The Senate

Finance and Public Administration Legislation Committee

Data Availability and Transparency Bill 2020 [Provisions] and Data Availability and Transparency (Consequential Amendments) Bill 2020 [Provisions]

April 2021

© Commonwealth of Australia 2021

ISBN 978-1-76093-218-3

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License.

The details of this licence are available on the Creative Commons website: https://creativecommons.org/licenses/by-nc-nd/4.0/.

Members

Chair

Senator Claire Chandler	LP, TAS

Deputy Chair

Senator Tim Ayres	ALP, NSW

Members

Senator James Paterson	LP, VIC
Senator Kimberley Kitching	ALP, VIC
Senator Matt O'Sullivan	LP, WA
Senator Malcolm Roberts	PHON, QLD

Senate Finance and Public Administration Committee Secretariat:

Sarah Redden, Committee Secretary
Kate Campbell, Principal Research Officer
Trish Carling, Senior Research Officer
Kate Morris, Research Officer
Michaela Le Cheile, Administrative Officer

Website: www.aph.gov.au/senate_fpa
PO Box 6100 E-mail: fpa.sen@aph.gov.au
Parliament House Ph: 02 6277 3846
Canberra ACT 2600 Fax: 02 6277 5809

Contents

Abbreviations

ABA	Australian Banking Association
ACCC	Australian Competition and Consumer Commission
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977*
ADSPs	accredited data services providers
AFP	Australian Federal Police
AIC	Australian Information Commissioner
Allens Hub	Allens Hub for Technology Law and Innovation
AMA	Australian Medical Association
APF	Australian Privacy Foundation
APP	Australian Privacy Principle
APRA	Australian Prudential Regulation Authority
APS	Australian Public Service
ARDC	Australian Research Data Commons
ASCL	Australian Society for Computers and Law
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
bill	Data Availability and Transparency Bill 2020
BSA	BSA | The Software Alliance
commissioner	National Data Commissioner
committee	Finance and Public Administration Legislation Committee
consequential amendments bill	Data Availability and Transparency (Consequential Amendments) Bill 2020
Electronic Frontiers	Electronic Frontiers Australia
EM	explanatory memorandum
FOI Act	*Freedom of Information Act 1982*
IDN	Indigenous Data Network
Joint committee	Parliamentary Joint Committee on Human Rights
Law Council	Law Council of Australia
MBS	Medicare Benefits Schedule
NACCHO	National Aboriginal Community Controlled Health Organisation
NHMRC	National Health and Medical Research Council
NSWCCL	New South Wales Council for Civil Liberties
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner
PBS	Pharmaceutical Benefits Scheme
PHRN	Population Health Research Network
PIAC	Public Interest Advocacy Centre

PJCIS	Parliamentary Joint Committee on Intelligence and Security
Privacy Act	*Privacy Act 1988*
RBA	Reserve Bank of Australia
Scrutiny committee	Senate Standing Committee for the Scrutiny of Bills
UNSWICS	University of New South Wales Institute for Cyber Security

List of Recommendations

Recommendation 1

5.182 The committee recommends that assurances are provided to Parliament regarding appropriate ongoing oversight by security agencies of data sharing agreements and potential security risks.

Recommendation 2

5.183 The committee recommends that any relevant findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector are taken into account as part of the development of any additional data codes and guidance material and inform continued engagement with the national security community.

Recommendation 3

5.189 The committee recommends that consideration is given to whether amendments could be made to the bill, or further clarification added to the explanatory memorandum to provide additional guidance regarding privacy protections, particularly in relation to the de-identifying of personal data that may be provided under the bill's data-sharing scheme.

Chapter 1
Introduction

1.1 On 4 February 2021 the Senate referred the provisions of the Data Availability and Transparency Bill 2020 (the bill) and the provisions of the Data Availability and Transparency (Consequential Amendments) Bill 2020 (the consequential amendments bill) to the Senate Finance and Public Administration Legislation Committee (the committee) for inquiry and report by 29 April 2021.[1]

Conduct of the inquiry

1.2 Details of the inquiry were made available on the committee's website. The committee also contacted a number of organisations and individuals inviting submissions to the inquiry. Submissions were received from 31 organisations and individuals, as detailed at Appendix 2.

1.3 The committee held a public hearing in Canberra on 20 April 2021. The witness list for the hearing can be found at Appendix 3.

Compatibility with human rights

Data Availability and Transparency Bill 2020

1.4 The statement of compatibility with human rights for the bill states that the bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.[2]

1.5 The Parliamentary Joint Committee on Human Rights (joint committee) examined the bill in its Report 2 of 2021 and Report 4 of 2021, where it raised a number of concerns and requested further information from the minister. Further detail is available in Chapter 4 of this report.

Data Availability and Transparency (Consequential Amendments) Bill 2020

1.6 The statement of compatibility with human rights for the consequential amendments bill states that the bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.[3]

1.7 The joint committee had no comment on the consequential amendments bill.

---

1 *Journals of the Senate*, No. 84, 4 February 2021, p. 2976.

2 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 82.

3 Data Availability and Transparency (Consequential Amendments) Bill 2020, *Explanatory Memorandum*, p. 10.

Consideration by the Senate Standing Committee for the Scrutiny of Bills

Data Availability and Transparency Bill 2020

1.8 The Senate Standing Committee for the Scrutiny of Bills (Scrutiny committee) examined the bill in its Scrutiny Digest 1 of 2021, where it raised a number of concerns and requested further information from the minister. It further considered the bill in its Scrutiny Digest 3 of 2021 and Scrutiny Digest 5 of 2021, taking into account responses provided by the minister.

