Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au
@efa_oz

Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

6 November 2020

Dear Commissioner,

RE: Exposure draft of the Data Availability and Transparency Bill

EFA welcomes the opportunity to provide comment on the exposure draft of a new Data Availability and Transparency Bill for Australia.

EFA's submission is contained in the following pages.

We are disappointed that the Office of the National Data Commissioner's offer to meet with us to discuss the proposed laws—which we were only too happy to do—did not ultimately result in a meeting. The initial discussions indicated a refreshing openness from government and we were of the belief that a meeting was likely to be productive and fruitful.

We are unclear on why our correspondence attempting to schedule a meeting elicited no response, particularly given the initial approach was made by your office. We assume this was an unfortunate oversight that will not recur.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Justin Warren
Board Member
Electronic Frontiers Australia

Introduction

EFA is concerned by the government's proposal to override existing privacy legislation by creating a new framework that will operate in parallel to existing laws. The Bill as written would create a "back door" mechanism for accessing data that would otherwise be protected from access and that was provided to government on the assumption that it would be so protected. This is particularly concerning when the proposed laws can override the robust protections provided for sensitive data, such as that collected about individuals by the Census.

Unlike all similar nations, Australia lacks a Federal enforceable human rights framework that contains both privacy and data protection provisions. This Bill risks further undermining Australians' right to privacy and to have their data protected from unauthorised access. In a time of increasing threats to data security and privacy, it is strange that the government would seek to further increase the risks to Australians by proposing a Bill such as this.

EFA believes that this Bill should not be introduced and that Australia must first create a Federally enforceable human rights framework that contains both privacy and data protection provisions.

Summary of Recommendations

1. **EFA recommends** that the Bill be delayed until Australia adopts robust, federally enforceable privacy protections based on a comprehensive human rights framework.
2. **EFA recommends** that the existing body of privacy law be reviewed carefully and either explicitly amended or repealed in order to ensure compatibility with this new law.
3. **EFA recommends** that a more nuanced data categorisation scheme be developed that recognises different types of data as being more or less sensitive, and that only the least sensitive data is dealt with by this Bill.
4. **EFA recommends** that s 8(d) be excised from the Bill entirely.
5. **EFA recommends** that the introduction of the Data Availability and Transparency Bill should be delayed and the Bill should be reconsidered once the review into the Privacy Act is completed.
6. **EFA recommends** taking a unified approach to privacy and data protection that will simplify the existing system of laws and provide clarity to individuals and agencies alike. The approach should be based on a human rights framework.
7. **EFA recommends** that individuals whose data has already been collected into existing datasets be provided with the opportunity to "opt out" of sharing of their data before any data sharing authorisations are made.
8. **EFA recommends** that the focus of the Bill should be on sharing and releasing data about government and its operations and that data about individuals should be excluded from the scope of the Bill.
9. **EFA recommends** that use of the Five Safes/Data Sharing Principles approach be abandoned and that it should be replaced with a more robust risk management framework developed in consultation with privacy and risk management experts.

10. **EFA recommends** that the advocacy functions described in the Bill be split out from the regulatory and oversight functions and these oversight functions be given to the Office of the Australian Information Commissioner. The National Data Commissioner should concentrate on advocacy, education and advice.

11. **EFA recommends** that the government should adopt the Australian Law Review Council's recommendation for a tort of serious invasion of privacy.[1]

12. **EFA recommends** that Division 2 of the Bill be removed entirely and that individuals' right to gather together as a class is protected.

13. **EFA recommends** that all decisions made should be reviewable by the Information and Privacy Commissioner, and the Courts, on both merit and judicial review grounds.

Missing Protections

Australia is unique among western nations in that it does not have a robust federally enforceable human rights framework that would underpin the proposed legislation and ensure individuals are provided with certain baseline protections. As a consequence, the proposed laws remove existing protections without providing robust additional ones in exchange.

EFA recommends that the Bill be delayed until Australia adopts robust, federally enforceable privacy protections based on a comprehensive human rights framework.

Law Provides Backdoor Data Access

EFA is concerned that the proposed Bill seeks to provide a blanket override of other, existing, privacy and data protection legislation, including but not limited to:

- The *Privacy Act 1998*[2]
- The *Census and Statistics Act 1905*[3]
- The *Archives Act 1983*[4]

An explicit goal of the proposed Bill is to provide a parallel mechanism that would bypass the specific and nuanced privacy and data protection features in each of these existing laws. The restrictions within these existing laws have not been adequately considered in detail during the development of the proposed Bill and this risks exposing sensitive data that the Parliament has already determined should remain private and unshared for specific and well evidenced reasons.

