PRIVACY BY DESIGN: DELIVERING GOVERNMENT SERVICES USING MOBILE APPLICATIONS

Gabrielle Hurley*

The Department of Human Services (DHS) has been developing its online service delivery capacities since 2007, and primarily focussed on Medicare, Centrelink and Child Support services' customers accessing online services from their home computers and laptops. However, in late 2012, the department commenced the roll out of its mobile applications program, Express Plus, which leverages the Department's online services capabilities. DHS has released Express Plus Apps for Jobseekers, Families Students and Seniors as well as an App for Medicare and a multilingual App. These mobile applications (Apps) have been designed for use on iPhones and android smart phones and are downloadable from the App Store and Google Play. In the future Express Plus App releases will further expand the reach of the Department's online services into the Australian community.

Utilising mobile apps to deliver online services that were originally designed for computers and laptops has raised and continues to raise design, implementation and post release issues for DHS, particularly from a privacy perspective. These issues include designing Apps that incorporate the features of smart devices without minimising privacy protections, designing compliant privacy notices and ensuring information security in the design and use of the Apps. It continues to be an interesting online journey, as it is the essential operating nature of the App downloaded onto a person's smart device that has raised unique privacy issues for the department when delivering government services.

Smartphones are quickly becoming the world's dominant computing device with more than one billion currently in use.[1] More specifically, in Australia between June 2011 and June 2012, there was a 104 per cent increase in the number of adults with a smartphone.[2] Comparatively from a global perspective according to research conducted in July 2012, Singapore at 92% was the country with the highest smart device penetration among adults aged 15 to 64 years old and Australia was the fourth at 79%.[3]

The attraction of a smart phone or smart device is that it is far more than just a phone. In addition to internet access, a smartphone can have the ability to synchronise with a computer, create documents and spread sheets, listen to music, manage social networks through various applications and take pictures.[4] The rapid increase in smart device ownership correlates with a rapid increase in the usage of Apps.

Apps are 'software applications often designed for a specific task and for a particular set of smart devices such as smartphones, tablet computers and internet connected televisions. They organise information in a way suitable for the specific characteristics of the device and they often closely interact with the hardware and operating system features present on the devices.'[5]

Apps are also market driven as they are developed and designed to provide a service, whether commercial or free, to the person wishing to download that App to his/her smart device. In 2012, the App marketplace was dominated by Apps that offered social networking,

---

* *Gabrielle Hurley is Deputy General Counsel, Department of Human Services. This paper was presented at the 2013 AIAL National Administrative Law Conference, Canberra, ACT,19 July 2013.*

games, photo taking and sharing, navigation and location tracking, and finance and banking.[6]

The rapid growth of Apps in the market place is evident from the statistics below:

- In the US it has been reported that 80% of consumers' time on mobile devices is spent in Apps and that every minute 47,000 Apps are downloaded by users worldwide.[7]
- In Australia, the number of adult smartphone users who download Apps increased from 2.41 million in June 2011 to 4.45 million in June 2012 – an increase of 85 per cent.[8]
- The average number of Apps downloaded between February 2013 and May 2013 by Australians who had ever downloaded an App, was eight free Apps and four paid Apps.[9]
- The App store for iPhones went live on 10 July 2008 with around 500 Apps available. In 2013 there are more than 850,000 Apps in the store with 50 billion downloads and $10bn having been paid to iOS developers to date.[10]

DHS Express Plus Apps

In mid-2011, legislation[11] was enacted that merged the former agencies of Medicare and Centrelink into DHS which already included the Child Support Agency, Australian Hearing and Commonwealth Rehabilitation Services within the Department. As a result the Australian government further developed its service delivery reform agenda as DHS became the primary means by which the government delivered services to the Australian community.

From 2007, Centrelink, Medicare and Child Support services developed and increased their online services presence. Online services focussed on customers using fixed computer terminals, the traditional means of online interaction at the time. The advantage of online services was that customers did not have to attend DHS offices, wait in queues for assistance or contact a call centre and wait on the phone for assistance.

