Priva
Founda

http://www.privacy.org.au

Secretary@privacy.org.au

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

Deborah Anton
Interim National Data Commissioner
Department of Prime Minister and Cabinet
One National Circuit
BARTON ACT 2600

**DATA SHARING AND RELEASE - LEGISLATIVE REFORMS AND DISCUSSION PAPER**

This submission from the Australian Privacy Foundation (APF) responds to the Discussion Paper on Data Sharing and Release. The APF does not support the proposed Data Sharing and Release proposal as it represents an unacceptable risk for no demonstrated benefits.

## General comments

The APF continues to express serious concerns about the proposed data sharing and release when Australia has weak privacy protections in place. Data sharing or any similar process must have a foundation of strong privacy laws. Any attempt to build any data sharing process without strong privacy protections will lead to the harm of individuals and a further erosion of trust in the Government.

The ACCC has recently released a final paper in the Digital Platforms Inquiry[1] that has recommended reforms of the privacy laws in Australia to deal with the impact of digital platforms. The APF would contend that those reforms are necessary before any consideration of legislation for data sharing and release.

[1] Available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

The APF would go further and state that the following reforms are essential before proceeding with data sharing and release legislation:

1. The privacy laws in Australia are benchmarked to meet similar standards to the General Data Protection Regulation (GDPR)
2. A Human Rights Act is enacted which covers basic human rights including privacy
3. The Office of the Australian Information Commissioner (OAIC) receives adequate funding and resources to ensure it is an adequate regulator
4. There is a tort for the right of action for a breach of privacy
5. There is a free and independent dispute resolution process available (funded by the Government) to seek and receive compensation for data breaches

**Recommendations**

The privacy laws in Australia need to be of an adequate standard before any data sharing and release legislation can proceed.

## Benefits to the public?

The APF is not convinced there is any benefit for the public in data sharing and release. In fact, we remain highly concerned about harm to individuals from data sharing and release. No independent evidence has been provided detailing how the public will benefit. Even if the public did in theory receive a benefit - is that benefit outweighed by the costs and risks? No detailed analysis has been attempted or offered.

It is however easy to discern why the Government is very determined to implement this proposed reform. It would enable the Government to better track its citizens to discover possible criminal activity and to raise revenue. The recent experience with robodebt and Centrelink is a case study on how data sharing can harm people. Robodebt occurred when the Australian Tax Office data was auto matched against Centrelink data. The data matching resulted in mass mail outs to Centrelink recipients. Several problems have become evident from robodebt:

1. Receiving debt notices and queries from Centrelink is highly stressful for people. It is a harm in itself to suddenly insist there is a debt or discrepancy.

2. Many people have successfully challenged the debts claimed which indicates large problems with accuracy.
3. Two Legal Aid Victoria cases were dropped when Centrelink admitted in both cases that the debt claimed was not owed.

Centrelink continues to defend its actions on the basis that it is legislatively required to recoup debts (although it is unclear how an alleged debt is an actual debt). However, this response misses the fundamental point which is that consent, accuracy and a fair process are essential to maintain trust or comply with best practice privacy. The robodebt data sharing was done without consent, the data was not accurate (as yearly data was matched against fortnightly data) and the process was not fair. If robodebt is an indication of how data sharing will work, this is a strong reason why it should not proceed as it will definitely harm people.

## The Data Commissioner

The APF does not support having a separate role for a Data Commissioner. This is yet further unnecessary complexity when the sharing and release of data should be regulated by an adequately resourced OAIC.

As it is, there is now an absurd situation (although the APF is grateful that a regulator is doing this work) where the ACCC is now taking a leadership role on privacy issues. This has included two serious cases of privacy breaches[2] that the ACCC is enforcing under the Australian Consumer Law. There is also wide ranging and important analysis of privacy issues in the *Digital Platforms Inquiry* and the review of *Customer Loyalty Schemes*.

The situation with privacy is incredibly confusing for any person trying to work out which regulator to complain to in Australia. The addition of a data commissioner adds to this confusion.

**Recommendation**

The role of the data commissioner should be rolled into the OAIC. The OAIC should be adequately resourced to be a strong and effective regulator.

