Mobile payments and the slippery slope of privacy loss…

July 2015

Speed read

In this fourth addition to our series about mobile payments, we consider privacy aspects, particularly as to the collection and use of personal information.

A major concern (and opportunity) in the mobile payments context is the accumulation and use of Big Data, the sharing of personal information between market participants, and the identification of specific consumer behaviours. Cybersecurity is also a big privacy issue too, which we have already covered in our last article.

Using cross-platform data (e.g. payments and loyalty data) enables a company to provide targeted services and marketing – and this is something that many consumers will value, at least regarding enhanced services (and even use of targeted ads if that leads to lower fees). However, this raises privacy issues that mobile payment participants will need to handle carefully.

Some consumers don't want this sharing and use of information. Increasingly, there will be competition for the consumer's wallet between providers that share and use personal information, and those that don't. A great example is the recent positioning of Apple (pro-privacy) relative to the likes of Facebook and Google (wide use of personal information).

If there are breaches, the Privacy Commissioner will take quicker action, and possibly even name and shame wayward companies under the Commissioner's new "name and shame" regime, which we describe in our article here.

In this article, we overview the applicability of the Privacy Act and related law, provide recommendations as to legal compliance, and explore why mobile payments have the potential to trigger a slippery slope of privacy loss…

The Detail

The story so far

This article follows on from our earlier ones:

- *How does Apple make money from Apple Pay?*
- *Introduction to NZ mobile payments regulation and law*
- *Cybersecurity risk and mobile payments*

And this article will be followed by:

- *Retailers pay banks more over payWave/PayPass than over EFTPOS*
- *Mobile payments and competition law*

The privacy issue

Mobile payment platforms (and those involved in them around the sides) gather highly personal information, including credit/debit card details, purchase details,

plus other private data that is routinely available on mobile devices, such as the user's location. Increasingly, there are also links to other data, often held by additional players, such as information collected for loyalty programmes, or networks and personal profiles associated with social media. A comprehensive profile is possible.

This, in itself, is not a new problem. For years, consumers have been storing private information on their smartphones and saving credit card data with online retailers. Besides, Apple, for example, insists that:[1]

> *"We are not in the business of collecting your data... Apple doesn't know what you bought, where you bought it, or how much you paid. The transaction is between you, the merchant, and the bank."*

This is partially true – in fact, some merchants are reportedly complaining that Apple Pay is too private, and that customers still need to waste time swiping their loyalty cards because payment terminals will not recognise their identify from Apple Pay alone.[2]

Apple does, however, record the exact time of your purchase, and the Apple Pay terms and conditions state that if location data is turned on, the location of payments are aggregated to improve Apple's wider services.[3]

Apple sets the battle lines

Apple's approach is a great example of the emerging fight for the hearts and wallets of consumers arising out of privacy. Some consumers do not want to be marketed to, or have their personal information widely shared. These consumers are a market in themselves and will pay more for this.

Recognising this, Apple's CEO Tim Cook launched a strong pro-privacy initiative at Apple in June 2015.[4] While he didn't name names, Apple are clearly trying to distinguish themselves from the likes of Facebook and Google, for which targeted advertising and use of personal information is at the heart of their business models. These revenue models are starkly different.

Android payment platforms will be quite different from Apple Pay platforms in this way. Google is currently being sued for sharing personal information from its Google Wallet product with a third party app developer.[5] However, this is not indicative of future strategy, and Google has since abandoned this practice.

Returning to Apple, CEO Tim Cook said:

> *"At Apple, your trust means everything to us. That's why we respect your privacy and protect it with strong encryption, plus strict policies that govern how all data is handled....*
>
> *A few years ago, users of Internet services began to realize that when an online service is free, you're not the customer. You're the product. But at Apple, we believe a great customer experience shouldn't come at the expense of your privacy.*
>
> *Our business model is very straightforward: We sell great products. We don't build a profile based on your email content or web browsing habits to sell to advertisers. We don't "monetize" the information you store on your iPhone or in iCloud. And we don't read your email or your messages to get information to market to you. Our software and services are designed to make our devices better. Plain and simple."*

With the opportunities to integrate programmes and services with the mobile payment platform, mobile payment participants also face similar choices. If the choice is to offer targeted services across multiple platforms, and targeted marketing too, greater privacy compliance care will be needed.

Mobile payments and the slippery slope of privacy loss...

