public interest
ADVOCACY CENTRE

Data Availability and Transparency Bill 2020: Submission to the Senate Finance and Public Administration Legislation Committee

March 2021

Level 5, 175 Liverpool Street, Sydney NSW 2000
Phone: 61 2 8898 6500 • Fax: 61 2 8898 6555 • www.piac.asn.au

About the Public Interest Advocacy Centre

The Public Interest Advocacy Centre (PIAC) is an independent, non-profit legal centre based in Sydney.

Established in 1982, PIAC tackles barriers to justice and fairness experienced by people who are vulnerable or facing disadvantage. We ensure basic rights are enjoyed across the community through legal assistance and strategic litigation, public policy development, communication and training.

Our work addresses issues such as:

- Reducing homelessness, through the Homeless Persons' Legal Service
- Access for people with disability to basic services like public transport, financial services, media and digital technologies
- Justice for Aboriginal and Torres Strait Islander people
- Access to affordable energy and water (the Energy and Water Consumers Advocacy Program)
- Fair use of police powers
- Rights of people in detention, including equal access to health care for asylum seekers (the Asylum Seeker Health Rights Project)
- Transitional justice
- Government accountability.

Contact

Chadwick Wong
Public Interest Advocacy Centre
Level 5, 175 Liverpool St
Sydney NSW 2000

Website: www.piac.asn.au

Public Interest Advocacy Centre

@PIACnews

The Public Interest Advocacy Centre office is located on the land of the Gadigal of the Eora Nation.

Contents

Recommendation 1: Strengthen consent requirements under the Bill

Strengthen the requirement for consent by better defining the circumstances in which it will be 'unreasonable or impracticable' to seek consent of an individual to share their personal information under cl 16(2)(c), including by identifying relevant factors to be taken into account in making that decision.

Recommendation 2: Publish a register of efforts to seek consent for the sharing of personal information

Where personal information is shared by data custodians without the consent of individuals, on the basis that it is unreasonable or impracticable, the data custodian must publish the efforts undertaken to seek that consent and the reason for dispensing with consent.

Recommendation 3: Notification to individuals whose personal information is being shared

Insert a provision in the Bill which requires notification to individuals whose personal information is being shared under the data sharing scheme. Notification should include details of the data sharing entities, the purposes for which the information is shared, links to the relevant registers held by the Commissioner, and information about their rights.

Recommendation 4: Withdrawal of consent

Insert a provision in the Bill to make clear that individuals who consent to the provision of their personal information under cl 16(2)(c), or whose consent was not obtained on the basis that it was 'unreasonable or impracticable' to do so, are able to withdraw their consent for future use or sharing of their personal information.

Recommendation 5: Immigration detention medical records should be excluded

Immigration detention health records held by the Department of Home Affairs should not be classified as public sector data that could be shared under the proposed data sharing scheme.

Recommendation 6: Introduce regular audits by the National Data Commissioner

A provision should be inserted into the Bill to require regular audits by the National Data Commissioner into decision-making by data custodians, to ensure that any guidelines issued by the Commissioner are properly applied and that decisions appropriately balance the objects of the scheme and the rights of individuals.

Recommendation 7: Merits review and complaints by individuals of decisions by data custodians

Decisions made and actions taken by data custodians, especially those concerning the sharing of personal information or data which could be re-identified, should be subject to merits review and a complaints process. Individuals whose information is being shared should be notified of the proposed sharing, and given an opportunity to seek merits review or make a complaint if they object to the decision being made or the action being undertaken.

Recommendation 8: Australian Federal Police should be excluded from the scheme

The Australian Federal Police should be listed as an 'excluded entity' under cl 11(3).

Recommendation 9: Introduce a civil penalty regime for data breaches arising from negligence or recklessness

A civil penalty regime should be introduced to empower the National Data Commissioner to investigate and seek penalties against data sharing entities whose negligence, recklessness or poor security controls results in a data breach. Such civil penalty should be significant to ensure appropriate deterrence from inappropriate or inadequate security controls.

Recommendation 10: Review of the Data Availability and Transparency Act

In the event that the Data Availability and Transparency Bill is passed prior to the current proposed reforms to the Privacy Act are enacted, the proposed scheme should be reviewed to ensure the intended Privacy Act underpinnings remain in place and effective.