In late 2012, DHS released the Express Plus Apps series that leverages the types of services already being delivered online by Centrelink to conduct business with its customers. The Express Plus App project has been a resounding success story for DHS with DHS being recognised by the Australian Government with the 2013 Overall Excellence in government Award and Service delivery Category award for the Express Plus App.[12]

From late 2012 to early 2013, DHS delivered the first series of Express Plus Apps, ie Express Plus Students, Express Plus Jobseekers, Express Plus Families and Express Plus Seniors. These Apps deliver services for Centrelink and are available for free download to iPhones and Android smart devices and are distributed by Apple in the App Store and by Google in Google Play.

Some of the services available to customers (who must already be registered with Centrelink online services) include reporting employment income and viewing future appointments, Centrelink income or payment statements and child care summaries. A customer can also access his/her current and past payments and ascertain if any money is owed to DHS.

Since the initial release of the Express Plus App series DHS has also released Express Plus Medicare and Express Plus Lite (multilingual) to the App store and to Google Play. Express Plus Medicare offers services to Medicare customers and Express Plus Lite enables customers to meet their Centrelink jobseeker reporting obligations using one of the four available languages, ie English, Vietnamese, Basic Chinese or Arabic.

In developing the Express Plus Apps series, DHS has embraced the Privacy by Design approach, recognised in 2010 as the global privacy standard. [13] Essentially the approach 'requires the application of privacy enhancing practices throughout the life cycle of the personal information that is its collection, storage, use, disclosure and destruction.'[14] Relying on this approach, privacy considerations have guided the design and implementation phases of the Apps, as they are used by DHS customers to interact with DHS services.

Privacy and the App eco system

Australian government agencies are regulated by the *Privacy Act 1988* (the *Privacy Act*) and by the Information Privacy Principles (IPPs)[15] which (amongst other things) articulate an agencies obligations with respect to the collection, storage (security), use and disclosure of personal information.

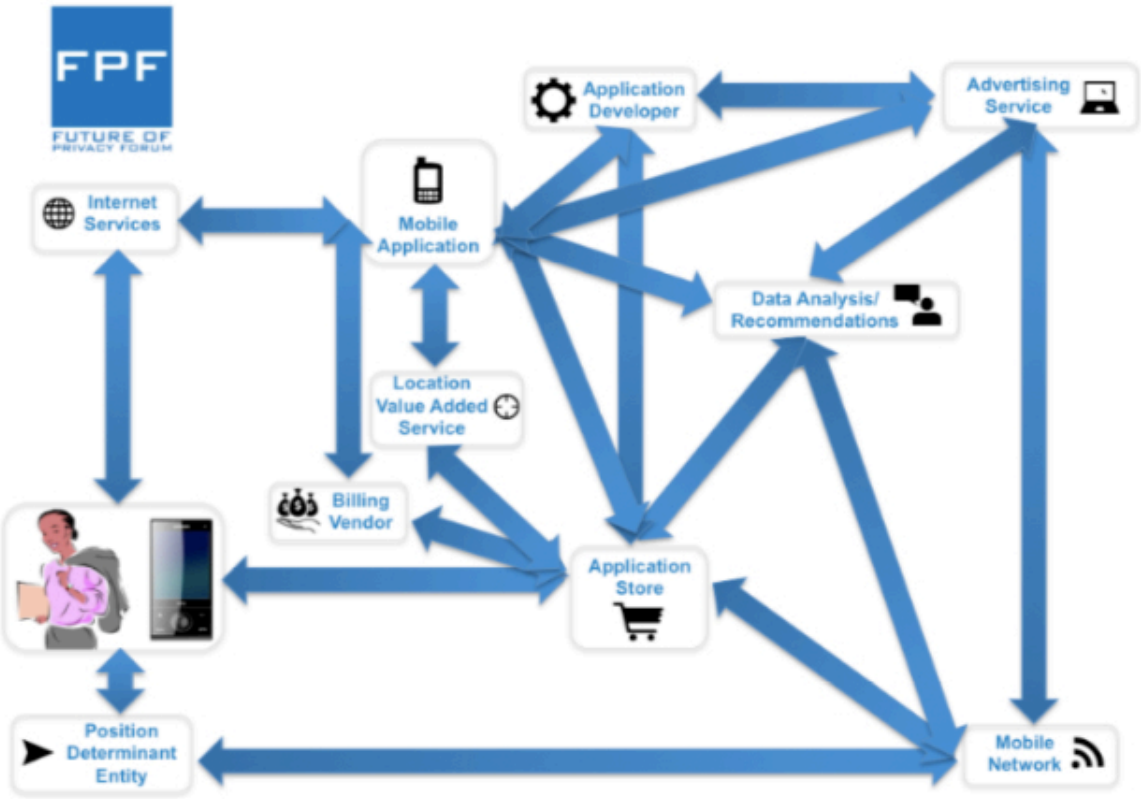
The Australian Privacy Principles (APPs) will commence on 12 March 2014 and will apply to government agencies and private entities covered by the *Privacy Act*. The APPs will specify additional privacy obligations for government agencies which are not covered by the current IPPs. To understand the proposed changes, the Office of the Australian Information Commissioner has issued a useful comparison guide that summarises and analyses these key changes.[16]