1.9 Further detail on the Scrutiny committee's consideration is contained in Chapter 3 of this report.

Data Availability and Transparency (Consequential Amendments) Bill 2020

1.10 The Scrutiny committee had no comment on the consequential amendments bill.

Financial impact statement

Data Availability and Transparency Bill 2020

1.11 The explanatory memorandum states that the financial impact of the bill was $20.5 million from 2018-19 to 2021-22, and $11.1 million from 2020-21 over four years and $0.7 million ongoing from 2024-25.[4]

Data Availability and Transparency (Consequential Amendments) Bill 2020

1.12 The explanatory memorandum states that the financial impact of the consequential amendments bill was $20.5 million from 2018-19 to 2021-22, and $11.1 million from 2020-21 over four years and $0.7 million ongoing from 2024-25.[5]

Acknowledgments

1.13 The committee thanks those individuals and organisations who contributed to the inquiry by preparing written submissions and giving evidence at the public hearing.

Structure of the report

1.14 Chapter 2 contains an overview of the bills and the proposed data sharing scheme.

1.15 Chapter 3 provides further detail on the Scrutiny committee's consideration of the bill.

---

[4] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 1.

[5] Data Availability and Transparency (Consequential Amendments) Bill 2020, *Explanatory Memorandum*, p. 3.

1.16 Chapter 4 canvasses the joint committee’s examination of the bill.

1.17 Chapter 5 sets out the key issues raised by submitters and concludes with the committee's views and recommendations.

Chapter 2
Overview

Overview of the bills

2.1 The Data Availability and Transparency Bill 2020 (the bill or principal bill) and the Data Availability and Transparency (Consequential Amendments) Bill 2020 (the consequential amendments bill) were introduced to the House of Representatives on 9 December 2020.[1]

2.2 The bills are central to the Commonwealth Government's commitment to data sharing reform which was informed by a 2017 Productivity Commission inquiry report. As the explanatory memorandum (EM) to the bill set out:

> In 2018, the Australian Government committed to reform the way it shares public sector data. Reforms are necessary to realise the benefits of greater data availability and use identified by a Productivity Commission inquiry, supporting economic and research opportunities and the Government's vision for streamlined and efficient service delivery.[2]

2.3 The principal bill establishes a new data sharing scheme which will serve as a 'pathway and regulatory framework' for sharing public sector data for three permitted purposes, subject to new safeguards and enforcement mechanisms.[3]

2.4 Subject to the exclusion provisions under clause 17 and regulations, the public sector data which can be shared under the scheme encompasses 'all data collected, created, or held by the Commonwealth, or on its behalf'. The concept of data includes facts, statistics, and other information capable of being communicated, analysed or processed via physical or electronic means.[4]

2.5 As the submission from the Office of the National Data Commissioner (ONDC) stated:

> The bill establishes a scheme for controlled access to public sector data, which leverages existing frameworks for specific aspects of data management, rather than repeating or replacing them. This approach allows the data sharing scheme to fit neatly into the existing architecture of the national data system, minimising duplication and ensuring tailored protections are preserved.[5]

---

1 *House of Representatives Votes and Proceedings*, No. 92, 9 December 2020, p. 1517.

2 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 3.

3 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 3.

4 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 5.

5 Office of the National Data Commissioner, *Submission 20*, p. 2.

Design of the bills

2.6 The ONDC emphasised that the bill and its underlying policy positions were developed in response to the recommendations in the Productivity Commission's 2017 *Data Availability and Use* inquiry report and involved extensive co-design and engagement with the public service and stakeholders across academia, the private sector and civil society.[6]

2.7 It advised the committee that this collaborative approach enabled the ONDC to understand the concerns and expectations of the community and key stakeholder groups around data sharing and 'refine policy positions accordingly'.[7]

2.8 The ONDC also informed the committee that privacy was integral to the development of the data sharing scheme and was carefully considered at each stage of the legislative process. It explained:

> When developing the Bill, the ONDC adopted a 'privacy by design' approach to identify, minimise and mitigate privacy impacts wherever possible. Three independent Privacy Impact Assessments (PIAs) have been undertaken to identify strengths and weaknesses in the early policy positions and planned legislative framework, and the draft Bill itself. This approach reflects the ONDC's commitment to ongoing, proactive management of privacy. Privacy safeguards were also strengthened in response to guidance and advice from NDAC [National Data Advisory Council] and privacy experts, including the Office of the Australian Information Commissioner.[8]

Legislative framework

2.9 The legislative makeup of the data sharing scheme comprises:

- the principal bill;
- the consequential amendments bill; and
- three kinds of disallowable legislative instruments:
  - regulations;
  - ministerial rules; and
  - data codes.

2.10 The three kinds of legislative instruments may be used to address how using certain technology or methodologies affects entities' obligations under the bill. The EM noted that this approach allows the bill to remain 'technology neutral'.[9]

---

6 Office of the National Data Commissioner, *Submission 20*, pp. 4.

7 Office of the National Data Commissioner, *Submission 20*, pp. 4–5.

8 Office of the National Data Commissioner, *Submission 20*, pp. 4–5.

9 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 72.

2.11 Regulations and ministerial rules will set the parameters of the scheme and establish key criteria and thresholds for engaging with the scheme. Data codes will be issued by the National Data Commissioner (the commissioner) and are primarily intended to clarify how the scheme will operate and how legislative requirements should be complied with, and may implement administrative improvements.[10]

2.12 The commissioner, which the bill will establish as an independent regulator for the scheme, may also issue 'non-legislative guidelines' that participating entities must have regard to and may release 'other guidance' as necessary.[11]

2.13 The bill is drafted as 'principle-based legislation' in order to 'ensure it remains relevant and adaptable to evolving technology and public expectations'.[12]

Operation of the data sharing scheme

2.14 The data sharing scheme enabled by the bills will allow accredited users to request controlled access to government data for three permitted purposes (as set out in Clause 15 of the bill). The three purposes are set out below.

(1) Improving government service delivery
Data sharing for this purpose could enable improved designs of systems, engagement and processes involved in government service delivery. For example, improving user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify details.