1. Introduction

The Public Interest Advocacy Centre (**PIAC**) welcomes the opportunity to make a submission to the Senate Finance and Public Administration Legislation Committee (**Committee**) on the *Data Availability and Transparency Bill 2020* (the **Bill**).

PIAC's work focuses on tackling barriers to justice and fairness experienced by marginalised communities. While PIAC does not oppose appropriate, secure and informed consent-based sharing of public sector data for the purposes of improving socio-economic outcomes, we are concerned that the Bill fails to protect the rights of the most vulnerable.

We have previously participated in the consultation on the exposure draft of the Bill. The concerns we raised in relation to the exposure draft have not been abated in the current form of the Bill.

Many of our concerns are shared by the Senate Standing Committee for the Scrutiny of Bills (**Scrutiny Committee**)[1] and the Parliamentary Joint Committee on Human Rights (**PJCHR**).[2]

We welcome this further consideration by the Committee of the Bill.

2. Context

PIAC's submission draws on our experience in working with people from marginalised communities.

The lack of transparency and accountability in the Bill disproportionately affects marginalised communities, including homeless people, people with disability, First Nations people, young people, elderly people, and asylum seekers. These communities are more likely to access welfare services, such as income support and public health services, and are disproportionately subject to corrective services or detention. Some members of these communities may be among those least empowered to understand how their data is used.

According to the Office of the Australian Information Commissioner (**OAIC**)'s 2020 Australian Community Attitudes to Privacy Survey:

> Two-thirds of Australians believe that vulnerable groups, such as children under 12 years old (68%) and 13-17 years old (64%), elderly Australians (67%) and people with an intellectual disability (67%), require additional protection under the Privacy Act. A significant minority of Australians also support the additional protection of young adults (42%), people who speak English as a second language (39%) and new migrants to Australia (38%).[3]

1 Scrutiny Committee, *Scrutiny Digest 1 of 2021*, 29 January 2021, 4-20; Scrutiny Committee, *Scrutiny Digest 3 of 2021*, 17 February 2021, 10-27.
2 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021* [2021] AUPJCHR 16, 5-18.
3 Office of the Australian Information Commissioner, *2020 Australian Community Attitudes to Privacy Survey*, September 2020, 68.

In the same survey, 83% of Australians 'would like the government to do more to protect the privacy of their data.'[4] Privacy remains a major concern for 70% of Australians in 2020[5], with 61% of Australians identifying data security and data breaches as among the biggest privacy risks.[6] Only 36% of Australians are comfortable with government agencies sharing their personal information, with 40% of Australians uncomfortable with this. 70% of Australians are uncomfortable with government agencies sharing their personal information with businesses.[7]

Within this context of low public trust in government sharing of data, the Bill facilitates the sharing of an 'extremely wide range of data held by Commonwealth bodies with other government and non-government entities'. [8] This legislation assumes good faith on behalf of every government agency that holds the personal data of Australians, and so has inadequate transparency, control, checks and balances for all Australians, especially those who are marginalised. We recommend significantly stronger oversight and confidence-building measures before this legislation is passed.

Our submission addresses how the following issues in particular affect these communities:

- Consent issues, including specific sensitivities with asylum seeker health records;
- The broad power vested in data custodians as sole decision-makers in sharing data and the overarching need for greater accountability and transparency in the scheme;
- The use of data by law enforcement agencies; and
- Civil penalties for data breaches.

3. Consent

The Bill proposes, at cl 16(2)(c), that personal information of individuals can be shared without the consent of the individuals if it is 'unreasonable or impracticable' to seek consent. While we recognise the inclusion of consent in the 'project principle' is an improvement on earlier considerations where consent was not intended to be required under the legislation, this remains an issue of concern.

We echo the concerns of the Scrutiny Committee as to the breadth of this 'unreasonable or impracticable' exception, especially given the Minister's statement that privacy interests are to be 'balanced' with the public interest in sharing public sector data, and that the Bill does not assume one must prevail at the expense of the other.[9] We share the Scrutiny Committee's view that privacy interests should be 'clearly central to the operation of the scheme' and that the public interest test should prioritise privacy interests in decision-making under the scheme.[10] Likewise, we share the PJCHR's concerns that 'public interest' is not defined and it is unclear to what extent privacy interests will factor into public interest determinations.[11]

4 Ibid, 65.
5 Ibid, 4.
6 Ibid, 6.
7 Ibid, 27.
8 PJCHR, [1.17].
9 Scrutiny Committee, *Scrutiny Digest 3 of 2021*, [2.20].
10 Scrutiny Committee, *Scrutiny Digest 1 of 2021*, [1.11], [1.17].
11 PJCHR, [1.25].