Section 6 of the *Privacy Act* defines personal information to mean:

> …information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The *Privacy Act* and the IPPs require an agency to have measures in place that protect a person's privacy ie personal information. To put measures in place it is necessary to identify when an agency is collecting, using or disclosing personal information and also to ensure that when personal information is being maintained it is kept secure. To undertake this exercise for Apps it is essential to understand the personal information flows and the entities involved, particularly as Apps and smart devices rely on both the internet and telecommunications systems.

Diagram: The App Eco System



The Future of Privacy Forum has produced a diagram (above) that depicts the App Eco System.[17] It provides a helicopter view of the potential entities involved and the flow of personal information or non-personal information to and from entities. It also illustrates the interrelationship of the telecommunication system and the internet.

The entities that may be involved at any one time as a result of a consumer downloading an App potentially include:

- internet providers;
- distributor/App stores –Google Play, App Store;
- billing vendors (paid App) – eg Paypal, credit card vendors;
- location value added service – GPS facility – eg Google maps;
- mobile App;
- App developers;
- advertising services;
- data analysis/recommendations eg Google analytics;
- mobile networks; and
- position determinant entities (PDEs) – which provide the precise location information of devices in an operator's CDMA network.

A diagram depicting the entities and personal information flows for the Express Plus App series would be less complex than the App Eco System diagram above. Express Plus Apps are available for free and have been designed to prevent third parties from accessing the information in the App. This means that the billing vendor, App store distributor, advertising services and data analysis/ recommendations entities would not be part of a personal information flow diagram for Express Plus Apps.

Designing privacy notices

In circumstances where agencies are collecting personal information from individuals, the *Privacy Act* requires agencies to take reasonable steps to make individuals aware (before information is collected or as soon as practicable afterwards) of the purpose for which the information is being collected, if the collection is authorised or required by law, and any person body or agency to which information of that kind is usually disclosed.[18] An agency's obligations are usually satisfied by giving the individual a privacy notice that outlines the required information.

The informational content requirements of a privacy notice and assurance that the notice is accessed, read and understood in the context of the design restraints of an App and a smart device can be quite challenging. Some of these challenges include:

- Apps are accessed using smart devices that have small screens (although tablets have more capacity) which limits the text space that is available before the consumer has to scroll down the page. Successful Apps do not require consumers to scroll though pages of text.
- Consumers can be highly motivated to install an App without having full regard to notices about the personal information that may be collected by the App developer or third parties.
- Consumers can suffer notice fatigue which results in a person ignoring notices or warnings that they see all the time.