(2) Informing government policy and programs
Data sharing for this purpose (which is intended to be 'interpreted broadly') could help enable the discovery of trends and risks to inform public policy making, enable modelling of policy and program interventions, and provide a holistic understanding of cross-portfolio problems.

(3) Research and development
Data sharing for this purpose will enable accredited academics, scientists and innovators in the public and private sectors to access public sector data to gain insights and undertake activities to 'advance knowledge and contribute to society'.[13]

2.15 In addition to outlining the three 'permitted purposes' for data sharing, the bill also precludes data sharing for certain enforcement related purposes, such as law enforcement investigations and operations. The bill also does not authorise

---

10 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 72.

11 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 3.

12 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 9.

13 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 5–6.

data sharing for purposes that relate to or could jeopardise national security, including the prevention or commission of terrorism and espionage. The minister may also preclude additional purposes through a rule making power to address any future risks that may emerge.[14]

2.16 Participants in the data sharing scheme are known as 'data scheme entities' (see clause 11 of the bill), of which there are three categories as detailed in Table 2.1

Table 2.1 Data scheme entities

Data custodians	Commonwealth bodies that control public sector data and have the right to deal with that data.
Accredited users	Entities accredited by the commissioner to access public sector data. To become accredited, entities must satisfy the security, privacy, infrastructure and governance requirements set out in the accreditation framework. Entities can be from all levels of government, as well as industry, research and others in the private sector. Accreditation is not limited to Australian entities to encourage international cooperation on projects in the public interest (with appropriate controls in place).
Accredited data service providers (ADSPs)	Entities accredited by the commissioner to perform data services such as data integration. Government agencies and users will be able to draw upon an ADSP's expertise to help them share and use data safely.

Source: Data Availability and Transparency Bill 2020, Explanatory Memorandum, pp. 3-4; Data Availability and Transparency Bill (Consequential Amendments) Bill 2020, Explanatory Memorandum, p. 5.

[14] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 6.

2.17 Part 5.2 of the bill relates to the accreditation framework of the data sharing scheme. Users and data service providers must be accredited by the commissioner before they can access shared data. The process involves the assessment of prospective recipients of data against criteria set out in the bill. The accreditation seeks to:

- ensure that data recipients are capable of managing the data accountably;
- minimise the risks of unauthorised access; and
- ensure that only users who comply with obligations under the bill can seek access to data.[15]

2.18 The commissioner may also receive security advice, including security assessments from ASIO,[16] about applicants seeking accreditation in order to assist them to make an informed accreditation decision. Additionally, the commissioner will be able to control systemic and entity-specific risks by putting conditions on, suspending, or cancelling accreditation for reasons of security or otherwise as provided by the accreditation framework.[17]

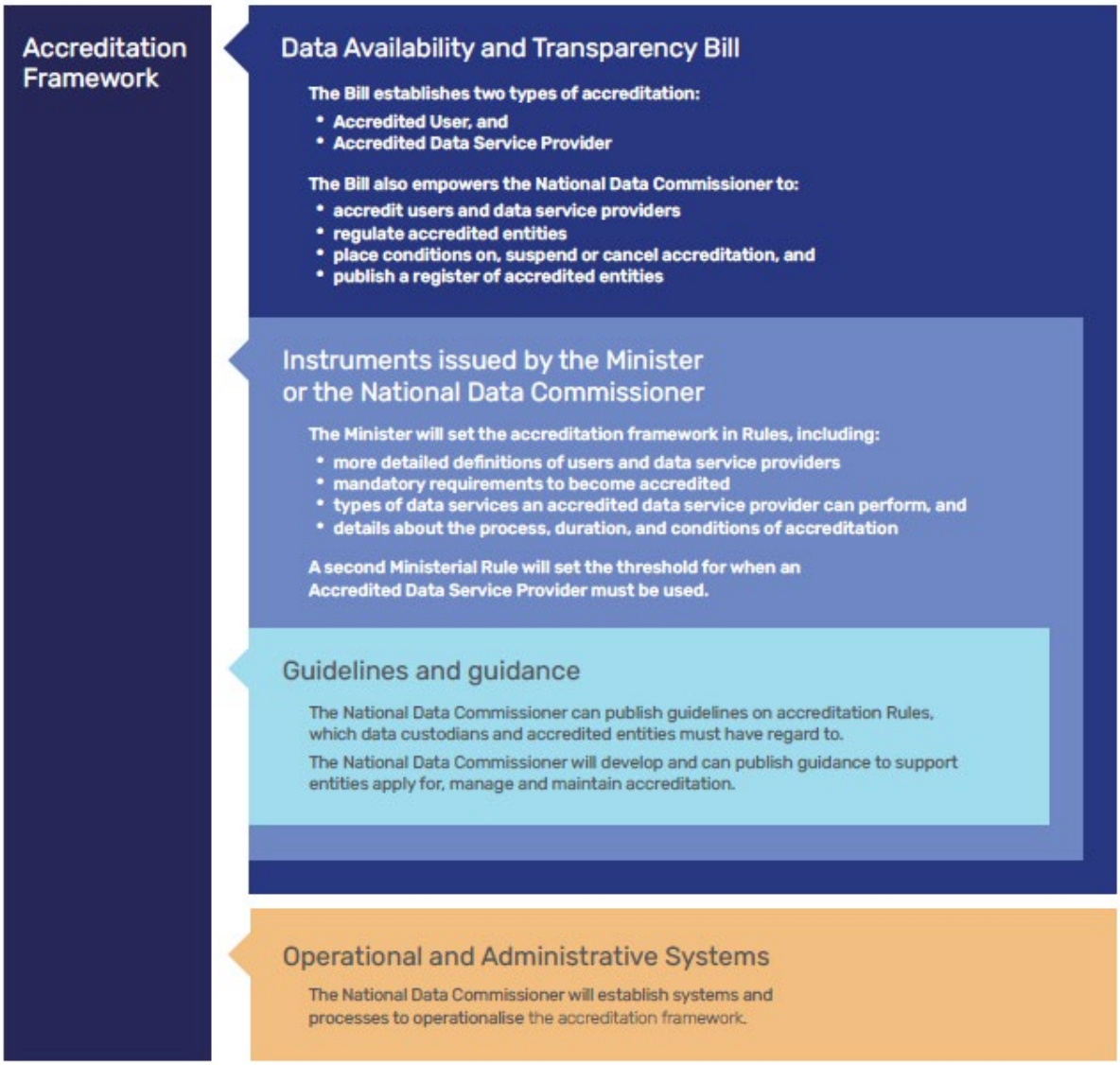
2.19 As set out in the following graphic, the legal framework for accreditation will be drawn from the bill and the specific details will be contained in legislative instruments issued by the minister or commissioner.