EFA recommends that the existing body of privacy law be reviewed carefully and either explicitly amended or repealed in order to ensure compatibility with this new law.

---

[1] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion Paper* (Commonwealth of Australia, 2014) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/> ('*Serious Invasions of Privacy in the Digital Era*').
[2] *Privacy Act 1988*.
[3] *Census and Statistics Act 1905*.
[4] *Archives Act 1983*.

Lack of Consent

The proposed Bill defines public sector data as "data lawfully created, collected or held by or on behalf of Commonwealth bodies" which is an extremely broad categorisation. This definition includes data that is obtained from individuals under threat of force or legal sanction that cannot be said to be provided consensually. It also includes data that is obtained by more subtle coercion, as receiving government services is often made contingent on providing certain data to government.

Performing research on people using data collected through coercion is profoundly unethical. Such data should be explicitly excluded from the set of data available to be shared under this Bill.

EFA recommends that a more nuanced data categorisation scheme be developed that recognises different types of data as being more or less sensitive, and that only the least sensitive data is encapsulated by this Bill. If the objectives of the proposed laws are achieved, less more sensitive data could then be included into the scheme, once the benefits clearly outweigh the risks.

EFA is also concerned by the inclusion of s 8(d) which appears to permit sharing of data collected about Australians with foreign entities. The caveat that an international agreement be binding on Australia is not sufficient to provide adequate protections for Australians.

Data forcibly collected from Australians should not be shared with foreign persons.

EFA recommends that s 8(d) be excised from the Bill entirely.

Bill Adds Legal Complexity

By providing a parallel and potentially overriding legal framework for data access, the proposed Bill risks adding greater complexity and challenge to interpretation of the law in what is already a complex and difficult area. The existing body of case law will need to be re-examined to consider the parallel implications of multiple pieces of overlapping law.

Section 22 of the Bill appears to have the effect of preventing future laws from restricting sharing of data authorised by this Bill. This would appear to preempt the ability of Parliament to change its mind and to restrict sharing of data in other contexts without amending the laws including in this Bill, yet this Bill does not see fit to take the time to amend other existing laws that restrict sharing of data. This approach to legal drafting risks creating a sequence of increasingly complex overrides and preemptions that will make it difficult, if not impossible, to be sure in advance what the law actually permits.

EFA considers it more prudent to examine the existing body of privacy and secrecy laws and to judiciously condense or amalgamate the law into a more unified system, centred on a human rights framework that protects individual privacy but also provides for sharing of government data such that government can better serve the populace.

The existing review of privacy legislation[5] that is currently underway provides just such an opportunity.

---

[5] 'Review of the Privacy Act 1988', *Attorney-General's Department* <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

EFA recommends that the introduction of the Data Availability and Transparency Bill should be delayed and the Bill should be reconsidered once the review into the Privacy Act is completed.

EFA recommends taking a unified approach to privacy and data protection that will simplify the existing system of laws and provide clarity to individuals and agencies alike. The approach should be based on a human rights framework.

Retrospective Action

The prospect of sharing and release of existing datasets preempts the ability of those who provided data under one set of assumptions to reconsider supplying that data now that the situation has changed. This violates the principle of informed consent, whereby those who are providing often quite sensitive information must give their informed consent to the uses this data will be used.

It is highly likely that people will reconsider the safety of providing information to government if they risk that data being repurposed without seeking their consent, particularly for sensitive data such as that provided in the Census. The backlash to the change in approach during the 2016 Census whereby the 'snapshot' nature of individual Censuses was changed to a longitudinal approach is evidence that Australians may avoid providing information if they no longer believe they can trust government promises to keep that data protected.

By providing a "back door" access mechanism to data that was provided under the assumption that it was protected by existing legislation, the Bill risks making data collection more difficult and datasets could become less reliable as people avoid collection or deliberately falsify data in order to avoid what they feel is surveillance.

This is particularly relevant in the operation of the *Archives Act* where data is provided under the assumption that it will not be released until a great deal of time has passed.

EFA recommends that individuals whose data has already been collected into existing datasets be provided with the opportunity to "opt out" of sharing of their data before any data sharing authorisations are made.

Start Small and Build

Data about individuals is inherently risky to share or release. The existing body of privacy legislation demonstrates data about people must be handled with care, and the research shows that data privacy has been a concern of individual Australians for many years[6], and remains so.[7]

[6] 'Australian Community Attitudes to Privacy Survey 2017', *OAIC* <https://www.oaic.gov.au/updates/videos/australian-community-attitudes-to-privacy-survey-2017/>.
[7] 'Australian Community Attitudes to Privacy Survey 2020', *OAIC* <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/>.

