with the narrow approach suggested in the audit report. Confusion over how the exemption may apply in practice can affect the timeliness and scope of use and disclosure. Whilst a risk of uncertainty is the advertent breach of the <i>Information Privacy Act 2009</i>, a perhaps greater risk is that an officer may not do something or may delay doing something which they should for fear of breaching the Act.</p> <p>Recent events in responding to terrorism threats highlight the significance of being able to collect, use and disclose all available information, no matter how seemingly innocuous in its appearance, in a timely manner to ensure community safety. Public enquiries into matters such as domestic violence, child safety and responses to terrorism have consistently raised concerns with respect to information exchange and the siloing of information between agencies. The community would expect that if the QPS is in possession of information which is relevant to matters such as investigation, community safety and counter-terrorism, the QPS would appropriately use that information to fulfil its statutory functions regardless of the purpose for which the information was originally obtained. It would be contrary to community expectations that law enforcement agencies internally silo operational information on the basis that such information had originally been provided for another purpose.</p> <p>Under section 2.3 of the <i>Police Service Administration Act 1990</i>, the QPS is charged with significant responsibilities relating to law enforcement and community safety. Whilst the QPS has a strong privacy culture, it has always proceeded with its operational activities on the basis that it was not parliament's intention, when enacting the <i>Information Privacy Act 2009</i>, that the operational exemption in section 29 would be interpreted in such a way as to impact adversely on the ability of the QPS to carry out its statutory responsibilities to investigate crime and protect the community.</p>		
--	--	--	--	--

		It is appropriate, in an administrative context, to adopt a restrictive approach in relation to the collection, use and disclosure of personal information. However, viewing the operational functions of law enforcement agencies through an administrative prism is apt to create risks for such agencies in fulfilling their statutory responsibilities. The Federal Government, in collaboration with State and Territory governments is developing a holistic counter-terrorism framework. However, such a framework is only as strong as its weakest link. Where a law enforcement agency is given powers which parliament considers necessary to ensure community safety, there are real risks of those powers being frustrated by an unnecessarily restrictive interpretation of operational exemptions in privacy legislation. The concerns and challenges outlined in the current audit perhaps gives rise to a need to reconsider the application of the exemption in section 29 in the current law enforcement and security context.		
3	DET, TMR and QPS ensure the sources of information about privacy accessible from the app are consistent and complete to give users enough information about the agency's practices in handling personal information in the context of the app	The QPS accepts this recommendation. The Online Reporting Forms accessible through the application are housed on the website. They have the look and feel of the Whole of Government, and subsequently have the WOG footer, which links to a generic WOG privacy statement. This is a mandatory requirement. We have addressed this concern by adding the brief privacy/collection statement on each form on the website, so the user has to read it and then agree before accessing the form. On the website, accessed through the app, there is a web link to the privacy statement. Also, there is a 'view privacy statement' button which has been overlaid on the online reporting screen so it is available throughout the whole report, therefore reducing the instance of persons clicking on the WOG privacy link at the bottom of the page.	Inspector John VAN EGMOND Policelink	December 2017
4	DET, TMR and QPS explain to the users the reasons for the permissions to access a device's features	The QPS accepts this recommendation. The QPS has made amendments to the app so that the user will be prompted to grant access on downloading the app, these prompts will include specific information as to how permissions are used, differentiated by app native functionality.	Inspector John VAN EGMOND Policelink	December 2017
6	DET, TMR and QPS updates the collection notices within forms about specific collections or specific questions.	Information Privacy Principle 2 requires agencies, when requesting information from a person, to take reasonable steps to ensure that the person is generally aware as to the authority and purpose of collection, the intended uses of the information, and the entities to whom the information is routinely disclosed. The object of IPP 2 is to enable persons to make informed decisions as to whether or to not provide information. Whilst the audit report focuses on collection notices, IPP 2 does not mandate the use of collection notices as the only means by which information may be given in compliance with IPP 2. The focus on the content of collection notices, rather than the totality of information provided is inconsistent with the role and purpose of IPP 2 and the broad range of information delivery which may be used to comply with this principle. The App	Inspector John VAN EGMOND Policelink	December 2017

