Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

18 January 2018

Manager
Consumer data Right Team
Structural Reform Group
The Treasury
Langton Crescent
Parkes ACT 2600

By email: data@treasury.gov.au

RE: Draft Privacy Impact Assessment – Consumer Data Right

This submission from the Australian Privacy Foundation (the "Foundation") responds to the Privacy Impact Assessment for the Consumer Data Right.

General comments

Both the process to develop this Privacy Impact Assessment ("PIA") and the draft PIA itself appear to be a failure. It fails all the people in Australia who will ever use 'open banking' by not providing a proper opportunity to identify the implications and risks associated with the proposal while there is still a chance to address them. In this context, the very recent announcement by the Government to delay the introduction of 'open banking' is welcome. We argue that even more time is required to rectify the failures in this process and the fundamental flaws in the current draft PIA.

The success of 'open banking' will depend heavily on gaining the trust and confidence of Australians in the system, and this in turn will only be well founded if such trust and confidence is based on a scheme that is trustworthy (worthy of trust). People need to be certain that the risks are well understood and acknowledged, and that their data will be collected minimally, stored securely (both against unintended re-identification and the inevitable hacking), used as requested, not exposed to coerced or widespread distribution, deleted on demand or as soon as practicable, and that the risks that will grow over time are not merely projected on defenceless data subjects but are pushed back on the proponents, so there are consequences (including fines and compensation, which the subject can take legal action to pursue) for misuse or foreseeable neglect.

The PIA is a fundamental part of the process to identify and address privacy and personal data security risks. A failed PIA process means that this trust and confidence is eroded, that the basis for any claim to be trustworthy is put in question.

The Foundation also contends that the Government's recent track record on privacy is also relevant to the PIA, and assessment of whether the proposed scheme is worthy of trust in the ways noted above.

The Government has consistently failed to address privacy concerns in relation to

- the Census (particularly the decision to retain identified records from 2016),
- telecommunications metadata retention,
- My Health Record (with its non-informed non-consent model and absence of individual access logging for the million or so users),
- the independence and continued existence of a statutory regulator focused on protecting privacy and data protection (with the title 'Privacy Commissioner' now a mere formality appended to the remnant Information Commissioner when convenient, despite the conflict between that commissioner's role in data exploitation and the privacy role of data protection) and
- Assistance and Access laws (popularly known as the 'war on encryption') to name a few.

The public's many concerns on these matters still remain mostly unresolved, and the continuing failure to put personal information security and privacy before expedience, political uses, 'disruption' or data exploitation adds to concerns about a looming failure of IT and data security in the face of ever more sophisticated attacks and ever more extensive breaches.

In this context, Treasury (the Government) chose to do an internal PIA, including key elements over the holiday period when no-one outside is available. That is, the best practice approach of using an expert independent external privacy firm to conduct an open, rigorous consultation process and draft the PIA was avoided in favour of a closed, in house formality. In the circumstances, this is a quite incomprehensible decision. It is arguably maladministration.

To illustrate how poor this decision is, it is worth reviewing recent history. The Australian Bureau of Statistics (ABS) similarly chose to do an internal PIA in November 2015 before the Census in 2016. That PIA overturned several key findings from a previous open, external PIA (namely, that keeping identified census records creates unacceptable privacy risks), it failed to expose the proposal to public or expert scrutiny or consultation, and also misused the summer holiday shutdown period to try to avoid public notice. The ensuing Census in 2016 was a disaster on privacy (among other things), and the century-long trust in the ABS, which was previously excellent, was undermined. We understand that the ABS is now arranging an independent external PIA for the next census, and appears more willing to engage in bona fide consultations.

Based on the Foundation's review of the PIA and the PIA process we contend that no one in Australia should have any trust and confidence in 'open banking' until the serious concerns outlined below are properly ventilated and fixed.

The regulatory context

Australia is introducing 'open banking' following the introduction of 'open banking' in the UK. Australia often follows UK innovations – sometimes with much success, but sometimes without the necessary critical distance needed to learn from problems and avoid repeating failures. However, in a privacy regulation context it should be noted that the UK has far better privacy protections for its citizens than Australia does. When the UK introduced 'open banking', it was in the context of a strong privacy regulation regime, with much more robust remedies for individuals to use to protect their rights and pursue abuses.

In Australia, 'open banking' is being introduced with weak existing privacy regulation, still no right for individuals to take legal action on their own behalf (despite five recommendations over three decades to address this international anomaly), and an inactive, underfunded regulator increasingly overwhelmed by an endless series of other responsibilities, with prospective privacy complainants forced to wait many months before a file can be opened.