We also agree with the Scrutiny Committee's views that the Bill should include an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified. This is especially so where consent cannot be obtained.[12]

We have three further comments in addition to the Scrutiny Committee and PJCHR's concerns.

First, the concepts of 'unreasonable or impracticable' are not defined, either in the Bill or in the *Privacy Act 1988* (Cth), where the phrase originates. Guidance on this phrase, as issued by the OAIC, is limited. It is not clear which existing guidelines, standards and ethics processes will apply to the data sharing scheme, or what further guidance will be provided. In the absence of clear definition and guidance, the data custodian is entrusted with wide discretion to determine whether this threshold is met, with determinations not being subject to review. As such, there is limited accountability and transparency in these decisions. This provides little assurance to the community that Commonwealth agencies sharing personal information will interpret these concepts narrowly and appropriately, with due regard to privacy.

This issue affects marginalised communities disproportionately, given their greater interaction with Government services. People who rely on Government services may not be in a position to provide informed consent given the inherent power imbalance when requesting services. In certain circumstances, even where a person is informed about how their personal information will be handled, it can be practically difficult to withhold consent for the proposed management of their personal information. For example, consent procedures for the use of immigration detention medical records – where a person arriving in detention signs a consent form to say that their information can be used to assist with their placement – have been criticised as inadequate for allowing a person's information to be used by the Department of Home Affairs for purposes other than a patient's health care.[13]

A person's ability to consent to the subsequent sharing and collection of that information at the initial point of providing it is even more limited. This is especially so given the way the Bill interacts with Australian Privacy Principles (**APP**) 3 and 6 under the *Privacy Act 1988*. APP 6 generally permits use or disclosure of an individual's personal information only for the 'primary purpose', being the purpose for which it was collected. It cannot be used or disclosed for any other purpose unless the individual has consented, or one of the exceptions at subclause 6.2 or 6.3 of the *Privacy Act* applies. The Bill has the effect of falling entirely within the exception of subclause 6.2(b), being an exception where use or disclosure is authorised by Australian law.[14] Given the Bill 'authorises data custodians to share public sector data with accredited entities from all levels of government as well as industry, research, and others in the private sector',[15] this significantly expands the possible use and disclosure of an individual's personal information, and in ways which could not reasonably be envisaged at the time the information was collected. Similar considerations apply in respect of APP 3, concerning the collection of sensitive information.

---

12 Ibid, [2.23].

13 D Marr, O Laughland and B Code, "Asylum seekers' medical records being used against them, says mental health chief – video", *Guardian Australia*, https://www.theguardian.com/world/video/2014/aug/04/asylum-seeker-health-records-used-against-them-video.

14 Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*, 6 September 2020 (**Privacy Impact Assessment**), 25.

15 Explanatory Memorandum to the *Data Availability and Transparency Bill 2020*, Part 1, [17].

In those circumstances, the disclosure of personal information ought to be subject to strong consent requirements, and the 'unreasonable or impracticable' exception must be better defined. The legislation should identify factors that should be taken into account in determining whether it is unreasonable or impracticable to seek consent and identify what a decision-maker must be satisfied of before concluding that seeking consent is unreasonable or impracticable. It should not, for instance, include instances where a homeless person is unable to be located at a particular point in time for their consent to be sought, or where it is 'inconvenient' or costly to obtain consent from a person with disability, or where a person fails to respond to Government contact. For the Government to build confidence in the community that data is being shared appropriately, consent of those least empowered must not be bypassed.

Where it is genuinely unreasonable or impracticable to seek consent before personal information is shared, the efforts to collect consent and the reason for dispensing with the consent requirement must be recorded in a public register (obviously in a form that does not identify individuals). This allows for increased scrutiny and accountability of decisions made by data custodians, and ensures that those decisions are subject to review by the National Data Commissioner.