[15] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 7.

[16] Office of the National Data Commissioner, additional information received 22 April 2021, p. 2.

[17] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 7.

Figure 2.1 Accreditation framework



[Source: Department of the Prime Minister and Cabinet, Accreditation Framework – Discussion Paper, 2020, p. 4.]

2.20 Accreditation does not guarantee that data will be shared. This is because data custodians must be satisfied that any data sharing meets the requirements of the bills before making the final decision on whether or not to share data with accredited entities.[18]

2.21 A graphical representation of the key controls included in the bill was tabled by the ONDC at the public hearing on 20 April, and can be found at Appendix 1.[19]

---

[18] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 7.

[19] Office of the National Data Commissioner, *How will the Data Availability and Transparency Act work?*, April 2021, p. 1 (tabled 20 April 2021).

Data sharing principles

2.22 Once a data custodian is satisfied a proposed project is for a permitted purpose, the data sharing principles must be applied to assess and control risks of sharing 'in a holistic manner'. The principles are a framework for best practice risk management, enabling parties to adapt controls to suit the needs and context of each sharing arrangement.[20]

2.23 The principles are set out in clause 16 of the bill and are structured to manage risks arising across five key elements of the sharing process – project, people, settings, data, and outputs:

- The **project principle** considers the intended use of the shared data, including public interest, consent and ethics requirements.
- The **people principle** considers users accessing the data to ensure they can be trusted and have the right skills for the project.
- The **settings principle** assesses if data is shared in a controlled environment tailored to the data type and sensitivity, subject to security standards.
- The **data principle** requires data to be protected, including taking a 'data minimisation' approach so only data that is reasonably necessary to achieve the project is shared.
- The **outputs principle** ensures the results and outcomes of the projects are agreed, including whether they are appropriate for publishing.[21]

2.24 Controls set to manage risk within each principle can be 'dialled up or down' to suit the overall needs of each project.[22]

Data sharing agreements

2.25 Clauses 18, 19 and 20 of the bill go to details relating to data sharing agreements. Once a data sharing request is accepted, an accredited entity or ADSP needs to enter into a data sharing agreement with the data custodian that documents how the data will be used and shared. The bill sets out the mandatory terms that must be included in the agreement, which include how the project serves the public interest. These mandatory terms are designed to support robust and accountable sharing practices.[23]

2.26 Mandatory terms of data sharing agreements made under the data sharing scheme will be included in a publicly available register.[24] This will provide the

---

[20] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 8-9.

[21] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 8–9.

[22] Office of the National Data Commissioner, *Submission 20*, p. 6.

[23] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 27–28.

[24] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 27–28.

public with information about what data is being shared and why, who is accessing data, and how it is being safely shared.[25]

Oversight of the data sharing scheme and avenues for redress

2.27 As set out in Part 4.2, the bill will create a new independent regulator, the National Data Commissioner.[26] The commissioner's role is to regulate and oversee the data sharing scheme, with the position modelled on other regulators such as the Australian Information Commissioner.[27]

2.28 As regulator, the commissioner will provide advice, advocacy and guidance to ensure the scheme operates as intended. The commissioner will also work with data scheme entities to build data capability, promote best practice data sharing and use, and address cultural barriers to sharing.[28]

2.29 Part 5.3 of the bill relates to complaints under the scheme. The bill provides means for data scheme entities to raise issues about breaches or decisions under the data sharing scheme. For example, a complaints mechanism will enable data scheme entities to complain to the commissioner about potential breaches of the legislation, and this will trigger the commissioner's regulatory powers to investigate and address the situation.[29]

2.30 Existing avenues for redress in other schemes will continue to be available, including where the situation involves sharing or shared data. As the EM to the bill explained:

> For example, a person affected by a decision based on shared data may seek review of that decision, where legislation governing that decision sets review rights. A person may also complain about government activities to the Commonwealth Ombudsman, to other Ombudsmen and regulators, or to the Australian Information Commissioner about suspected mishandling of their personal information.[30]

2.31 Clause 28 of the bill ensures that when personal information is shared, affected individuals will have the means to seek recourse if their information is dealt with in a way contrary to the law. This may include through the *Privacy Act 1988* or equivalent state or territory law.[31]

---

25 Office of the National Data Commissioner, *Submission 20,* p. 6.

26 An Interim National Data Commissioner was appointed on 9 August 2018. When the bill becomes law, a National Data Commissioner will be appointed as an independent statutory office holder.

27 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 3.

28 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 8.

29 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 8.

30 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 8–9.

31 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 33.

