Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

20 November 2019

Office of the Australian Information Commissioner

By email: consultation@oaic.gov.au

RE: OAIC *Draft Privacy Safeguard Guidelines (Consumer Data Right)*

This submission from the Australian Privacy Foundation (the "Foundation") responds to the OAIC *Draft Privacy Safeguard Guidelines* (the "Guidelines").

General comments

The process to develop the Consumer Data Right (CDR) and pass it into law has been very poor from a privacy and data protection governance perspective. Treasury did not implement a 'privacy by design' approach, and only conducted a Privacy Impact Assessment (PIA) as an afterthought. This PIA by Treasury was done internally and not conducted independently, decreasing the likelihood of identifying flaws and risks for data subject which had been overlooked by agency insiders and lacking the credible oversight and transparency which a properly conducted PIA can offer. An independent and external PIA process was eventually commissioned, but this was so late that the CDR legislation had already passed into law, depriving legislators and citizens of the benefit of proper and timely expert scrutiny of the systemic privacy risks created by this CDR scheme. It is unclear what if any impact that second PIA will have if and when it is eventually published; from the process to date, it appears to have been done without any intention that it contribute

meaningfully to analysis, development and debate about the scheme while this could still be taken into account in the statutory process.

Unfortunately, this means that the Guidelines are being built on a CDR regime that has really failed to consider or incorporate best privacy practice. It also follows that this means that the privacy of individuals whose personal information will be dealt with under the CDR scheme is poorly protected. This poor protection is even greater when considering the weak privacy regulation in Australia. For example, the UK has 'open banking' (comparable in some respects to CDR). However, in a privacy regulation context the UK has far better privacy protections for its citizens than Australia does, so UK citizens have some prospect of redress for the potential flaws inherent in such CDR / 'open data' schemes. The UK privacy regulatory environment (in comparison to Australia) is vastly superior for three main reasons:

1. the UK has adopted and complies with the *General Data Protection Regulation* (GDPR), which has real teeth and viable remedies;
2. the UK has a *Human Rights Act,* which offers UK citizens effective litigation options if their rights and interests are hurt by poor laws or bad practices; and
3. the UK has an adequately funded, robust and active privacy regulator.

By contrast:

1. the Australian *Privacy Act* and our undeveloped common law offer no effective basis for an Australian citizen to directly enforce their privacy and data protection rights and interests if these are abused (despite five reviews over three decades consistently recommending legislative action to fix this fundamental deficiency);
2. there is no statutory equivalent of the *Human Rights Act*; and
3. years of persistent attacks compromising the regulatory structures we used to have leave Australians with no dedicated Privacy Commissioner, and a concerning lack of capacity in the surviving OAIC: a matter of under-funding, lack of expertise with consequent susceptibility to regulatory capture, conflicting goals, and an unduly inward-looking corporate culture that rarely applies the full force available to it.

This is not a slight cosmetic difference in regulation – it is a significant difference in privacy protections. The Guidelines carry a much higher burden than the equivalents in the UK, and need to be up to the task.

We acknowledge that in drafting these Guidelines the OAIC is working from existing very poor regulation. However, where possible the OAIC should act decisively to make sure these Guidelines are as aspirational and supportive as possible for strong privacy protections.

The role of the OAIC

The APF remains concerned that the OAIC is a very ineffective regulator and dispute resolution body. We do appreciate that some of these issues are related to being under-funded. For this reason, we repeatedly call for a substantial funding increase for the OAIC to match the ever-expanding obligations which it is called on to address, and the rapidly deteriorating personal information security and privacy threat environment created by ever-more aggressive schemes to exploit the personal information of Australians.

However, the comparative and absolute ineffectiveness of the OAIC is becoming starker in the light of recent activity by the ACCC on enforcement related to privacy issues. Two big cases which involved serious privacy concerns, *Equifax*[1] and *Health Engine,*[2] were run by the ACCC (under the *Australian Consumer Law*) and not the OAIC (under the *Privacy Act*). The OAIC has no outstanding enforcement action we are aware of, and their investigation of the Facebook/Cambridge Analytica scandal has taken over 18 months while overseas jurisdictions have already enforced fines.[3]

A regulator (even an under-funded regulator) must be active and assertive in enforcement because otherwise its inactivity sends a clear message to business and agencies that compliance with the law is, in effect, not compulsory and there are few or no consequences for non-compliance. Far from being beneficial, seeing others get away with bad corporate behaviour or unwarranted exploitation of sensitive personal information has a potential corrosive effect on the willingness of responsible entities to identify and actively comply with their own data protection obligations. The APF contends that the OAIC has been sending this message (that there are no enforcement consequences for abusers, and no alternative options for victims) for much of the time since the *Privacy Act* was enacted.