The UK privacy regulatory environment is vastly superior for three main reasons:

1. UK has adopted and complies with the *General Data Protection Regulation* (GDPR);
2. UK has a *Human Rights Act*; and
3. UK has an adequately-funded, active privacy regulator

This is not a minor technical difference in regulatory context – it is a significant difference in privacy protections. For this reason, any comparison with the UK or using a similar approach to open banking is fundamentally flawed from a privacy perspective: if something goes wrong for the citizen in Australia, there is very little they can do compared to the robust options in the UK.

To put it bluntly, Australia does not have the privacy regulation foundation necessary to add extra features to facilitate the increased data flow of sensitive personal data, and that invite businesses to put pressure on individuals to submit to an expectation that they 'consent' to a potentially risky new model without any backstop.

As the 'open banking' PIA was done internally, there is a fundamental conflict of interest on the regulatory context that arises. The Government appears to want to put in 'open banking', based on a UK model, but does not want to give Australians the same privacy protections as apply in the UK. The apparently preferred answer is to ignore this major issue altogether, and to recommend cosmetic changes only. This conflict of interest (between an apparent financial industry and government preference to project risk onto the subject alone, and a public interest in the citizen having sufficiently strong, legally enforceable and robust rights to insist that those entities can be made responsible and liable when something goes wrong) is why it was completely inappropriate for Treasury to do an internal PIA for open banking, rather than an open, independent PIA.

Recommendations:

Australians deserve 'best practice' privacy protections and remedies. The following should be enacted as a prior foundation for any move towards 'open banking':

1. **Review and improvements to the *Privacy Act 1988* to be benchmarked to be as good or better than the GDPR**
2. **A *Human Rights Act* or similar to be introduced, including the legal right for an individual or group to sue for breach of their rights, including a breach of privacy or data protection**
3. **A well-funded, independent and active privacy regulator, with significant powers (in line with the ACCC and ASIC) to discipline the largest financial and global data businesses**

Consultation

The consultation process is a critical part of identifying privacy impacts with 'open banking'. The consultation process for the PIA has been an abject failure for a number of reasons, which need to be addressed.

The consultation on the PIA

Treasury first told consumer advocate stakeholders by email that a draft 'open banking' PIA had been prepared (by Treasury) on 12 November 2018. This was the first mention of a PIA in any context or consultation. At the time of the first email, the draft had already been prepared. **All** of the stakeholders objected to this flawed consultation process.

(A proper process would be for the PIA consultation to be well organised and occur in a way that flushes out the potential for unintended or unwanted consequences or risks to individuals (not only to business or government data users), so that these can be widely considered, potential mitigations can be flagged and their effectiveness can be subject to informed critical scrutiny during the PIA drafting process.)

Treasury then released the draft PIA for consultation on 21 December 2018 (days before the summer break when many offices and people cease routine operations), with submissions due on 18 January 2019 (with most of the time allowed for submissions to be developed and for submitters to consult colleagues, boards, members, experts or professional advice to overlap the period when most professional, government and civil society organisations were in recess and unavailable). Given that many people take leave at this time, a reasonable suspicion is raised that this may have been a deliberate attempt to ensure that few or no submissions were received, stakeholders had no chance to consult with others, and there was no reaction in the media or public sphere.

Given that a long delay in the introduction of 'open banking' was announced before Christmas, this short pre-Christmas consultation process appears to have been quite unnecessary and a potential abuse of procedural fairness.

The consultation process before the PIA

The PIA claims to have conducted extensive consultations on privacy throughout the open banking consultations. The Foundation has attended most of the consultations. As stated above, the PIA was not mentioned at any of those consultations. Privacy was mentioned at those consultations, but privacy was not the focus. The consultations were mainly led by the ACCC. The sort of issues and matters necessary for a PIA, and the existence of a PIA plan, were not addressed.

On pages 32 and 33 of the PIA, the OAIC *PIA Guidance* is quoted. The PIA then states that there has been extensive consultation "on privacy risks and concerns and strategies to mitigate them". This is where the privacy consultation has been so poor. A PIA is a rigorous process, and not simply a discussion of privacy risks.

Further and more importantly, when there is a consultation on a significant change like 'open banking', it is not possible to run a reasonable consultation process for a PIA ***without telling people that this is what you are doing*.** It is simply an unfair tactic to not tell stakeholders that all of those consultations on a wide range of issues was actually the PIA process. Worse, it undermines the effectiveness of the consultation. It also demonstrates why it is essential that a credible, open, independent PIA be conducted by an external entity with expertise and experience in effective PIA consultation and design.