2.32 Part 5.4 of the bill establishes mechanisms for the commissioner to monitor and gather information about the operation of the scheme and the entities participating in it.[32] The commissioner can conduct assessments and investigations to determine whether an entity is breaching or has breached requirements under the scheme. This may occur in response to complaints or the commissioner's own initiative. [33]

2.33 Part 5.5 of the bill provides the regulatory powers to monitor and enforce the requirements of the data sharing scheme.[34] A range of mechanisms are contained in the bill to deter and address non-compliance, which are modelled on the powers available to other regulators with similar mandates. Options available to the commissioner to deal with a non-compliant entity include:

- entering into an enforceable undertaking with an entity;
- issuing a direction for an entity to comply;
- seeking a civil penalty; and
- investigating possible criminal offences.[35]

Consequential amendments bill

2.34 The consequential amendments bill operates in conjunction with the principal bill and amends relevant Commonwealth legislation to control for security risks and ensure that the principal bill operates as intended.[36]

2.35 Specifically, the consequential amendments bill makes amendments to:

- Part IV of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to allow the Australian Security Intelligence Organisation (ASIO) to provide advice in relation to the exercise of a power under Part 5.2 of the principal bill, and to limit the notice and review processes for foreign entities in relation to security assessments.
- Schedule 1 of *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) to exclude the commissioner's accreditation decisions made on the basis of an ASIO security assessment for foreign entities from judicial review under the ADJR Act.
- Section 7 of the *Freedom of Information Act 1982* (FOI Act) to clarify the interaction between the FOI Act and the principal bill and preserve, to the extent possible, the intended operation of both schemes.

---

[32] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 57.

[33] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 58–59.

[34] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 59.

[35] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 8.

[36] Data Availability and Transparency (Consequential Amendments) Bill 2020, *Explanatory Memorandum*, p. 5.

- Section 50 of the *Privacy Act 1988* (Privacy Act) to enable the Australian Information Commissioner to transfer complaints to the commissioner where appropriate.[37]

[37] Data Availability and Transparency (Consequential Amendments) Bill 2020, *Explanatory Memorandum*, p. 5.

Chapter 3
Examination by the Senate Standing Committee for the Scrutiny of Bills

3.1 Pursuant to Senate Standing Order 25(2)(A), this chapter of the report will take into account comments published by the Standing Committee for the Scrutiny of Bills (Scrutiny committee).

3.2 The Scrutiny committee examined the Data Availability and Transparency Bill 2020 (the bill) in its Scrutiny Digest 1 of 2021, where it raised a number of concerns and requested further information from the minister. It further considered the bill in its Scrutiny Digest 3 of 2021 and Scrutiny Digest 5 of 2021, taking into account the responses provided by the minister.[1]

3.3 The Scrutiny committee voiced concerns that the bill may:

- trespass on personal rights and liberties;
- insufficiently define administrative powers; and
- inappropriately delegate legislative powers.[2]

3.4 The concerns raised by the Scrutiny committee can be broadly grouped under the following five categories:

- privacy;
- significant penalties;
- significant matters in delegated legislation;
- broad delegation of investigatory powers; and
- reversal of evidential burden of proof.

3.5 This chapter will now provide an overview of each of the concerns raised, as well as the responses from the then minister, the Hon. Stuart Robert MP, to those concerns.

Privacy

3.6 The Scrutiny committee considered that the data sharing scheme has the potential to trespass on an individual's right to privacy, given that it enables the sharing of data including 'personal information' and 'sensitive information' as defined by the *Privacy Act 1988* (Privacy Act).[3]

---

1 A number of submitters to the inquiry referenced the Scrutiny committee's views. More detail is available in Chapter 5 of this report.

2 Senate Standing Committee for the Scrutiny of Bills, *Index of Bills Considered by the Committee, as at 24 February 2021*, p. 2.

3 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 4.

3.7 It set out three core areas of concern, each relating to the intention of the bill to include significant matters in delegated legislation:

(1) the data sharing principles;

– standard of consent for sharing
– lack of definition of 'public interest'
– reliance on 'data codes'

(2) the scope of the scheme (data sharing purposes and receiving entities); and
(3) the review and complaint mechanisms.

3.8 Each of these will be examined in turn.

Data sharing principles

3.9 The Scrutiny committee's concerns around the data sharing principles can be further broken down into three issues:

- standard of consent for sharing;
- lack of definition of 'public interest'; and
- reliance on 'data codes'.

Standard of consent for sharing (definition of 'unreasonable or impracticable')

Context

3.10 Clause 16 of the bill establishes data sharing principles (based on the internationally recognised 'five safes' framework) which are intended to manage the risks of sharing public sector data. These principles were detailed in Chapter 2 of this report.

3.11 The principles are structured to support data custodians to consider the risks arising across five key elements of the sharing process:

(1) the proposed project;
(2) the setting in which the data is shared and accessed;
(3) the persons involved;
(4) the data involved; and
(5) the outputs involved.[4]

3.12 Where the data being shared includes personal information, paragraph 16(2)(c) requires consent for sharing to be sought from the individuals concerned, unless it is 'unreasonable or impracticable' for the data scheme entities to do so.[5]

---

4 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 4.

5 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 4.

3.13 The explanatory memorandum (EM) explained that the standard of consent required is that set by the Privacy Act, and that the 'unreasonable or impracticable' language is drawn from section 16A of that Act. It also noted that the standard should be 'interpreted using relevant guidance on consent made by the Australian Information Commissioner'.[6]

3.14 The EM further detailed:

> The question of whether seeking consent is reasonable or impracticable may depend on the amount, nature and sensitivity of the data involved, and whether individuals gave informed consent for uses including the proposed sharing at the point the data was originally collected. Where it is unreasonable or impracticable to seek consent, parties must still consider implementing other controls to protect privacy, under this and other data sharing principles.[7]

Concerns

3.15 In regard to this, the Scrutiny committee voiced concern that there was a 'significant amount of flexibility' in the meaning of 'unreasonable or impracticable' in that context, and that this may undermine the effectiveness of clause 16 as a safeguard against undue trespass on the privacy of individuals whose data may be shared under the scheme.[8]

3.16 The Scrutiny committee also noted that, while the data sharing principles contemplate minimising the sharing of personal information as far as possible and sharing only the data reasonably necessary to achieve an applicable purpose, there are no requirements for sharing only de-identified data in the principles or elsewhere in the bill.[9]

Lack of definition of 'public interest'

Context

3.17 The Scrutiny committee observed that paragraph 16(2)(a) requires a judgement to be made about whether the sharing can be reasonably expected to serve the public interest. It highlighted that 'public interest' is not defined in the bill, and the EM does not provide guidance about the factors that might be considered when evaluating public interest for the purposes of data sharing.[10]

---

6 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 22.

