Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

5 November 2017

Open Banking Review Secretariat
The Treasury
Langton Crescent
Parkes ACT 2600

By email: obr@treasury.gov.au

RE: Open Banking Review – Issues Paper

This submission from the Australian Privacy Foundation (The "APF") responds to the Issues Paper for the Open Banking Review.

The APF has had the opportunity to review the joint consumer submissions from Consumer Action Law Centre, Financial Rights Legal Centre and Financial Counselling Australia. We support those submissions.

General comments

Privacy is about the control of personal information. The APF strongly supports the rights of individuals to have effective control over their personal information. The APF also supports strong privacy laws which we contend need to be in place before any type of open banking is considered. Australia currently does not have strong privacy laws compared to a number of other countries.

Many individuals have a lack of trust about the control of their personal information. This has been evidenced in the last Census, MyHealth and Centrelink debt collection processes. Individuals do not understand how their information is being used, don't feel they have any control and consent to the uses of personal information is often bundled.

In the above context, the issues paper has given almost no consideration to the potential costs and harm to consumers of the proposed changes. Open banking poses considerable risks for people that have not been addressed and any benefits are likely to be outweighed by detriment.

Our submission specifically addresses our concerns below about potential risks and detriment for people.

Existing privacy laws

The existing privacy laws in Australia are inadequate compared to other countries[1]. The international comparisons in the issues paper specifically failed to consider the (better) privacy regulations generally in place with open banking. This is a major oversight.

The use and disclosure of personal information needs to be strongly regulated to ensure people are protected.

Three relevant examples of inadequacy in the current law that are relevant to open banking are:

1. Bundled consent. It is still standard practice in banking in Australia to bundle consent for the use of personal information. This is not meaningful consent.
2. It is still difficult to withdraw consent for the use and disclosure of personal information. This process is often buried in privacy consents.
3. There is evidence that even when consumers access information they do not get all relevant information. See the Grubb case where a dispute ensued following a request for personal information.[2] The technical definition of personal information is narrow.

The existing privacy laws are inadequate to protect people in an open banking regime in Australia.

Recommendation: The current privacy laws need to be reviewed and enhanced to meet best practice before the open banking regime can proceed.

Banking and confidentiality

Bankers and customers have a special relationship under the common law in Australia. Although the relationship is contractual, the courts over many years have implied additional duties into the contract. Bank's owe their customers a duty of confidentiality at common law.[3]

The duty of confidentiality requires that banks will keep their customers' personal and financial information secret. There are three exceptions:

1. Where disclosure is under compulsion of law
2. Where the interests of the bank require disclosure
3. Where the disclosure is made by the express or implied disclosure of the customer

It is also noted that the Code of Banking Practice expressly acknowledges this common law duty at clause 24.

Customers of banks have strong expectations of confidentiality that have been confirmed by the common law. Relying on the Privacy Act 1988 to determine how data sharing would work and what would constitute consent would be insufficient given the duty of confidentiality. It is arguable that consent to share data that would comply with the Privacy Act would be inadequate to meet the higher duty of confidentiality.

Recommendation: Any open banking regime would need to meet the duty of confidentiality owed by banks to its customers.

[1] For example the European Union privacy laws
[2] See Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC (19 January 2017)
[3] See Tournier v National Provincial and Union Bank of England [1924] 1 KB 461

Trust and banking

We would also note that there is considerable public lack of trust in banks. The Labor Party is calling for a Royal Commission into the banks. Although the Government does not agree with the need for a Royal Commission it is taking action on banking issues including regular open meetings with the CEOs of the major banks. We do not propose to comment on how that trust can be restored. However, we do want to comment about the risks of further erosion of any existing trust by the open banking regime.

Trust is an important part of banking. People need to trust that their financial information is secure. Any loss of data on a large scale or systemic mistakes in data sharing would erode trust.

A relevant overseas example is the Equifax data breach in the USA. Over 143 million social security numbers were compromised in the breach following the hack. It has been named as the worst data breach in US history.[4] This type of data breach would be equally catastrophic in banking. Security of data must be the highest priority.

Recommendations: People need confidence about security before any open banking regime is considered. An independent audit should be considered to ensure trust.

Access to personal information

Very few people know about their right to access personal information and even fewer access their personal information. According to the Australian Community Attitudes to Privacy Survey 2017[5] (**Privacy Survey)** only 37% of Australians know that they can request access to their personal information. Significantly, there is no reliable data available about rates of access to personal information.

It is significant that people rarely access their personal information. This issue has not been investigated. However, some of the problems seem to be that:

1. Access to personal information is difficult. It is hard to find who to ask and it takes time to get the information
2. It is unclear whether the person has been given all the information requested. The OAIC is under-resourced and compliance is uncertain.
3. The business can simply refuse to provide information requiring a complaint to the OAIC where the only adverse consequence for the business is being told to give the information

Any proposed open banking regime would need to address the above issues.

Consent

Meaningful consent is required for people to engage in any open banking regime. Bundled consent is commonly used in banking and has led to a situation where people do not read privacy consents at all. This is not meaningful consent.

[4] Many articles but for example see https://www.theverge.com/2017/9/22/16345580/equifax-data-breach-credit-identity-theft-updates

[5] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2017 available at https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017#s1-0-summary-of-results

It is worth noting there was and continue to be problems associated with transferring contracts without meaningful consent. An example, is energy companies where this was a serious and common problem[6]. Another example is also found in telecommunications. These problems caused considerable consumer harm including high costs, stress and inconvenience. This type of harm is unacceptable and there needs to be measures in place to prevent this. Meaningful consent is only the start of the measures required. Those measures will be need to form part of the design of the regime.

For consent to be meaningful the following would need to happen:

1. The consent must be separate
2. The disclosure must be consumer tested (including behavioural testing) to ensure it works
3. The disclosure needs to cover the nature of the consent, withdrawal of consent, possible risks including credit reporting consequences
4. People must be able to access external dispute resolution to resolve any breaches of confidentiality and privacy

Recommendation:

1. **Consent must be meaningful, not bundled, tested and include access to external dispute resolution to resolve any complaints.**
2. **Consumer protection measures need to be implemented to prevent people moving banking services without consent, for example, an ability to opt out of data transfer to third parties permanently**

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely

Kat Lane
For the Australian Privacy Foundation Board
0447 620 694
Kat.Lane@privacy.org.au

[6] For example, see http://www.smh.com.au/business/energy-retailer-fined-for-switching-customers-without-consent-20170123-gtxfgv.html