Second, individuals whose personal information is being shared ought to be notified of the details of that sharing. The Bill does not presently contemplate this notification process. While there are certain points at which notification may occur – such as when consent is being sought, or when validation of the output is being sought under cl 21(1)(b)(ii) – individuals should also be notified at the point of sharing to ensure transparency in data sharing. This empowers individuals in at least three ways:

- they are able to withdraw consent if they so choose, as discussed below;
- they are able to exercise their broader rights under the *Privacy Act* if they know who holds their information; and
- they should be able to challenge decisions to share their personal information. We discuss this point later in this submission.

Third, the Bill should make it clear individuals can withdraw consent to the sharing of their personal information, whether that consent was provided expressly or impliedly, or not at all (by reason of it being 'unreasonable or impracticable' to obtain consent at the time). Individuals ought to be able to request that their personal information be updated, deleted or not to be used in particular ways. This is especially so where consent was not able to be obtained in the first instance, and the individual is subsequently informed of the sharing of their information. The Bill should acknowledge that consent must be current and specific.

Recommendation 1: Strengthen consent requirements under the Bill

Strengthen the requirement for consent by better defining the circumstances in which it will be 'unreasonable or impracticable' to seek consent of an individual to share their personal information under cl 16(2)(c), including by identifying relevant factors to be taken into account in making that decision.

Recommendation 2: Publish a register of efforts to seek consent for the sharing of personal information

Where personal information is shared by data custodians without the consent of individuals, on the basis that it is unreasonable or impracticable, the data custodian must publish the efforts undertaken to seek that consent and the reason for dispensing with consent.

Recommendation 3: Notification to individuals whose personal information is being shared

Insert a provision in the Bill which requires notification to individuals whose personal information is being shared under the data sharing scheme. Notification should include details of the data sharing entities, the purposes for which the information is shared, links to the relevant registers held by the Commissioner, and information about their rights.

Recommendation 4: Withdrawal of consent

Insert a provision in the Bill to make clear that individuals who consent to the provision of their personal information under cl 16(2)(c), or whose consent was not obtained on the basis that it was 'unreasonable or impracticable' to do so, are able to withdraw their consent for future use or sharing of their personal information.

3.1 Specific sensitivities in immigration detention health records

We have particular concerns that the Bill's provisions may not adequately safeguard the confidentiality of immigration detention medical records or sufficiently protect against the unintended use of the personal information they contain.

PIAC made comments on the exposure draft of the *Data Availability and Transparency Regulations 2020*, in respect of provisions which were prescribed for the purposes of cl 17(4)(a) – that is, legislative provisions which were proposed to be excluded from data sharing scheme.

We have not seen, and are not aware of, any proposed amended set of Regulations.

The exposure draft of the Regulations indicated that certain 'especially sensitive' public sector data would be excluded from the scheme, such as My Health Records data (the handling of which will remain governed under other legislation). However, immigration detention medical records were not excluded from the scheme. If this remains the case, we strongly call for the exclusion of such records from the scheme.

PIAC's Asylum Seeker Health Rights project seeks to ensure that asylum seekers held in Australian onshore immigration detention have access to the same standard of health care available in the Australian community. As with patients in the Australian community, patients in immigration detention are entitled to confidentiality and privacy in the management of their medical records, which contain sensitive health information and often detailed personal information.

The Commonwealth Government, through the Department of Home Affairs, contracts International Health & Medical Services (**IHMS**) to provide health services in Australian immigration detention facilities. The *Privacy Act 1988* regulates how IHMS and the Department of Home Affairs handle an individual's medical records and requires the application of the Australian

Privacy Principles when handling and disclosing information. The Department of Home Affairs' privacy policy describes that it 'will use personal information for the purposes for which it was collected, and for secondary purposes where permitted by law or where permission is given by the individual.'[16]

The Department is authorised to disclose personal information in circumstances specified under the *Migration Act 1958* and the *Citizenship Act 2007* and for certain law enforcement purposes. Where a third party otherwise seeks to access a person's medical record, the person's signed consent is required.

As described above, the Bill has the effect of expanding the circumstances in which a data custodian, such as the Department of Home Affairs, is permitted by law to use or disclose an individual's personal information under APP 6.

We are concerned that the data sharing scheme could enable the information in detention health records held by the Department of Home Affairs, to be more broadly shared with other entities without due regard to the standards of confidentiality that normally apply to a patient's health information in other contexts.

The disclosure of personal information in the health records of asylum seekers and refugees in detention for purposes other than a person's health care can infringe a person's rights to privacy and dignity and can also result in harm to the individual. For example, it can expose information that could compromise a person's safety if returned to their country of origin.