[1] https://www.accc.gov.au/media-release/equifax-formerly-veda-to-pay-35-million-in-penalties
[2] https://www.accc.gov.au/media-release/healthengine-in-court-for-allegedly-misusing-patient-data-and-manipulating-reviews
[3] https://www.theguardian.com/australia-news/2019/oct/19/australian-privacy-watchdog-fails-to-deliver-findings-on-cambridge-analytica-scandal-after-18-months

The OAIC must become a strong regulator and in particular, a strong enforcer of the CDR and the Guidelines. We note that the Financial Services Royal Commission was highly critical of the lack of enforcement action by Australian Securities and Investments Commission (ASIC). This criticism would also apply to the OAIC in its role as regulator in privacy if there was ever any review. The vulnerabilities created by the CDR scheme make such a review more likely unless there is strong enforcement and regulatory action.

As a dispute resolution body which is at present the primary option for Australians seeking to enforce their privacy rights, in our view the OAIC must:

- Investigate complaints and make determinations
- Publish those decisions
- Cease relying on section 41 to close complaints
- Develop guidance on how compensation should be routinely awarded in proven CDR complaints, at a level that makes non-compliance commercially unattractive

By failing to investigate and decide complaints, the OAIC fails not just those who would make complaints but everyone, because there is no developed set of precedents and no sense of predictable outcome.

Even though EDR is available for CDR complaints, there are issues with EDR where non-financial loss is limited to $5,000. There will be complaints that should be dealt with by the OAIC. The OAIC needs to make sure that privacy breaches are properly compensated.

The drafting of the Guidelines

The Guidelines are very long and confusing. We acknowledge that the legislation and rules themselves are also confusing and long, a governance failing which afflicts many aspects of privacy law in this country. We remain concerned that compliance with the CDR laws, rules and Guidelines is likely to be poor and inconsistent because they are difficult to understand and follow. Dividing the Guidelines into parts that mirror the rules does not really fix this problem.

The APF recommends that the Guidelines be independently tested and evaluated with those who will need to use them to assess whether they are readable, comprehensible and can be easily understood by these users. It may be necessary to change the parts completely or

rewrite them substantially to improve the likelihood that the requirements in the Guidelines can be easily understood -- both by those whose information is covered and those working with this information -- and they will be incorporated into compliance and good practice.

APP 12 – Access to Personal Information

There has been a concentration on the CDR and how that will "provide greater choice and control over how their data is used and disclosed." The CDR is essentially a personal information "data portability" right. That is, a mechanism for how Australians can transfer their personal data from one entity in the financial sector to a third party to provide a service.

Australian Privacy Principle 12 (APP 12) is the provision in the existing privacy law which already creates a right of access to your own personal information. This right applies widely, and goes well beyond the CDR. It is a fundamental privacy right to be able access your own personal information.

Our experience is that APP 12 works very poorly. There is no guarantee that you can access your information for free, so some businesses charge costs to make it difficult or impractical to access your personal information. Then there are the businesses that will not respond to requests, or that provide incomplete or low integrity information. Even more alarming, it seems that currently you cannot access your own CDR personal information (as the laws are currently drafted).

The OAIC needs to do substantial work to ensure that APP 12 actually works, in general and in the context of the CDR. People should not have to go to a third-party broker to get their own information. However, as it currently stands it appears that the OAIC will be encouraging this type of brokerage (an artificial market, based on a failure to recognise and enforce existing privacy law rights) just so people can get their own information. The APF remains concerned that dodgy third parties will mislead people into believing that they have to go to a third party to get their own information when this is not true.

The OAIC must:

- Review the operation of APP 12
- Work towards making access free of charge, either with mandatory industry agreement or by legislative change

- Consult on changes to improve the operation of APP 12
- Identify adequate and mandatory standards of responsiveness and data integrity (completeness, currency, relevance, accuracy) in the provision of your data
- Introduce automatic fines and compensation for poor compliance

Consent

Consent has been a very poor way to protect the privacy of people. People sign forms all the time that they do not read. People quite rightly surmise that the fine print is not negotiable, and it is often not comprehensible. So, when people sign a lengthy, obscurely worded consent, they often have little idea what they have agreed to (and are now bound by). The situation is even worse for vulnerable people who can simply not have the bandwidth or literacy to understand what is happening in that moment.

There is a well developed jurisprudence in the consumer credit, finance and banking sectors that identifies potential abuses of the consent process in the underlying transactions, establishes models for detecting when these occur, and provides various legal and practical remedies to mitigate their worst effects. In our view the flaws of the consent process for dealings with personal information in these sectors should be addressed by building on this existing body of consumer friendly law.

Testing

We maintain that for consent to be effective there must be independent consumer testing on what works and what does not work to communicate and inform the reader about the key implications and choices they face. The result of this evaluation must then be incorporated into this Guideline. There is no evidence that this has occurred.