7 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 24.

8 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 5.

9 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 5.

10 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 5.

Concerns

3.18 The Scrutiny committee stated:

> In contexts where commercial and economic interests may be considered to factor into the 'public interest', the committee is concerned that privacy interests are not clearly central to the operation of the scheme.[11]

Reliance on data codes

Context

3.19 The Scrutiny committee noted that the application of the data sharing principles will be clarified in 'data codes' – legislative instruments made by the National Data Commissioner (commissioner) that serve as binding codes of practice for the data sharing scheme.[12]

Concerns

3.20 The Scrutiny committee stated:

> The committee's view is that significant matters, such as privacy safeguards for data sharing, should be included in primary legislation unless a sound justification for the use of delegated legislation is provided. In this instance, while the explanatory memorandum explains the approach of using legislative instruments rather than regulations to establish data codes, there is no explanation of why these matters cannot be included in primary legislation.[13]

Scope of scheme – data sharing purposes and receiving entities

Context

3.21 Clause 15 establishes the three permitted data sharing purposes:

- delivery of government services;
- informing government policy and programs; and
- research and development.[14]

3.22 These purposes are not specifically defined; rather, the EM emphasised that the purposes are to 'construed broadly'.[15]

Concerns

3.23 The Scrutiny committee identified that a broad construction of the permitted purposes for data sharing 'risks interpretations which may unduly trespass on privacy'. While acknowledging that the bill seeks to manage this risk through

---

[11] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 5.

[12] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 5.

[13] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 6.

[14] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 6.

[15] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 22.

paragraph 15(2)(c) by enabling the minister to make rules prescribing 'precluded purposes', it indicated it did not consider this to be satisfactory. It stated:

> …the committee's view is that significant matters, such as privacy safeguards and the permissible scope for sharing personal information, should be included in primary legislation unless a sound justification for the use of delegated legislation is provided. In this instance, the explanatory memorandum states that 'this approach is intended to manage unintended expansions or interpretations of clause 15, and to ensure the scheme continues to operate as intended and in line with community expectations'.[16]

3.24 The Scrutiny committee also emphasised that its scrutiny concerns in this regard were heightened by the breadth of the application of the bill, in particular that data may be shared with private sector entities with no requirements that the safeguards that apply to, for example, university research, apply to these entities.[17]

Summary of concerns

3.25 Given the potential impact on an individual's right to privacy as a result of the use and disclosure of personal information under the data sharing scheme, the Scrutiny committee requested the minister's advice as to whether the bill could be amended to:

- include a public interest test which prioritises privacy interests in decision-making under the scheme;
- provide guidance on the face of the bill about the circumstances in which it will be 'unreasonable or impracticable' to seek an individual's consent for sharing their personal information;
- require that, where possible, data that includes personal information be shared in a de-identified way;
- clarify the scope of the permitted data sharing purposes, and include guidance on the face of the bill about precluded purposes; and
- provide minimum standards for ethics approvals for private entities seeking to use data that includes personal information.[18]

Minister's response

3.26 The minister responded to the Scrutiny committee's concerns. The Scrutiny committee considered the minister's advice and outlined its concluding views in Scrutiny Digest 3 of 2021 and Scrutiny Digest 5 of 2021, as detailed below.

---

[16] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 6.

[17] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 6.

[18] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 7.

Requests to include a public interest test which priorities privacy interests, provide guidance on the face of the bill about 'unreasonable or impracticable' exception, and clarify the scope of the permitted data sharing purposes

3.27 The minister advised that questions of whether a project can reasonably be expected to serve the public interest and questions in relation to consent requirements must be resolved on a project-by-project basis.[19]

3.28 He also advised that the bill's intended approach is to ensure privacy interests are appropriately balanced with the public interest of a project, rather than assuming that one must prevail at the expense of the other, and that this approach is consistent with the objects of the Privacy Act.[20]

3.29 The minister further noted that he is 'open to giving consideration' to amendments to the bill to require that the National Data Commissioner (commissioner) must issue guidance on certain matters, including application of the data sharing principles, in consultation with relevant entities. The Scrutiny committee welcomed this advice.[21]

3.30 The minister also advised that he did not consider the level of detail to be included in the guidelines appropriate for inclusion in primary legislation, but acknowledged the importance of striking a balance between flexibility and parliamentary scrutiny.[22] The Scrutiny committee did not accept this response, and reiterated its concerns that the guidelines will be established in non-legislative instruments that are not subject to tabling or scrutiny by the Parliament.[23]

3.31 As a result, the Scrutiny committee requested that an addendum to the EM containing the key information provided by the minister in response to its concerns be tabled in Parliament as soon as is practicable.[24]

3.32 The minister's response did not provide a direct response as to the Scrutiny committee's request that he provide guidance on the face of the bill about the circumstances in which it will be 'unreasonable or impracticable' to seek an

---

[19] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 16.

[20] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 16.

[21] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 14.

[22] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 14.

[23] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p.16.