For the purposes of the Express Plus App series and to minimise and overcome the App design challenges, DHS has put in place the following privacy design features:

- **Design one** - multi layered privacy notice approach - a short privacy notice is inserted in the terms and conditions which must be accepted by the customer before he/she can successfully download an Express Plus App. The short privacy notice includes a URL link to the long privacy notice which is on the DHS website.[19] After accessing the long privacy notice on the website, the customer can directly return to the terms and conditions in the App.

- **Design two** – a static privacy tab has been designed for the Express Plus App series and placed on the landing page of the App. Behind the privacy tab is the long privacy notice and when clicked the long notice can be read in its entirety. The privacy tab is always visible on the App and is available anytime that the customer wishes to review the long notice.

- **Design three** – the upload and capture function of the Express Plus App series uses the camera function of the smart device which enables the customer to take a photo of a document and to provide the photo to DHS using the App. For example; in Express Plus Families, a Proof of Birth claim can be made by taking a photo of the new born child's

Birth Certificate, uploading it to the claim in the App and submitting it to DHS for processing.

An additional privacy measure has been designed with this function. Before a customer uploads a photo of a document to the App using the smart device camera, a pop up screen appears and the customer is required to indicate that they have read and agree with the privacy notice in the tab. It is only after agreeing that the customer can successfully submit the claim and send the supporting photo to DHS.

Information security

Agencies have security obligations under the *Privacy Act* to take reasonable steps to keep personal information safe and secure from unauthorised access, modification or disclosure and also against misuse and loss.[20] The Office of the Australian Information Commissioner has recently issued a guide to information security that outlines some of the steps that entities covered by the *Privacy Act* can take to ensure that personal information is protected.[21]

DHS has put in place a series of security enhancing design features for the Express Plus Apps, which are summarised below:

- Any consumer can download the Express Plus App series onto his/her smart device. But, to use the App, the person needs to be a customer of DHS and registered for the relevant Online service, for example Centrelink Online Services or Medicare Online Services; this is a process that is undertaken directly with DHS prior to having an online account.
- To activate the App on the smart device and set up a PIN, a registered online user will need to do the following:
    (i) input their Customer Access number and password (created as part of the online services registration process)[22] and
    (ii) answer a secret question – set up as part of the online services registration process).
- Additional security measures in relation to a customer's PIN are:
    (i) three unsuccessful PIN attempts and the user is locked out of the App;
    (ii) the PIN must be changed every three months;
    (iii) because the App requires a smart device specific 4 digit PIN login, one device will support only one App download; if customers are sharing devices they cannot share the App.
- The Express Plus App series uses mobile portal technology to bring information to the smart device after the App is downloaded and successfully authenticated by the DHS customer. The technical state of the App at rest in the smart device is referred to as an 'empty container' – it is the mobile portal technology that reaches out from DHS services that gives the App life and this only occurs after successful authentication by the customer;
- Any technical information that is stored in the smart device for the purposes of the mobile portal technology requirements and activating the App has been encrypted by DHS. Therefore third parties (such as the entities identified in the App Eco System diagram) are unable to access technical information that is stored in the smart device after the App is installed and successfully authenticated by the customer.
- If a customer has lost his/her smart device, the customer can ask DHS to deactivate the device.

- In the future, new authentication processes will be implemented for current and future Express Plus Apps that will rely on the new myGov username and password process. myGov has replaced the Australia.gov portal link with respect to providing authenticated government services.[23]

Permission systems and privacy

Unlike Apple and the App store, Android does not review or restrict Android Apps that are distributed by Google Play. Instead Android 'uses permissions to alert users to privacy or security invasive applications.'[24] The specific permissions relevant to any App being distributed by Google Play are available to consumers in the store and are listed behind the permissions tab. The App developer relies on the consumer giving the developer access to certain features or information on their smart device in order to effectively operate the App, after it is downloaded by the consumer.