Form of the consent

There is no guidance at all on how the consent should be presented. For example, disclosure in personal credit requires:

- A minimum font size
- The use of Schumer boxes
- The use of bold and warnings

The OAIC has the opportunity to give detailed guidance on what best practice consent should look like. The OAIC should definitely be providing suggestions (and these things should have been in the rules) on exactly how to explain set out the consent information to maximise understanding of the key implications and choices.

Not simply relying on consent

ASIC recently released a report on *Disclosure: Why it shouldn't be the default.*[4] The consent being obtained is really just a disclosure which the person agrees to. This report is centrally relevant to the Guidelines here because the first roll out of the CDR is in 'open banking'. The report makes several observations about disclosure including:

- the importance of context,
- complexity,
- one size does not fit all,
- problems with warnings,
- how disclosure can backfire, and
- difficulties with consumer attention.

This means that other tools beyond consent are necessary to maximise the effectiveness of disclosure. This means that the Guidelines should do more, including making it clear to industry:

- that they cannot rely on more technical or formalistic compliance,
- that product design is important and should include behavioural insights,
- that helpful behavioural insights should be considered, including examples of ways to 'nudge' people to carefully consider the consent (and to avoid 'nudging' them to act against interest), and
- the importance of timing when delivering the consent.

The OAIC should also:

- Conduct or coordinate the comprehension and readability research (suggested above) as a basis for work on consent,
- Work with industry to improve product design,
- Audit and identify problems with how the consent is delivered, and

[4] See <https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-632-disclosure-why-it-shouldn-t-be-the-default/>.

- The ability to take swift, public and strong action against businesses that act exploitatively in their use of a consent model.

Deletion or Erasure of data

There is currently no right in the *Privacy Act* to delete personal information. The CDR consultations have frequently mentioned a right to delete. Unfortunately, this right became an option at the discretion of the accredited data recipient, rather than a right of the affected individual. This is a very poor outcome for the privacy rights of individuals, a backward step which is out of sync with the emerging global consensus that there is a place for certain forms of a right to delete.

De-identification has been proposed as an alternative to deletion, but it does not work to address the need. We have explained in prior submissions in relation to 'open data' models like CDR that the combination of big data advanced analytic tools (including machine learning, neural networks and AI) and the proliferation of matchable data sets from many sources together now mean it is effectively certain that any given de-identification method or practice will eventually succumb to ever-more-sophisticated re-identification techniques. There is a well developed literature confirming this emerging weakness. Re-identification is in the category of "when, not if".

The problems with de-identification include the following:

1. The business that has de-identified can re-identify. In other words, the compliance of the business is a risk in itself.
2. De-identification has proved to offer little impediment for hackers or even university researchers to prove that it does not work.[5]
3. De-identification cannot be 'future-proofed'. It gets easier over time to re-identify de-identified information.[6]
4. Re-identification may become viable, or be actually carried out, in a way that is undetectable for the data subject: at any time into the future, in a variety of locations and jurisdictions such as cloud and outsourced services, and involving a variety of contexts or actors. In all but trivial cases (like open demonstrations done on the

[5] For example, *Stop the Open Data Bus, We Want to Get* Off*,* Culnane, Rubinstein and Teague August 2019. Available at <https://arxiv.org/abs/1908.05004>.
[6] See the work of MA Rizoiu et al of NICTA, such as at <http://www.tiberiocaetano.com/papers/2016/RizXieCaeCeb16.pdf>.

Medicare 10% sample data set in 2016 by researchers) the subject is unlikely to be told, or to be able to find out, when a technique or their data set has been cracked.

5. The creation of this intrinsic mass risk has -- as a result of an inadequate regulatory response -- *not* been accompanied by an obligation on those circulating or releasing a data set which was ostensibly de-identified with a certain technique to conduct a long term global audit and research program to detect when re-identification against that given de-identification technique has become viable, or when that particular data set has actually been re-identified.
6. The risk consequent on re-identification is thus not mitigated, and any harm is projected onto the data subject alone, who is typically not well placed to understand, track or identify it.
7. The notion of a 're-identification offence' as a solution to this risk is quite impractical.

People in the UK and Europe have a right to delete under the GDPR. Australians do not. This means we are all exposed to the risk of a data breach and exposure of re-identified personal information. It is an unacceptable risk.

The CDR and Privacy Safeguard 12 of the Guidelines is looming as a complete failure, and it is likely that it simply will not adequately protect Australians' personal financial information. It will also make a mockery of privacy in Australia and this CDR as people **do not have control of their personal information if they cannot require its deletion**.

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

Yours sincerely

Kat Lane,
Vice-Chair
0447 620 694
kat.lane@privacy.org.au