Privacy by design

'Privacy by design' is a fundamental part of making sure that privacy is embedded into the process of designing 'open banking'. The PIA is a fundamental part of that design process. The OAIC PIA Guide states:

> *To be effective, a PIA should be an integral part of the project planning process, not an afterthought."* (page 3)

With 'open banking', this did not occur at all. A draft PIA was provided after many consultations. It was not included or mentioned in those many consultations. It literally was an afterthought. This means that this PIA is ineffective, and does not comply with the OAIC PIA Guidance. It should not be treated as the PIA for the proposed 'open banking' data and information scheme.

The OAIC PIA Guidance also states significantly:

> *Making a PIA an integral part of a project from the beginning means that you can identify any privacy risks early in the project and consider alternative, less privacy intrusive practices during development, instead of retrospectively."* (page 4)

That opportunity was critical, and it is a central part of what was missed. Discussing privacy as an agenda item in consultations on many other matters is no substitute for a rigorous, open PIA process, started at the beginning of the project and identified as such.

The importance of an external PIA for the 'Consumer Data Right'

This draft PIA was done internally by Treasury. The Foundation (or anyone else to the best of our knowledge) was not consulted about this decision. The PIA justifies that decision on several grounds, including building internal capability, and the iterative and lengthy nature of the consultative process. These justifications are not persuasive: 'building internal capability' to conduct a defective design process step is a wasted and ineffective effort; and the iterative nature of the consultation process should be embedded in a coherent, iterative, user- and risk-centred design methodology, not used as a justification for an incoherent, conflicted internal activity.

To the best of our knowledge, all consumer advocate stakeholders have criticised this decision, and not just "some".

The OAIC PIA Guidance states:

> *"Some projects will have substantially more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. The independent assessment may also help the organisation develop community trust in the PIA findings and the projects intent."* (page 10)

The Foundation agrees that for smaller and less significant projects, a full external PIA may not always be essential. However, 'open banking' is not a small project, it is a significant and important project requiring major changes with serious privacy risks.

More importantly, the success of the project depends heavily on public trust. If the public do not trust open banking (if they do not perceive that the proponents have demonstrated they are worthy of trust), they are much less likely to accept it, use it or endorse it.

In these circumstances, inward-looking arguments about 'building internal capability' are farcical when compared to the outward focus of building trust and doing a rigorous identification of privacy impacts. In our view, the OAIC *PIA Guidance* is clear that it would be preferable for an external PIA to be conducted. Treasury should have followed this Guidance.

The Foundation contends that the internal draft PIA must be abandoned, treated as 'disposable prototype' offering lessons for how a credible PIA needs to proceed, and an external, open independent PIA conducted. We have made repeated written representations to this effect to Treasury, and they have refused repeatedly.

An external independent PIA is essential because:

- Treasury does not have the expertise to do a PIA. The internal draft PIA produced misses major privacy risks (detailed below), and the consultation process for it was almost non-existent.

- There is no evidence of seeking guidance from experts, researchers, or professionals in the various disciplines and domains involved, and neither the Foundation nor any other privacy advocates were contacted to seek input on this point.

- Treasury has not complied with the OAIC *PIA Guidance*.

- Treasury has a conflict of interest. PIAs must be free of conflicts of interest. The aim is to flush out and resolve such conflicts and unintentional problems, not overlook them.

- 'Open banking' is a significant project with potentially diverse and serious privacy risks. The Government has repeatedly stated that open banking is a significant project. People need to be confident that all privacy impacts have been identified, and necessary changes or mitigations identified and made.

- Trust and confidence are essential. Trust is destroyed when Treasury produces a sub-standard PIA without proper consultation.

It remains unknown how such a poor decision (to do an internal PIA) was made, but that decision now needs to be fixed, as a matter of urgency. The pause announced recently enables this to occur with minimal disruption.

Recommendation

The Government arrange to appoint an independent external organisation with significant expertise in PIAs to conduct a PIA for the 'Consumer Data Right'.

Further action on 'open banking' must be delayed to enable a more rigorous, inclusive and coherent consultation process.