The Android permissions are broadly defined and rely on standardised descriptions available in the permissions tab. The developer does not have the capacity in the permission list in Google Play to change the description of the permission or to explain why it is required for the App to operate effectively. The following are extracts of Android permissions that are required for Express Plus App services to operate on the smart device:

- The Express Plus App offers a service that involves taking a photo of documents (upload and capture) using the smart device camera feature. The permission is described as follows:

  CAMERA
  TAKE PICTURES AND VIDEOS
  Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.

- The Express Plus App offers a location service for finding the closest DHS office using Google maps. The permission is described as follows:

  YOUR LOCATION
  APPROXIMATE LOCATION (NETWORK-BASED)
  Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.

  PRECISE LOCATION (GPS AND NETWORK-BASED)
  Allows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are, and may consume additional battery power.

- The Express Plus App offers a service that pushes Centrelink appointments to the smart device calendar. The permissions is described as follows:

  YOUR PERSONAL INFORMATION
  READ CALENDAR EVENTS PLUS CONFIDENTIAL INFORMATION
  Allows the app to read all calendar events stored on your device, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity.

ADD OR MODIFY CALENDAR EVENTS AND SEND EMAIL TO GUESTS WITHOUT OWNERS' KNOWLEDGE
Allows the app to add, remove, change events that you can modify on your device, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge.

Early in 2013, consumer reviews in Google Play (as opposed to the App store) relating to Express Plus Apps started to raise issues about the permissions that DHS was relying on to provide services in the Apps. The majority of issues raised were in the Express Plus Jobseeker App, however there were similar concerns being raised in consumer reviews for the Express Plus Students and Families App. These related to DHS as the App developer accessing the camera, GPS locator and phone facility on a customer's smart device.[25]

In response to these consumer reviews, DHS posted an explanation of the permissions being sought in the overview of each of the Apps in Google play and also in the Apple store and the DHS trouble shooting guide.[26] DHS explained that the permissions were required to allow the App to work effectively with the customer's device and assured customers that the information provided by the App was not used within the Department for any other purpose. In the explanation DHS highlighted that in order to provide the customers with particular functions in the App it would need to access the smart device capabilities.

The following information about the permissions was provided to consumers:

- Camera - the upload and capture facility required the customer to use the camera on the smart device therefore the App needed camera access.
- Access Personal Information - to add an appointment to the smart device calendar, personal information would be pushed from DHS using the App to the customer's calendar, however no information would be retrieved from the calendar as a result.
- Your location - for the office locator function the App needed permission to access the GPS facilities of the smart device, however this information when it is received by DHS would not be stored in its systems. On a practical note if the customer had turned off the GPS facility on their phone this function would not be available to the App anyway.
- Phone calls - if a customer needed to use the smart device call function while using the App, the App needed access to the phone call facilities of the smart device.

As a result of DHS's actions, the negative consumer reviews about privacy and permissions access slowed down considerably, however these issues continue to be raised with DHS as customers work to comprehend the permissions system used by Google Play.

Conclusion

From an App design perspective privacy issues need to be resolved and minimised within the context of the App Eco System as it relates to personal information data flows and potential connections to third party entities that support the system. With respect to Express Plus Apps, DHS has sought to design Apps that incorporate the special features of smart devices without minimising privacy protections, to provide compliant Privacy Notices and to ensure that reasonable steps have been taken to have in place a robust level of information security in the design and use of the Apps.

As an App developer and as the primary agency for delivering Australian government services, DHS continues to improve its App design to deliver more services using the current Express Plus Apps with a view to releasing new Apps in the future.