		<p>operates to direct users down particular paths before any personal information is sought. A user clicking on the "Report a Party" button could hardly be said be unaware of the general reasons for collection when they themselves have opted to take this path. Similarly, a user who clicks on the "Report Suspicious Activity" button and elects not to lodge an anonymous report could reasonably be expected to understand why information is being sought prior to the information being provided.</p> <p>In relation to the content of the notices, the previous comments relating to policing activities are also relevant. It may well be possible, in an administrative context which involves internal siloing of information, to identify and list with precision the particular derivative uses to which information may be put. However, in an operational law enforcement context, it is simply impossible to precisely identify the derivative uses to which information may be put.</p> <p>It is simply impossible to predict whether a piece of seemingly innocuous personal information provided, for example, in the reporting of a motor vehicle accident, will have significance in another law enforcement or community safety context. At the same time, the obligation imposed by IPP 2 is to sufficiently inform users of the purposes for which information may be used so that the users may make rational and informed decisions as to whether or not provide information. For the QPS, meeting its obligations under IPP2 requires that it not be artificially specific with respect to derivative uses of provided information.</p> <p>However, it is accepted that whilst the forms provide extensive information on the purpose for collection generally, the reasons for collection of specific information (e.g. ethnicity) may not be sufficiently articulated for users to make an informed decision as to whether to provide this information. The forms will be reviewed to address the issues raised in the audit.</p>		
7	QPS sets up a regime of cyber security testing for the Policelink mobile app, including vulnerability assessments and penetration testing	<p>The Queensland Police Service has an extremely robust information security framework which is designed to contain and protect extremely sensitive information. This framework has protected the QPS to date from the kinds of external attacks experienced by other government entities including the well-publicised hacking of the Department of Education and Training website in 2015 in which sensitive personal details of students were accessed. In preparation for the G20 summit in 2015, the QPS spent a significant part of its ICT budget in upgrading and testing its IT systems to counter the increased risks of cyber-attacks.</p> <p>Information security for the QPS is delivered by the Public Safety Business Agency (PSBA) Cyber Security Unit. The Cyber Security Unit is based in part on the former</p>	Inspector John VAN EGMOND Policelink	December 2017

		<p>Information Security Branch of the QPS which was transferred to PSBA as part of the consolidation of corporate functions for policing and emergency services. PSBA Cyber Security has been awarded the official ISO 27001 Information Security assurance by SAI Global Assurance Services in respect of restricted systems including QPRIME. ISO 27001 is the global standard for defining, operating and implementing an Information Security Management System (ISMS). ISMS uses a governance structure and controls guided by Government standards and frameworks. It is a combination of people, process and technology, and a system to secure critical (business) information assets against defined and unknown threats. PSBA was the first Queensland Government agency to receive this certification and level of information security assurance.</p> <p>While the QPS Security framework is based primarily on secure design and coding, the QPS recognises that a secure framework does not obviate the need for vulnerability assessment and penetration testing where warranted by the risk profile of the system. Mobile Apps that routinely undergo application vulnerability assessment are those to be delivered on corporate network connected devices, specifically the <u>QLite</u> device. This is because these Apps interact with heavily protected systems such as QPRIME. Testing requirements are assessed by the Mobile Capability Centre of QPS Community Contact Command. Mobile Apps which have been developed for public consumption are not normally the subject of vulnerability assessment because they do not have the same risk profile. Typically, such apps will not collect information but merely act as a public interface to systems which are themselves tested and secure. It is accepted that the QPS did not request PSBA Cyber Security to undertake vulnerability assessment and penetration testing of the PoliceLink mobile App on its deployment. The first few versions of the App contained only telephony and links to QPS web services, which later became QGOV forms. As the App did not itself collect or store personal information and operated only as a public interface, vulnerability assessment and penetration of the App was considered not necessary. As additional functions including hosted forms and image capture were added to the App, the risk profile changed. It is accepted that vulnerability assessment may have been appropriate as these additional functions were added. It is also accepted that PSBA Cyber Security identified a security vulnerability. This vulnerability was quickly addressed and no further issues were identified. Any potential security issues were also addressed as part of the general ICT security upgrade within the QPS in preparation for the G20 summit which did include penetration testing of the App. The Policelink Mobile App essentially functions as a public interface which plugs into a secure system. Whilst the audit did raise potential security issues, there is no evidence that the security of any personal information has been compromised.</p>		
--	--	--	--	--