The Bill proposes to exclude other types of especially sensitive data, such as My Health Record information, from the data sharing scheme. We consider that immigration detention health record information is a further type of sensitive data that should not be shared through this scheme.

Recommendation 5: Immigration detention medical records should be excluded

Immigration detention health records held by the Department of Home Affairs should not be classified as public sector data that could be shared under the proposed data sharing scheme.

4. Overarching transparency and accountability

The Bill proposes to allow data sharing in a wide range of circumstances, provided (in essence) that the sharing is for a data sharing purpose, is consistent with the data sharing principles, and is in accordance with a data sharing agreement.[17] The 'data sharing purposes' are very broad, being the delivery of any government service, informing government policy and programs, and research and development (including commercial research and development).[18] The sharing of data to inform government policy and programs is intended to be interpreted 'broadly'.[19]

In turn, the 'data sharing principles' are broad and vague – each principle is defined by reference to the term 'appropriate' or 'agreed'. The data must be shared for an appropriate project; made

16 Department of Home Affairs, Privacy Policy, https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/plans-and-charters/privacy-policy.
17 Bill, cl 13(1).
18 Bill, cl 15(1).
19 Explanatory Memorandum, Part 1, [30].

available only to appropriate persons; in a setting that is appropriately controlled; with appropriate protections applied; with outputs that are as agreed (between the relevant data scheme entities); and with risks that are appropriately mitigated. These principles may be informed by guidance provided by the National Data Commissioner. The inclusion of non-exclusive 'elements'[20] to assist with the interpretation of these broad principles is welcome, but not sufficient. As the Privacy Impact Assessment states, the 'high-level nature of the Data Sharing Principles poses a privacy risk'.[21]

Within this context, it is the data custodian who solely decides whether the proposed information sharing meets these broad parameters, and if so, to exercise its discretion to share the information with the accredited entity (be they a government, public or commercial entity). Any such decision is not subject to merits review. Any judicial review will be limited given the lack of transparency in decisions being made by data custodians as to the sharing of personal information.

The Explanatory Memorandum asserts that merits review is not available because data sharing decisions 'are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data'.[22] This claim is made in the context where there is no legal obligation to consider the unique circumstances of marginalised communities. The controversy surrounding the 'Robodebt' scheme should caution against a process which does not properly consider these communities.

We do not regard the proposed scheme as sufficiently robust in its protection of personal information in circumstances where:

- its parameters are:
    - purposes that possibly include all Government activity that is not expressly excluded (it is difficult to see what purposes might fall outside of delivery of government services and informing government policy and programs when interpreted broadly);
    - high-level principles which will be explained in non-legislative guidelines, to which data scheme entities only need to 'have regard to'[23]; and
    - the data sharing agreement which is agreed to between the agency and the accredited entity wishing to access that data;
- the decisions being made are not transparent, given there is no requirement for decisions to be published or affected individuals to be notified; and
- the decisions are not subject to merits review.

While the National Data Commissioner has oversight of the data scheme entities, their powers are largely confined to the complaints mechanism between data scheme entities (cl 88) and the assessments process (cl 99). There is no requirement that the Commissioner conduct regular assessments or audits of decision-making to ensure compliance with the Bill.

---

20 At subcl 16(2), (4), (6), (8), (10).
21 Privacy Impact Assessment, above n 14, 38.
22 Explanatory Memorandum, Part, [54].
23 Bill, cl 27.

This requires a significant level of trust in Government agencies holding sensitive information – data custodians – in circumstances where accountability and transparency is limited. Again, this affects marginalised communities most acutely.

The proposed model needs to have greater transparency and accountability built in, to ensure data custodians make decisions consistent with community expectations, and if not, that there are appropriate oversight mechanisms. This should include:

- requiring regular audits by the Commissioner into decision-making by data custodians, to ensure that any guidelines are properly applied and decisions appropriately balance the objects of the scheme and the rights of individuals;
- allowing merits review of decisions and complaints by individuals, especially in relation to matters which concern the sharing of personal information; and
- improving the consent mechanisms, as discussed above, including by way of notification of data sharing.

It is not apparent why an avenue for merits review should not be provided to challenge decisions of data custodians to share personal information or data which could be re-identified. While the Explanatory Memorandum states that 'existing avenues for redress in other schemes continue to be available',[24] decisions being made to share personal information under the proposed scheme should be subject to its own review process for affected individuals. This is especially in circumstances where the complaints process does not permit individual complaints.