The role of the OAIC

Treasury has told the Foundation that the OAIC has been involved and provided advice in the preparation of the PIA. It is unclear why the OAIC has not raised any concerns about how the PIA has been conducted, and the lack of compliance with the OAIC *PIA Guidance*. The OAIC should be a strong, independent regulator, and if it is involved in providing advice, it should be transparent about the advice, and set high standards for PIAs rather than run the risk of being perceived to acquiesce in a weak and inward-looking exercise which failed to engage stakeholders or identify and ventilate key risks.

The PIA overall

The main purpose of the PIA appears to be an overview of open banking. Very little of the PIA is actually devoted to privacy impacts in any detail or substance. This is disappointing. It comprehensively shows the impact of a lack of specific consultation. It also completely disregards the nature of the significant risks in introducing this scheme into an environment without the robust protective environment of the UK, and any discussion about whether open banking should proceed at all in its current form in the absence of a similar level of protection for the interests of consumers and citizens. It is just assumed that it is proceeding. This failure to address the privacy and data issues in substance, to consider the implications of introducing only one part of a model without the protections relevant for those issues, and to consider the implications of a defective protective regime confirm it is incomplete and inadequate for the task.

Privacy safeguards

The privacy safeguards set out in the PIA for the CDR are largely just mirroring the principles-based law in the Australian Privacy Principles (APPs) from the *Privacy Act 1988*. The Foundation has serious concerns about the overall effectiveness of the APPs in their current form, which have accreted a raft of exceptions, loopholes, exemptions and other provisions which both complicate and compromise the protection of Australian's privacy expectations. Those same concerns apply to the privacy safeguards for 'open banking'.

The fundamental issue is that the OAIC is, after years of changes and attacks, a weak and overwhelmed regulator, and there are little or no consequences for data breaches or data misuse, and no realistic alternative for victims of breach or abuse (unlike the position in the UK). The law is also weak. Large penalties or compensation payments are not handed out regularly by the OAIC for data misuse. There is no active auditing mechanism, and the OAIC would likely not know about many systemic problems. 'Name and shame' is not used as the sort of effective regulatory option that is part of the routine arsenal in other areas, and the risk of reputation impact from such adverse action is not in evidence in most industries, especially powerful ones like banking, finance and data exploitation and commercial surveillance.

The recent Banking Royal Commission has shown that even with significant fines, misconduct can still be a systemic problem, and even robust, well-resourced regulators can struggle to rein in a culture of contempt and abuse of citizen interests. With 'open banking' the main data holders (at least initially) will be banks. The PIA has not considered (at all) the risks of the sort of serious and systemic misconduct that has been identified in the Banking Royal Commission, and whether it has any implications for open banking. This is a significant oversight.

It also has little to say about the sort of 'regulation-busting' or 'forgiveness not permission' attitudes in data start-ups or global commercial surveillance giants. These have not yet triggered a Royal Commission in Australia, but they have triggered serious inquiries and responses in the EU and US.

Potential privacy risks

The PIA does set out a list of potential privacy risks with severity ratings. There is no in-depth analysis on how the risk ratings were reached. The PIA seems to concede that they were not in a position to do a meaningful assessment of risk. This is a fundamental feature of the sort of risk investigation that should be at the heart of a PIA, especially one looking at serious and widespread changes in major industries that generate plenty of data and material to apply to such a task.

The Foundation will not be going through each risk in detail in this submission, as this is the task that should be undertaken in a proper independent rigorous external PIA.

The Foundation does, however, want to point out a major risk that remains unresolved or even considered in meaningful detail. The main function of 'open banking' is to facilitate the movement of information to third parties, which it is hoped will then lead to positive consumer outcomes from the use of that data.

In the case of the first phase of 'open banking' this means moving information from major banks at the direction of their customer. It is not mentioned in the PIA, but the banks actually have a higher duty to keep information confidential then other organisations in Australia. Banks have two duties:

1. To comply with legislation, for example, the *Privacy Act*; and
2. A duty of confidentiality at common law

This means that customers of banks have greater protections at law for their data then when dealing with a third party. Accordingly, it is a serious matter to move sensitive personal data to a third party where you have less protections at law: this runs the risk of laundering the data into an environment where the traditional common law protections do not apply, exposing the subject to reduced protection.

Further, the third parties that are anticipated to want the data are data aggregators and 'fin-techs'. These are comparatively small often 'start-up' companies with usually no proven track record in dispute resolution, corporate responsibility, ethical practice or even compliance with the law. Indeed, the culture is often proudly averse to compliance or seeking permission, preferring to 'see what you can get away with' (and begging forgiveness when caught) or to 'move fast and break things'. Putting this sort of highly opportunistic governance-hostile culture together with weak privacy laws and a weak privacy regulator, and there seems no doubt that there will be serious and significant problems with data breaches and misuse of data. It is inevitable.