		<p>However, the comments of the OIC audit are taken on board. In relation to the conduct of vulnerability assessment and penetration testing, these services are not part of the standard suite of services provided by PSBA Cyber Security but is delivered by external contractors on a user-pays basis where warranted by the risk profile of the system. In accordance with the recommendations of the OIC, the QPS has allocated funding and engaged with PSBA Cyber Security for the early conduct of vulnerability assessment and penetration testing of the Policelink Mobile App.</p> <p>More generally, in relation to the development of Apps designed for public consumption, procedures will be amended to require such Apps to be assessed by the QPS Mobile Capability Centre to determine the necessity of vulnerability assessment and penetration testing prior to referral to PSBA Cyber Security.</p>		
--	--	---	--	--

Appendix B – Methodology

We thank the staff of the audited agencies for their support and co-operation.

Audit objectives

The objectives of the audit were to assess whether agencies effectively applied the privacy principles when developing and operating mobile apps.

The audit examined whether agencies:

- adequately considered privacy principles when planning and developing mobile apps
- applied the privacy principles when collecting personal information through mobile apps; and
- adequately managed the security, access and use of personal information collected through mobile apps.

We conducted this audit as part of our privacy review function, as set out in section 135 of the *Information Privacy Act 2009* (Qld) (IP Act).

We selected the mobile apps for review based on a range of criteria, including:

- mobile apps for use by the public or general community
- number of downloads – high volume increases risk
- type of information collected – the sensitivity of the information increases impact of a privacy breach
- date of last update – an app that is not being maintained might be more vulnerable to attack
- permissions/access requested – the greater the access, the higher the risk
- privacy notice or statement – visible privacy awareness mitigates against there being risks.

The audit did not assess the platforms for app distribution, their operating systems, the security or privacy aspects of the app stores or any vulnerabilities of the devices themselves. Similarly, collection and security at the point of the platforms were not within scope.

The audit did not review the rationale for developing the mobile apps or their cost-benefit proposition.

Lines of inquiry

Sub objective	Line of inquiry
Agencies have adequately considered privacy principles when planning and developing the mobile app	The agency has completed a Privacy Impact Assessment (PIA) or equivalent <i>(Information Privacy Principle (IPP) 1)</i>
	The agency has tested the privacy aspects of the app before deploying it (including technical testing) <i>(Sections 27, 31 and 33-37 of the IP Act, Schedule 3 of the IPPs and Schedule 4 of the National Privacy Principles (NPPs))</i>
Agencies are applying the privacy principles when collecting personal information through the mobile apps	The agency takes all reasonable steps to inform the user about the personal information it will collect and use <i>(IPPs 1-3 and NPP 1)</i>
Agencies are adequately managing the security, access, and use of personal information collected through the mobile apps	The agency ensures the personal information is stored securely <i>(IPP 4 and NPP 4)</i> or if applicable, transferred overseas appropriately <i>(Section 33 of the IP Act)</i>
	The agency ensures the personal information is used and disclosed appropriately <i>(IPP 10 and 11, and NPP 2)</i>
	Any external contracted service providers operate in accordance with the <i>Information Privacy Act 2009</i> (Qld) <i>(Chapter 2, Part 4 of the IP Act)</i>

Appendix C – Commonly used terms and acronyms

Term/Acronym	Definition
DET	Department of Education and Training
ICT	Information and communication technology
IP Act	<i>Information Privacy Act 2009</i> (Qld)
IPP	Information privacy principle
IS18	Information Standard 18 – Information Security
ISACA framework	Mobile Apps Audit Testing Framework, developed by ISACA, an independent, non-profit, global association, engaging in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA was previously known as the Information Systems Audit and Control Association.
Mobile app	Mobile application: a mobile app is a software application developed specifically for use on small, wireless computing devices, such as smartphones and tablets, rather than desktop or laptop computers.
NPP	National privacy principle
PIA	Privacy Impact Assessment
QPS	Queensland Police Service
TMR	Department of Transport and Main Roads