Australian governments' track record of data privacy and security is less-than-stellar.[8] Public trust in government is also declining.[9][10] In this environment, it would be more prudent to explore data sharing of less sensitive datasets before risking more sensitive datasets.

EFA recommends that the focus should be on sharing and releasing data about government and its operations as a first step in order to build competence and build trust. This would have the further benefits of providing an opportunity to refine the legal framework for data availability and transparency as initial flaws as discovered, as happens with any new system or framework, legal or otherwise.

Government will thus be able to increase trust in the populace that it is able to prudently and carefully handle their private data, and to demonstrate that the benefits of data sharing and transparency are real and worth investing in.

EFA considers the benefits of this approach to be fairly obvious and is somewhat puzzled why any government would choose to take the more dangerous approach of dealing with sensitive, personal data first. We welcome the government explaining why it is necessary to place Australians at greater risk of harm.

Low and Reducing Trust In Government

While Australians' desire for privacy remains high, trust in government has been decreasing for the past decade.[11] A rushed attempt to share data could well undermine trust in government further, particularly if data is shared inexpertly or recklessly. For example, the government was embarrassed by the release of the Medicare 'de-identified' dataset[12] after it immediately became apparent that individuals could be readily reidentified, often trivially so.

Economic Focus

EFA is very concerned by the economic focus that has driven the development of the Bill. It appears that data about people is viewed as a naturally occurring resource to be exploited rather than as the often sensitive and personal information about individuals that it actually is. By treating citizens interacting with their government, often mandatorily, as an opportunity to obtain a valuable commodity for free, the Bill converts people into mere passive things from which money—in the form of data—can be extracted, often by threat of force.

This approach inverts the relationship between the individual and the State so that the individual serves the economic needs of the state, rather than the state operating in service of the needs of the populace.

---

[8] Matt Bungard, 'Service NSW Cyber Attack: Data of 186,000 Customers Leaked', *The Sydney Morning Herald* (7 September 2020) <https://www.smh.com.au/national/nsw/data-of-186-000-customers-leaked-in-service-nsw-cyber-attack-20200907-p55t7g.html> ('*Service NSW Cyber Attack*').

[9] 'Australians' Trust in Government at an All-Time Low', *Government News* (8 February 2018) <https://www.governmentnews.com.au/australians-trust-government-time-low/>.

[10] 'Australian Community Attitudes to Privacy Survey 2020' (n 6).

[11] 'Australian Community Attitudes to Privacy Survey 2020', *OAIC* <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/>.

[12] Stephanie Anderson, 'Medicare Data Pulled over Breach Concerns', *ABC News* (Text, 29 September 2016) <https://www.abc.net.au/news/2016-09-29/medicare-pbs-dataset-pulled-over-encryption-concerns/7888686>.

Australians' data should not be used for profit.

EFA recommends that the focus of the Bill should be on sharing and releasing data about government and its operations and that data about individuals should be excluded from the scope of the Bill.

Use of Five Safes

Though the Bill has renamed the Five Safes framework[13] as five *data sharing principles* a change in label does not change their effect. This framework is not fit for purpose.[14] It takes an overly simplistic approach to risk management that encourages a checkbox approach to risk assessment and mitigation. This approach is likely to increase, not reduce, the potential for harm. The approach privileges the interests of governments and their institutions over those of individual citizens and uses poorly-substantiated claims of nebulous future benefits to justify this increased risk of harm.

EFA recommends that use of the Five Safes/Data Sharing Principles approach be abandoned and that it should be replaced with a more robust risk management framework developed in consultation with privacy and risk management experts.

Role of the National Data Commissioner

EFA considers it inappropriate for the National Data Commissioner to be tasked with both promoting the sharing and release of data and with regulation and oversight of entities responsible for protecting data. These two objectives are inherently in opposition. Regulation and oversight of the scheme should be performed by a body that is fully independent of a body tasked with promoting greater data sharing. The National Data Commissioner can perform either one of these roles effectively, but not both.

EFA notes that there is already a Commonwealth body with data oversight functions: the Office of the Australian Information Commissioner (OAIC). The OAIC already has broad experience in dealing with data privacy and handling of data breaches and has experienced staff familiar with regulatory functions and the complexities of privacy law.

Information is data with meaning, and it seems inefficient to add a second information commissioner, albeit one with reduced meaning.

EFA recommends that the advocacy functions described in the Bill be split out from the regulatory and oversight functions and these oversight functions be given to the Office of the Australian Information Commissioner. The National Data Commissioner should concentrate on advocacy, education and advice.