People will be walking into a high-risk situation, assured by the Government it is safe when it won't be at all. This is a recipe for both major impacts on individuals, and major damage to trust and confidence when the reality hits home.

The reason the above risks are so predictable is simple: the data is more valuable than the risk of any negative repercussions. The Facebook/Cambridge Analytica scandal is an example of an

inevitable data breach/data misuse. We need to learn how to avoid setting up such conflicted, 'toxic by design' schemes.

The PIA fails to discuss in any detail the above type of risk. It does not evaluate or consider that the supposed benefit (for example, a cheaper loan) may not be not worth the harm of one's sensitive personal information being misused (which may have long term and widespread implications). There is a real question to be considered about whether open banking can be done safely, given this failure to appreciate the nature of the risk from the perspective of the vulnerable Australian citizen.

Genuine consent

The APPs have had principles in place about consent for many years, including the issues set out in the PIA. Despite this, genuine informed consent in relation to the use of data remains incredibly rare. Most people are confronted with a page of fine print for a privacy consent that they simply do not read, and which makes vague generalisations without revealing the nature of the risk or the entities who may be able to exploit or misuse the data.

It is very likely that this harm, this abuse of a formalistic consent model, will continue with 'open banking'. The proposed changes have not been tested as yet.

At a minimum, changes to consent need to be tested to check they are effective. 'Open banking' should not proceed with identifying the nature of dangerous or abusive consent models, and reforms which ensure genuine and effective consent. This is another reason to do a proper independent external PIA.

Data is only transferred to trusted recipients

This is such a fundamental issue that it must be enshrined in legislation, and not in the Rules. The requirements to meet standards, such as be a member of an EDR scheme, must be legislated in the proposed Bill.

It is likely that accreditation tiers will lead to further privacy risk, and all data recipients must meet the highest standards of risk mitigation, and acceptance of responsibility and liability for their part in any abuse or failure.

A real risk with any smaller data recipient is that they go out of business, and just sell or suddenly "lose" the data beforehand. People affected will suddenly have no access to justice. There is no compensation scheme in place to deal with this. This needs further thought to develop an effective remedy that survives the passing of a failed start-up which succumbed to the temptation to use its access to sensitive data to stay afloat.

Remedies

As stated above, the access to EDR must be enshrined in legislation.

The OAIC has a very poor dispute resolution process, where they simply decline to investigate a complaint. They have made very few determinations, ever, and it takes a very long time to get the rare one that is actually made. If the OAIC is to have powers to resolve CDR disputes this must be subject to changes in the Privacy Act to ensure:

1. The OAIC cannot simply decline to make a decision unless it is frivolous or vexatious
2. The complaint must be investigated
3. The time limit to make a complaint must be changed to 6 years (in keeping with other legislation) not 12 months
4. All decisions must be published
5. The enforcement of determinations against a hostile powerful entity must be strengthened and made automatic

A direct right of action enshrined in the Bill is essential, and is strongly supported. Without this, the Australian environment will remain an international disgrace, with individuals having neither constitutional, statutory or common law rights to protect their own privacy and data interests.

Prevention

Broad enforcement powers are not enough. This has become completely apparent in the Banking Royal Commission. It is necessary to have powers of audit and a process to check compliance. Prevention should be a key role of regulators because fixing up the harm is never adequate compensation. The real capacity for heavy penalties, litigation by individuals and groups, and potential reputation impact by 'name and shame' need to be seen as essential elements of the preventive context.

Deletion

There is currently no right in the Privacy Act to delete personal information. The CDR consultations have mentioned a right to delete. This is a key right. It needs to be enshrined in legislation. The best way to manage the risk of misuse of data is to ensure there is none. Not only should there be a specific right to delete but a number of scenarios should trigger an order to delete. Some examples would be misuse of data, insolvency to name a few.

A further issue is the increasing need to consider strategies of 'data minimisation' (rather than deletion) at all stages of the data lifecycle as necessary responses to the growing risk of data lakes turning into a 'toxic asset', as Bruce Schneier has observed. The assumptions embedded in 'open banking' that 'data is the new oil or the new gold' may need to be revisited in light of the continuing decline in the effectiveness of IT and data security. This is another issue that needs to be explored at the independent PIA.

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

Yours sincerely,

Kat Lane,
Vice-Chair
Australian Privacy Foundation