[24] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 16–17.

individual's consent for sharing their personal information. Rather, the response reiterated the information set out in the EM.[25]

3.33 The Scrutiny committee stated that it remained concerned about the breadth of the 'unreasonable or impracticable' exception to the requirement to secure consent from an individual prior to sharing their personal information, in particular given the minister's advice that privacy interests will not be given priority in the public interest test.[26]

3.34 As a result, the committee requested the minister's further advice as to:

- whether the addendum to the EM can provide specific examples of current guidance on the meaning of 'unreasonable or impracticable' and provide information on where this current guidance can be accessed; and
- why it is considered necessary and appropriate for guidelines on aspects of the data sharing scheme (which may play an important role in minimising the risk of interpretations of the operation of the scheme that trespass on personal privacy) to be included in non-legislative instruments that are not subject to parliamentary scrutiny.[27]

3.35 In response to these two requests, the minister advised that he had approved an addendum to the EM to address the concerns of the Scrutiny committee, and that he would arrange for the addendum to be tabled in the House of Representatives 'as soon as practicable'.[28]

3.36 In regard to the proposed addendum, the minister advised that it would include further information about the meaning of the expression 'unreasonable or impracticable' in the context of clause 16(2)(c) of the bill, as well as information on where to locate guidance issued by the Australian Information Commissioner (AIC) on privacy and consent matters.[29]

3.37 In regard to the Scrutiny committee's request as to why it is necessary and appropriate for guidelines on aspects of the data sharing scheme to have the status of non-legislative instruments (and therefore not be subject to parliamentary scrutiny), the minister advised:

> The Bill establishes a framework of resources, of scaled legal weight, to assist its interpretation and application. These resources range from fact sheets, guidelines on aspects of the Bill which entities must have regard to

---

[25] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 13.

[26] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

[27] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

[28] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5 of 2021*, 17 March 2021, p. 36.

[29] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5 of 2021*, 17 March 2021, p. 36.

> when engaging with the sharing scheme, to legislative instruments subject to Parliamentary scrutiny that set binding legal requirements.
>
> I consider this scaled approach to be reasonable, and necessary to achieve the desired outcome of supporting both best practice data sharing and a graduated approach to enforcing compliance with the Bill. This approach is consistent with that of other principles-based legislative schemes, in particular the AIC's powers and framework of instruments to support understanding of, and compliance with, privacy law.[30]

3.38 The minister also noted that, from the AIC's experience, it is desirable from a regulatory perspective to have guidelines which entities must regard as an interim step between general guidance and legislative instruments. He explained:

> Learning from this [AIC] experience, the approach taken in the Bill enables the National Data Commissioner to produce both informal guidance material, and more formal "guidelines". Scheme entities must have regard for the guidelines however they are not binding. The guidelines do not alter the law but provide clear guidance from the Commissioner about their view of law applied and better practice. It is not appropriate for such guidance to be disallowable. Data codes made by the Commissioner, and rules made by the Minister, are binding on scheme entities and are legislative instruments subject to disallowance.[31]

3.39 The Scrutiny committee noted this advice, but reiterated its concerns that the guidelines may play an 'important role' in minimising the risk of interpretations of the operation of the scheme that may trespass on personal privacy.[32]

3.40 It reiterated its view that significant matters, such as the application of privacy safeguards for data sharing, may be more appropriately provided for in delegated legislation that is subject to scrutiny and disallowance.[33]

3.41 The Scrutiny committee drew its concerns on the matter to the attention of the Senate.[34]

Request to amend the bill to provide that, where possible, personal information is shared in a de-identified way

---

30 Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2021, 17 March 2021, p. 36.

31 Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2021, 17 March 2021, p. 37.

32 Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2021, 17 March 2021, p. 37.

33 Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2021, 17 March 2021, p. 38.

34 Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 of 2021, 17 March 2021, p. 38.

3.42 The minister advised that under the data principles, custodians must only share data that is reasonably necessary for the relevant data sharing purpose, and that this requirement is complemented by a requirement to minimise the sharing of personal information as far as possible without compromising the data sharing purpose.[35]

3.43 The minister also advised that the term 'de-identified' is not used in the data principle to ensure that the bill remains 'technology-neutral'.[36]

3.44 The Scrutiny committee acknowledged the advice, but stated that it remained concerned about the absence of an explicit requirement in the bill that, where possible, sharing of data is done in a way that does not allow an individual to be identified.[37]

3.45 It drew its concerns on this matter to the attention of the Senate.[38]

Request to amend the bill to provide minimum standards for ethics approvals for private entities seeking to use data that includes personal information

3.46 The minister advised that paragraph 16(2)(b) of the bill requires data scheme entities to observe any applicable ethics processes, and that the bill leverages existing frameworks to ensure that projects and research in specific fields meet accepted ethical standards. The minister noted that this requirement imposes a minimum standard for ethics approvals for all data scheme entities, irrespective of sector.[39]

3.47 The minister also advised that data custodians may require ethics processes in circumstances where no ethic processes would ordinarily apply, and that this constituted 'an added safeguard'.[40]

3.48 While noting the advice, the Scrutiny committee stated that it remained concerned that the ability to require a private entity who is otherwise not subject to existing ethics processes to undertake such processes was

---

35 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 14.

36 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 14.

37 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

38 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

39 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

40 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 15.

discretionary, with the decision to set this requirement being left to the various Commonwealth bodies empowered to share data under the bill.[41]

3.49 It drew its concerns on the matter to the attention of the Senate.[42]

Review and complaint mechanisms

Context

3.50 Decisions about data sharing made by Commonwealth bodies that are data custodians under the bill are not subject to internal or external merits review under the data sharing scheme. As the EM sets out:

> Data sharing decisions by data custodians will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data.[43]

Concerns

3.51 The Scrutiny committee raised concerns with this approach:

> Noting that privacy interests may be affected by decisions made by data custodians under the scheme, it is not clear to the committee why individuals whose privacy interests may be affected should not have access to merits review. The committee notes that, as many decisions under the scheme will affect individual interests as a class, most individuals will be excluded from the initial decision making process.[44]

3.52 It also identified that the lack of clarity around certain terms in the data sharing principles and purposes (as discussed above) clearly illustrate the broad scope for discretionary decision making by the data custodians. It continued:

> The committee is concerned that there is a risk that individuals' interests in their personal information being kept private may not be given sufficient weight in an evaluation of public interest. Further, it does not appear that the Commonwealth entity making initial decisions with respect to sharing of data must consult experts or seek other external input.[45]

3.53 The Scrutiny committee also observed that under the complaints mechanism established in Division 1 of Part 5.3, only data scheme entities may make a complaint about data sharing decisions. The EM stated that other entities could

---

41 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

42 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 17.