Individual Remedy For Data Breach Harm

The Bill does not provide for a private right of action to seek remedy or compensation for harm suffered as a result of inappropriate data sharing or data breach. Appeals to a potentially

---

[13] Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: Designing Data Access for Research' [2016] (1601) *Economics Working Paper Series* <https://uwe-repository.worktribe.com/preview/914753/1601.pdf> ('Five Safes').

[14] Chris Culnane, Benjamin IP Rubinstein and David Watts, 'Not Fit for Purpose: A Critical Analysis of the "Five Safes"' [2020] *arXiv:2011.02142 [cs]* <http://arxiv.org/abs/2011.02142> ('Not Fit for Purpose').

under-resourced and ill-informed regulator are not sufficient to ensure that agencies keep individuals safe. We have recent experience of the harms caused by agencies acting unlawfully, in some cases for many years[15], and it is unclear that government regulators are sufficiently able to safeguard individual safety.

While there is a place for regulators to address systemic issues that affect a large number of people, far too often individuals suffer ongoing harms while waiting for regulators to act. Regulators are often reluctant to take up the cause of individuals, preferring to take a more utilitarian "greatest good for the greatest number" approach that can leave many individuals unprotected.

A private right of action would fill in this gap and allow regulators to concentrate on systemic issues, allowing them to make efficient use of their limited resources, while also providing individuals with a pathway to justice if their specific case does not satisfy regulators' criteria for being of sufficient importance to pursue.

EFA recommends that the government should adopt the Australian Law Review Council's recommendation for a tort of serious invasion of privacy.[16]

Representative Complaints (Class Actions)

EFA is very concerned by the substantial amount of time and energy the Bill devotes to narrowing or excluding the potential for class actions. Division 2 appears to be designed to pre-empt the rights of individuals to gather together as a class to seek remedy for substantial harms suffered as a result of inappropriate data sharing.

That so much space is devoted to limiting the potential for class action is particularly concerning given the ongoing *Robodebt* debacle[17] in which a major agency of the government was found to have engaged in systematically unlawful behaviour[18] and repeatedly failed to discontinue this behaviour.[19]

This gives the appearance that the Australian government is very concerned that inappropriate data sharing *will* occur and that it is seeking to pre-emptively cut off an important way for individuals to counter the power and resources of the government.

---

[15] Paul Karp, 'Government Admits Robodebt Was Unlawful as It Settles Legal Challenge', *The Guardian* (online, 27 November 2019) <https://www.theguardian.com/australia-news/2019/nov/27/government-admits-robodebt-was-unlawful-as-it-settles-legal-challenge>.

[16] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion Paper* (Commonwealth of Australia, 2014) <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/> ('*Serious Invasions of Privacy in the Digital Era*').

[17] Luke Henriques-Gomes, 'Robodebt: Government Admits It Will Be Forced to Refund $550m under Botched Scheme', *The Guardian* (online, 26 March 2020) <https://www.theguardian.com/australia-news/2020/mar/27/robodebt-government-admits-it-will-be-forced-to-refund-550m-under-botched-scheme> ('Robodebt').

[18] Luke Henriques-Gomes, 'Robodebt Scandal: Leak Reveals Unlawful Debts Predate 2015 but Government Has No Plans to Pay Back Money', *The Guardian* (online, 30 May 2020) <https://www.theguardian.com/australia-news/2020/may/31/robodebt-scandal-leak-reveals-unlawful-debts-predate-2015-but-government-has-no-plans-to-pay-back-money> ('Robodebt Scandal').

[19] Letecia Luty and Jamie Luxton, '"It Should Not Have Taken so Long": Robodebt Took a Huge Toll – There Must Be Real Accountability | Letecia Luty and Jamie Luxton', *The Guardian* (online, 3 June 2020) <https://www.theguardian.com/australia-news/2020/jun/04/it-should-not-have-taken-so-long-robodebt-took-a-huge-toll-there-must-be-real-accountability> ('"It Should Not Have Taken so Long"').

This is not the behaviour of a government that can be trusted by its citizens.

EFA recommends that Division 2 of the Bill be removed entirely and that individuals' right to gather together as a class is protected.

Review of Decisions

The ability to seek review of decisions is an important feature of our legal system and forms a vital check on potential abuse of power. Such review must be independent of the government and the Commissioner, and all decisions must be reviewable.

The level of review provided in the current form of the Bill is overly narrow and leaves many decisions unreviewable.

EFA recommends that all decisions made should be reviewable by the Information and Privacy Commissioner, and the Courts, on both merit and judicial review grounds.