Mobile payments are bringing together a range of previously disparate industries and entities (banks, telcos, IT, merchants, loyalty cards, marketers, etc.) into one medium. This convergence will create opportunities for unprecedentedly innovative commercial ventures and relationships, which in the context of Big Data, provides huge opportunities, but heightened privacy issues too.

The rise of Big Data

Big Data refers to the modern business practice of mixing, matching, and utilising vast quantities of data. While much of this data is initially 'anonymous', combining data from multiple sources, and then subjecting it to heavy analysis, permits very specific and very personal consumer behaviours to be identified, as we describe in *Big Data in business - father learns of teenage daughter's pregnancy from retail chain.*

In the case of mobile payments, banks, telcos, and others need to establish strong commercial partnerships, to offer a mobile payments service in the first instance. Working in unison, it is a logical next step to aggregate their respective data sources in to further the shared commercial venture, and better identify the needs of their consumers. Similar concerns are already being raised in related industries, as we noted in *The Internet of Things - ramping up privacy and security considerations.*

The temptation of convenience (it's a slippery slope)

Let's add another factor to the mix: loyalty programmes. They're a win-win-win for many (but not for others, as we note above) – consumers like being rewarded for frequenting their favourite stores, retailers receive repeat custom, and the loyalty programmes accumulate Big Data that can be sold or utilised. In many cases, as with Target, the retailer and the loyalty scheme are the same entity.

Some mobile wallets are already able to incorporate other aspects of your physical wallet, including loyalty cards and saving coupons. Consider the convenience of retailers, loyalty programmes, and mobile payment providers being able to work together. Your mobile could record everything you've ever purchased under your personal profile, making you eligible for enormous rewards over time.

What's more, all of the other features on your smartphone can be utilised too. You could opt for retailers to send you real-time updates (perhaps by video!) of exclusive deals, which could be purchased at the push of a button. Plus, if you share the link with your friend via the personal contact list on your smartphone, both your account and your friend's new account (which has just been added to the retailer's database) will be eligible for further savings.

On vacation? Fear not, your phone has automatically updated your favourite retailers – you're already eligible for special holiday discounts from the stores nearest your new location.

Pregnant? They know that, too.

As services go, it's innovative, it's convenient, and it's a potentially slippery slope. In time, this sharing of data on a grand scale could expose unwary corporates to large legal and reputational risks.

What does privacy law say about this?

The Privacy Act 1993 defines 'personal information' as any information about an identifiable individual (which is pretty much everything used for mobile payments).[6] The Act itself is built around twelve Information Privacy Principles, which uphold the right to access and correct personal information, prohibit keeping personal information for longer than necessary, and place limitations on the use and disclosure of personal information.

Broadly, collecting and using data for purposes beyond what the consumer clearly knows it will be used for, entails greater Privacy Act risk. Thus, undertaking marketing, using Big Data, and matching multiple databases etc, increases this risk.

One solution is to get the consumer's consent, but simply putting that consent deep into a privacy policy may not be enough. One problem in this area, as we explore in *Read a PhD thesis? Or online terms?*, is that very few people actually read online terms and policies, many of which are almost impenetrable anyway. A survey shows that only 1 or 2 out of a thousand actually open online terms before they click the accept button. This raises questions as to the validity and enforceability of the terms themselves.

In the end, it all depends on the circumstances.

Reputational risk has now substantially increased, as the Office of the Privacy Commissioner recently added a new string to its bow, as we explain in *Privacy Commissioner to 'Name And Shame' Wayward Corporates From December 2014.*

1. Eddy Cue, Apple senior vice president, keynote speech introducing Apple Pay (September 2014), transcript here: http://www.nfcworld.com/2014/09/09/331431/transcript-apple-ceo-tim-cook-svp-eddy-cue-introduce-apple-pay-mobile-payments-nfc/

2. Bloomberg Business "Apple Pay is Too Anonymous for Some Retailers" (2014) http://www.bloomberg.com/bw/articles/2014-10-20/apple-pay-is-too-anonymous-for-panera-starbucks-and-other-retailers

3. Apple iOS8.1 and supplemental Apple Pay terms: http://images.apple.com/legal/sla/docs/iOS81.pdf

4. See https://www.apple.com/privacy/

5. Reuters "Google fails to dismiss privacy lawsuit over Google Wallet" (April 2015) http://www.reuters.com/article/2015/04/02/us-google-wallet-lawsuit-idUSKBN0MT1RI20150402

6. Note that the Privacy Act, which deals only with information about individuals, is not the only source of privacy and confidentiality law. However, considering these issues in a Privacy Act context is a valuable framework.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com