PIAC also supports the Scrutiny Committee's views concerning the lack of a dedicated complaints mechanism under the scheme, and the lack of requirement for complaints made to the Australian Information Commissioner or any other entity regarding the scheme to be notified to the National Data Commissioner. We agree that 'full visibility of complaints about the scheme may assist in reducing the possibility of tension between the dual roles of the National Data Commissioner as both regulator and champion of the data sharing scheme'.[25] Similar concerns about the lack of a complaints mechanism were also noted by the PJCHR.[26]

Recommendation 6: Introduce regular audits by the National Data Commissioner

A provision should be inserted into the Bill to require regular audits by the National Data Commissioner into decision-making by data custodians, to ensure that any guidelines issued by the Commissioner are properly applied and that decisions appropriately balance the objects of the scheme and the rights of individuals.

Recommendation 7: Merits review and complaints by individuals of decisions by data custodians

Decisions made and actions taken by data custodians, especially those concerning the sharing of personal information or data which could be re-identified, should be subject to merits review and a complaints process. Individuals whose information is being shared should be notified of the proposed sharing, and given an opportunity to seek merits review or make a complaint if they object to the decision being made or the action being undertaken.

24 Explanatory Memorandum, Part 1, [56].
25 Scrutiny Committee, *Scrutiny Digest 3 of 2021*, [2.32]-[2.33].
26 PJCHR, [1.31].

5. Data sharing with law enforcement agencies

The Bill precludes the sharing, collection and use of data for an 'enforcement related purpose': cl 15(2)(a).

PIAC previously submitted that the former cl 15(4) – which was a carve out of the exclusion of 'enforcement related purpose' – should be removed or amended to provide clarity about the scope of 'enforcement related purpose'. Clause 15(4) has now been amended to clarify that data sharing involving any person undertaking an activity listed in cl 15(3) will remain precluded. The current drafting of cl 15 provides important explicit protection against the use of data by law enforcement agencies for surveillance and monitoring activities.

However, we share the PJCHR's view that the Australian Federal Police should be expressly listed as an 'excluded entity' under cl 11(3) of the Bill, given that enforcement related purposes are precluded from data sharing and that operational data from the AFP is expressly excluded under cl 17(2)(b)(ii).[27] As the Explanatory Memorandum states, 'While enforcement related activities are legitimate functions of government, they are best carried out under dedicated laws'.[28] No explanation has been provided as to why the AFP otherwise ought to remain within the scope of the scheme.

Recommendation 8: Australian Federal Police should be excluded from the scheme

The Australian Federal Police should be listed as an 'excluded entity' under cl 11(3).

6. Penalties for data breaches

One of the objects of the Bill is to 'enable consistent safeguards for sharing public sector data'.[29] As the Explanatory Memorandum explains, this includes 'robust safeguards to protect privacy and data security'.[30] However, there are limited ramifications for breaches of these safeguards, especially where a data scheme entity is negligent or reckless in respect of data security. A civil penalty regime for these types of data breaches is necessary given the significant broadening of data sharing envisaged by the Bill. This is especially the case if it captures highly sensitive personal information.

The data security safeguards contained in the Bill are currently focused on the 'front end' of data sharing – that is, prior to the data being shared. The safeguards include the accreditation process, which includes consideration of appropriate data security controls; the mandatory terms of the data sharing agreement; and the data sharing principles, specifically the 'setting principle'[31] (noting that these principles are applied by the data custodian in their sole discretion). The *Privacy Act* continues to apply in relation to data handling and security, in particular APP 11.

Where these safeguards fail however, and a data breach occurs, the responsible entity is not subject to any penalty under the Bill. The *Privacy Act* provides for civil penalties for a 'serious

27 PJCHR, [1.24].
28 Explanatory Memorandum, Part 2, [111].
29 Bill, cl 3(b).
30 Explanatory Memorandum, Part 2, [8].
31 Ibid, [129].