Endnotes

1 Business Insider – Australia (online), 'How price sensitive global consumers will shape the next smartphone growth wave', 2013. Accessed on 14 July 2013 and available at http://au.businessinsider.com/bii-report-how-price-sensitive-global-consumers-will-shape-the-next-smartphone-growth-wave-2013-3.
2 ACMA, 'Mobile apps emerging issues in media communications', Occasional Paper 1 May 2013 and statistics taken from ACMA, Smartphones and tablets; take up and use in Australia, ACMA Communications Report 2011-12 series, p 2.
3 Flurry Analytics, 'Active devices during July 2012 versus Adult population, 15 – 64 years old, per country'.
4 ACMA, Report 3 'The emerging mobile telecommunications service market in Australia', Communications Report, December 2011, 2010-11 series , p 3.
5 Article 29 Data Protection Working Party, *Opinion 02/2013*, On apps on smart devices, Article 29 of *Directive 95/94/EC*, p 4.
6 ACMA, 'Mobile Apps, Emerging issues in Media and Communications', Occasional Paper 1, May 2013 p 9.
7 ACMA,'Mobile Apps, Emerging issues in Media and Communications', Occasional Paper 1, May 2013, p 7.
8 ACMA, 'Smartphones and tablets; take up and use in Australia', Communications report 2011-12, series 2012 p 2 in ACMA, 'Mobile Apps Emerging issues in media communications', Occasional paper 1 May 2013 p 7.
9 Nielsen, 'Australian Connected Consumers Evolving Patterns of Media Consumption in the Digital Age', February 2013, p 63 In ACMA,' Mobile Apps, Emerging issues in Media and Communications', Occasional Paper 1, May 2013, p 7.
10 *Guardian Newspaper* online,' Apple's App store at 5; 10 key moments on the road to 50bn downloads,' accessed on 14 July 2013, available at http://www.guardian.co.uk/technology/appsblog/2013/jul/10/app-store-5-apple-ipad-iphone.
11 *Human Services (Centrelink) Act 1997* and *Human Services (Medicare) Act 1973* as amended by the *Human Services Legislation Amendment Act 2011.*
12 Australian Government ICT awards program, accessed on 14 July, available at http://agimo.gov.au/collaboration-services-skills/australian-government-ict-awards-program.
13 *Privacy by Design* is an approach that was developed by Dr Ann Cavoukian, Information and Privacy Commissioner, Ontario Canada in the 1990's. Further information about *Privacy by Design* is accessible at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf. The approach was recognised in October 2010 as the global privacy standard in a resolution by the *International Conference of Data Protection and Privacy Commissioners* in Jerusalem.
14 OAIC, 'Mobile privacy – A Better practice guide for mobile app developers – Consultation Draf, April 2013, p 2.
15 Section 14 of the *Privacy Act 1988* (Cth) sets out the eleven IPPs.
16 OAIC, 'Australian Privacy Principles and Information Privacy Principles – Comparison Guide', April 2013 available at http://www.oaic.gov.au/.
17 *The Future of Privacy Forum*, App Eco System, accessed on 14 July 2013, available at http://www.futureofprivacy.org/mobileapplicationdataflow/.
18 IPP2 of section 14 of the *Privacy Act 1988* (Cth) APP5 from 12 March 2014.
19 'Privacy Notice for Express Plus App series' accessed on 14 July 2013, available at http://www.humanservices.gov.au/customer/information/privacy-notice-for-express-plus-mobile-apps. From 12 March 2014, the short privacy notice in the terms and conditions and the long privacy notice behind the privacy tab will also link to the Privacy Policy, a requirement under the Australian Privacy Principles.
20 IPP 4 of section 14 of the *Privacy Act 1988* (Cth). APP11 from 12 March 2014
21 OAIC, 'Guide to Information Security', reasonable steps to protect personal information, April 2013, available at http://www.oaic.gov.au/.
22 *For Express Plus Medicare* the customer uses their myGov authentication to access the Medicare App.
23 myGov website available at https://my.gov.au/LoginServices/. The myGov authentication process is used in the Medicare App.
24 AP Felt et al, 'Android Permission: User Attention, Comprehension, and Behavior' University of California, Berkely. 2012, available at http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-26.pdf.
25 Google Play retains all consumer reviews for Apps that it distributes and the reviews mentioned in this article are available in *Google Play Express Plus Jobseeker*, *Student and Families* reviews.
26 DHS, 'Express Plus Mobile Apps trouble shooting guide', accessed on 14 July 2013, available at http://www.humanservices.gov.au/customer/enablers/express-plus/troubleshooting.