Appendix D – References

- Apple Developer, *App Store Review Guidelines, 5.1.1 Data Collection and Storage*
- Australian Bureau of Statistics, *Queensland Police Records and Information Management Exchange (QPRIME)*, Queensland Police
- California Department of Justice, *Privacy on the go: Recommendations for the mobile ecosystem*, January 2013
- Deloitte, *Australian Privacy Index 2016: Trust without borders*
- Deloitte, *Gov on the Go: Boosting public sector productivity by going mobile*, William D. Eggers and Joshua Jaffe, 2013
- Department of Science, Information Technology and Innovation, *Government Information Technology Contracting Framework (v5.0.3)*, Queensland Government, December 2015
- Google Play, Developer Policy Center, *Privacy and Security*
- Karen Curtis, Australian Government Privacy Commissioner, *Putting the Privacy into Service Delivery Reform*, speech to Human Services Delivery and Payment Reform Summit, June 2010
- Mohammed J Khan, *Mobile App Security – Audit Framework*, ISACA (Information Systems Audit and Control Association) Journal, volume 4, 2016
- New Zealand Privacy Commissioner, *Need to know or nice to have: Making app privacy your competitive advantage*, 2014
- Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2017*
- Office of the Australian Information Commissioner, *Mobile privacy: A better practice guide for mobile app developers*, September 2014
- Office of the Information Commissioner Queensland, *Guideline Information Privacy Act 2009: Privacy and Mobile Apps*, February 2014
- Queensland Government Chief Information Office, *Information Standard 18: Information Security (v 5.0.1)*, November 2010
- Queensland Government Chief Information Office, *Information Standard 18: Information Security – Implementation Guideline (v1.0.2)*, July 2011
- Queensland Government Chief Information Office, *Network transmission security assurance framework (NTSAF) (v2.0.0)*, March 2016
- Queensland Government Chief Information Office, *Queensland Government Authentication Framework (v2.0.0)*, November 2010
- TechTarget, *Definition of Mobile App*, December 2013
- Teks Mobile Australia, *What Are The Mobile App Developers Doing In Australia?* November 2015
- United Kingdom Information Commissioner's Office, *Privacy in mobile apps: Guidance for app developers*, Information Commissioner's Office, United Kingdom, 2013

Appendix E – Overview of Privacy Impact Assessment (PIA) process

A PIA is a tool that agencies can use to assess the privacy impacts of a new project and where necessary, identify ways in which the obligations set out in the *Information Privacy Act 2009* (Qld) (IP Act) can be met.

The full process is outlined in OIC's **Guideline: Undertaking a Privacy Impact Assessment** (PIA Guideline), which is available on the OIC website: www.oic.qld.gov.au. While each project is different, a PIA should generally include the following steps:

1. Conduct a threshold assessment

Work out the extent to which the project will benefit from a PIA.

⑦ *Generally, if personal information is involved in the project, a PIA will be necessary. You can conduct a threshold assessment by completing the questions set out in Appendix A.*

2. Plan the PIA

Consider how detailed the PIA will be, who will conduct it, who needs to be consulted, when it needs to be delivered, and whether the PIA report will be published and if so, in what format.

3. Describe the project

Prepare a 'big picture' description of what the project will deliver and what it will achieve, why it is needed, timeframes, and any links to existing projects. This will provide context for the PIA process.

4. Identify and consult with stakeholders

Identify who has an interest in or is affected by the project, the level of consultation warranted by the project and how the consultation will be conducted.

Tip: Consultation may need to occur throughout the PIA process rather than at a single point.

5. Map the personal information flow

Describe how personal information will be collected, stored, used and disclosed in the project from beginning to end.

⑦ *Appendix B provides guidance on the level of detail required to sufficiently describe the personal information flow.*

6. Identify the privacy issues

Compare the project's personal information handling practices against the privacy obligations set out in the IP Act to identify any privacy issues.

⑦ *Appendices C and D provide a list of questions that you can use to work through each privacy principle and identify potential privacy issues.*

7. Identify options to address the privacy issues

Consider what options will address the privacy issues. If there are multiple options, evaluate the cost, risk and benefit of each option to identify the most appropriate option.

⑦ *Appendix E provides a list of common privacy issues and possible ways of addressing them.*

8. Prepare the PIA report

Provide a report that sets out the information gathered throughout the PIA and its findings to the relevant governance body for approval.

⑦ *Appendix F outlines suggested content for a PIA Report.*

9. Action the agency's response to the PIA Report

Incorporate the tasks necessary to action the agency's response to the PIA report into the wider project management process.

Tip: A PIA is a living document. It should be updated to assess that controls are current and working well.

For additional information and assistance 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.

First published 26 March 2016 and last updated 31 July 2017