interference' with an individual's privacy,[32] or for entities that 'repeatedly' interfere with an individual's privacy.[33] It does not, however, have a general penalty regime for data breaches that do not constitute a 'serious interference' or 'repeated' interference. This is further limited by the OAIC's position that it 'will not seek a civil penalty order in all matters involving a "serious" interference with privacy.' The OAIC has stated that it is more likely to seek a civil penalty where the interference is 'particularly serious or egregious in nature', the entity has a 'history of serious interferences with privacy' or the OAIC considers the serious interference arose because of a failure by the entity to 'take its obligations seriously' or has a 'blatant disregard' for its privacy obligations.[34]

The only penalty provisions under the Bill are in relation to unauthorised sharing, collection or use of data[35], compliance with mandatory terms of a data sharing agreement[36], breaches of conditions of accreditation[37], provision of false or misleading information to the Commissioner[38], compliance with notices made under cl 104 regarding the provision of information and documents, and breaches of directions of the Commissioner made under cl 112.

Given the potential for a wide variety of entities, public and private, to be accredited under this scheme and the potential for sensitive personal information to be shared without consent, it is necessary for the Bill to include a civil penalty regime for certain types of data breaches, as a further data security safeguard. Civil penalties should apply to data breaches which occur as a result of negligence or recklessness in the sharing, collection, use or disclosure of data which is subject to the scheme. This excludes data breaches which occur due to malicious or criminal attacks where the conduct and security controls of the data sharing entity was otherwise appropriate.

Data breaches have occurred in respect of public sector data in a number of high-profile incidents, with significant consequences. These include:

- the Department of Immigration and Border Protection's data breach in February 2014, resulting in the release of sensitive personal information of people in immigration detention, including asylum seekers;
- the Federal Court's data breach in March 2020 resulting in the publication of the identities of asylum seekers; and
- the Services NSW data breach in 2020 which resulted in the personal information of 186,000 customers being stolen.

This is not to suggest that each of these incidents warranted civil penalties. However, each of these data breaches resulted in significant consequences which disproportionately impacted marginalised communities, and should have been subject to investigations as to potential civil penalties.

32 *Privacy Act*, s 13G(a).
33 *Privacy Act*, s 13G(b).
34 OAIC, *Guide to privacy regulatory action*, June 2020, [6.30].
35 Bill, cl 14.
36 Bill, cl 20.
37 Bill, cl 30.
38 Bill, cl 32.

Civil penalties should be considerable to ensure further safeguarding of personal information. We note that the European Union's General Data Protection Regulation provides for significant fines, being up to 20 million euros or up to 4% of the total worldwide annual turnover, whichever is higher.[39]

Recommendation 9: Introduce a civil penalty regime for data breaches arising from negligence or recklessness

A civil penalty regime should be introduced to empower the National Data Commissioner to investigate and seek penalties against data sharing entities whose negligence, recklessness or poor security controls results in a data breach. Such civil penalty should be significant to ensure appropriate deterrence from inappropriate or inadequate security controls.

7. Review following Privacy Act reform

On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the *Privacy Act*. On 30 October 2020, the Government published the terms of reference for this review, which includes broad issues concerning the scope and application of the *Privacy Act*, a statutory tort for serious invasions of privacy, the rights of individuals to direct action to enforce privacy obligations under the Act, and the effectiveness of the notifiable data breach scheme.

Given the intention of the Bill to operate alongside the *Privacy Act* and the *Privacy Act* underpinnings for the Bill, it is critical that the *Data Availability and Transparency Act*, if passed, be subject to review shortly after any reform to the *Privacy Act* to ensure this data sharing scheme remains fit for purpose and contains the safeguards intended in the Bill.

Recommendation 10: Review of the Data Availability and Transparency Act

In the event that the Data Availability and Transparency Bill is passed prior to the current proposed reforms to the Privacy Act are enacted, the proposed scheme should be reviewed to ensure the intended Privacy Act underpinnings remain in place and effective.

8. Conclusion

The proposed data sharing scheme, underpinned by the Bill, represents a significant reform to the way in which public sector data is shared and used by governments and other public and private entities. For such significant reform to be successful, it must have confidence and support from the community. PIAC shares the concerns of the Scrutiny Committee and PJCHR in relation to consent, privacy and public administration. We are also concerned that these issues disproportionately impact marginalised communities and are not sufficiently addressed by the Bill. Any data sharing scheme must be underpinned by strong transparency and accountability requirements, informed consent of individuals and strong data security safeguards, and must not stray into areas best dealt with through specific, purpose-built legislation.

39 General Data Protection Regulation, Regulation (EU) 2016/679, art 83(5).