[2] See information on two separate cases: ACCC v Equifax at https://www.accc.gov.au/media-release/equifax-formerly-veda-to-pay-35-million-in-penalties. And ACCC v. Health Engine at https://www.accc.gov.au/media-release/healthengine-in-court-for-allegedly-misusing-patient-data-and-manipulating-reviews

## Privacy Impact Assessment

The APF does support the recommendations in the Privacy Impact Assessment (PIA) but notes that these recommendations are not sufficient to safeguard privacy. As we have outlined above, Australia needs strong privacy laws, human rights laws, a strong regulator, free dispute resolution and a tort for invasion of privacy as minimum safeguards. These issues were outside the scope of the PIA but they are still essential.

## Trust/Social licence

The Australian Government has a very poor track record on privacy protection. Australia is internationally renowned for privacy abusive legislation such as the metadata retention[3] and the anti-encryption laws[4]. In this context it is very difficult (and we would argue impossible) to build trust with Australians.

It is necessary to repeal the privacy abusive laws to rebuild trust with people. There is no indication of this happening. In those circumstances, we would predict that distrust will continue to grow and the introduction of data sharing will cause further problems.

## Consent

People must consent to data sharing and release of personal information. The PIA specifically mentions that this should occur. It is unclear why this was not a recommendation in the PIA.

Privacy is about the control of personal information. To have control of your own personal information consent must be a vital and necessary part of the process. If there is no meaningful consent there is no control of your personal information.

The conclusion in the Discussion Paper that requiring consent will lead to biased data is a clear indication of a Government centred approach rather than an approach focused on the individual and the control of their own personal information. This is a serious problem. It

[3] *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015
[4] Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018

clearly shows that data sharing and release is all about the Government and not the people. It is worth reminding the Government that you govern for the people not for bureaucracy.

**Recommendation**

Consent is a necessary part of privacy. Consent must be required for all data sharing and release.

## Deletion and De-identification

The APF has been involved in the consultations on the Consumer Data Right. At the beginning of the process we were promised a right to delete personal information. That right would have been consistent with best practice privacy safeguards in the GDPR. The right to delete was watered down to a choice by the business on whether to de-identify or delete. This is an awful result for people who may want to use the Consumer Data Right. It leaves them exposed to data breaches.

Deletion is the only way to be sure that data cannot be re-identified or misused in future. De-identification does not work. It is in the category of "when not if" for re-identification. There are several obvious problems with de-identification:

1. De-identified information can re-identified by the Government department. In other words, the compliance of the Government with its own rules is a risk in itself.
2. De-identification has proved to be little trouble for hackers or even university researchers to prove that it does not work.[5]
3. It cannot be future proofed. It gets easier over time to re-identify de-identified information.

**Recommendation**

De-identification cannot be relied on to protect personal information. People must have a right to delete personal information whenever possible.

[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.

## Remedies

There needs to be real and serious consequences for non-compliance with the Data Sharing and Release laws.

There must be legal liability for releases of data that harm individuals. This is required to ensure there is trust in the system. Liability must flow from harm. If it is not set up in this way then there is insufficient incentive to ensure compliance. There must also be significant fines for data breaches.

People must have access to a free and independent dispute resolution process that must make a determination and has the power to award significant compensation. If the OAIC is used for this purpose then it must:

1. Have an adequate time limit to make complaints of 6 years;
2. Make determinations when a complaint is made (not simply cease to investigate)
3. Have the power and award compensation for harm and provide guidelines on this issue
4. Have sufficient power to compel the Government to provide any required information to investigate the complaint

We also refer to the Australian Law Reform Commission Report[6] which recommended enacting legislation to deal with serious invasions of privacy. Those recommendations have not been actioned. However, now that there is a proposal for data sharing it is now essential that those recommendations are enacted to provide a clear remedy for individuals affected by serious invasions of privacy.

**Recommendations:**

**- There must be legal liability for data breaches. Individuals should be able to seek compensation for harm.**
**- Fines for data breaches**

[6] https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

**- Provide a free and rigorous dispute resolution process with the ability to award significant compensation**
**- The ALRC Report recommendations in relation to serious invasions of privacy should be enacted urgently to give individuals access to justice in the event of harm from data releases.**

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

Yours sincerely,

Kat Lane
Vice-Chair
Australian Privacy Foundation
[redacted]

**About the Australian Privacy Foundation**

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems.

The APF makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters. Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be

critical of their performance. When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.