43 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 8.

44 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 15.

45 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 7.

instead complain through 'existing legal mechanisms' and set out the example of a person complaining to the AIC about the mishandling of their personal information under the Privacy Act.[46]

3.54 The Scrutiny committee commented that it was unclear why persons with privacy complaints must make a complaint through a separate mechanism and stated:

> The committee is concerned that establishing a narrowly focused complaints mechanism may result in the Data Commissioner rarely or never hearing privacy complaints, which may result in privacy concerns not being given adequate consideration in decision making under the scheme.[47]

3.55 The Scrutiny committee also drew attention to the fact that much of the detail about the complaints process is not contained in the bill but left to data codes (i.e. legislative instruments made by the commissioner).[48]

3.56 In light of these concerns, the Scrutiny committee requested the minister's advice as to why individuals whose privacy interests may be affected by the data sharing scheme should not have access to merits review and the dedicated complaints process established in the bill.[49]

Minister's response

3.57 In response, the minister advised the following:

- That individuals with privacy concerns will have access to existing complaints and administrative review processes (including the complaints mechanism under the Privacy Act and where relevant, the complaints mechanisms in relation to state or territory privacy regulators).[50]
- That the commissioner may conduct 'own-motion' investigations into potential breaches in response to a 'tip-off' from the public or media.[51]
- That other redress options to address concerns unrelated to privacy (such as judicial review or complaining to the Commonwealth Ombudsman) were available.[52]

---

46 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 55.

47 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 8.

48 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 8.

49 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 8.

50 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 19.

51 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 19.

52 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 19.

- That merits review of substantive decisions based on shared data that has 'exited' the scheme may be available, if provided for by the legislation under which the decision was made. These frameworks would have their ordinary operation, without being replicated in the bill.[53]
- That the bill includes mechanisms to facilitate 'regulatory cooperation' which will allow for monitoring of systemic privacy breaches.[54]

3.58 The Scrutiny committee acknowledged this advice but reiterated its concerns and drew particular attention to clause 21 of the bill:

> While also noting the minister's advice in relation to the requirements in subclauses 21(1) and (2) that personal information in the scheme must be validated or corrected by the individual before it can 'exit' the scheme, the committee notes that paragraph 21(1)(b)(iii) also permits data as 'output' to be shared in circumstances prescribed by the rules. While the explanatory memorandum states that any such rules created must be consistent with the bill, the committee is concerned that allowing delegated legislation to expand the circumstances in which output may be shared may undermine the value of this measure as a safeguard as described in the minister's response.[55]

3.59 It continued:

> Further, while noting the minister's advice in relation to the mechanisms for regulatory cooperation and requirements to notify the Commissioner of data breaches, the committee remains concerned that the bill does not require any information to be given to the Commissioner with respect to complaints received by the Australian Information Commissioner, or other bodies who may receive complaints about the scheme, such as the Commonwealth Ombudsman, or Commonwealth entities acting as data custodians within the scheme. In raising this scrutiny concern, the committee notes 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.[56]

3.60 The Scrutiny committee drew its concerns on the matter to the attention of the Senate.[57]

---

[53] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 19.

[54] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 19–20.

[55] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 20.

[56] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 20.

[57] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 20.

Significant penalties

Context

3.61 Clause 14 of the bill creates new criminal offences for unauthorised sharing and unauthorised collection or use. The maximum penalty for both offences is imprisonment for two years. Additionally, subclause 104(3) also creates an offence for failing to comply with a notice to provide information or documents to the commissioner, which is subject to a maximum penalty of imprisonment for 12 months.[58]

3.62 The Scrutiny committee's expectation is that the rationale for the imposition of significant penalties, especially if those penalties involve imprisonment, will be fully outlined in the EM. In particular, it expects that penalties should be justified by reference to similar offences in Commonwealth legislation, as this not only promotes consistency, but guards against the risk that liberty of the person is unduly limited through the application of disproportionate penalties.[59]

Concerns

3.63 The Scrutiny committee expressed dissatisfaction with the rationale and level of detail provided in the EM about the offences and penalties. It concluded:

> The committee acknowledges the importance of providing robust safeguards against the misuse of data under the new scheme, and notes that other Commonwealth legislation imposes comparable penalties for offences relating to the use and disclosure of sensitive data. However, given the significance of the penalties that may be imposed under proposed clauses 14 and 104 the committee would expect a comprehensive justification for the penalty in each of those provisions to be included in the explanatory memorandum.[60]

3.64 It drew its scrutiny concerns to the attention of the Senate.[61]

Significant matters in delegated legislation

Context

3.65 The bill contains multiple clauses (77, 86, 137 and 139) that provide for matters relating to the accreditation of entities under the data sharing scheme to be detailed in the rules (that is, in delegated legislation). For example, clause 86 of the bill enables rules to be prescribed for the accreditation framework,

---

58 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 8.

59 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, pp. 8–9.

60 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 9.

61 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 9.

providing for procedures, requirements and any other matters relating to the accreditation of entities for the purposes of the data sharing scheme.[62]

Concerns

3.66 The Scrutiny committee's view is that such 'significant matters' (such as the accreditation of entities for the purposes of sharing public sector data) should be included in primary legislation, unless a sound justification for the use of delegated legislation is provided. It highlighted that the EM for the bill contains no such justification for any of the clauses in question.[63]

3.67 It further observed:

> The committee's scrutiny concerns in this regard are heightened by the extent to which the bill relies on delegated legislation to determine the scope and operation of the data sharing scheme, especially in relation to privacy protections…[64]

3.68 The Scrutiny committee therefore requested the minister's advice as to:

- why it is considered necessary and appropriate to leave procedures, requirements and other matters relating to the accreditation of entities for the purposes of the data sharing scheme to delegated legislation; and
- whether the bill could be amended to include 'at least high-level guidance' regarding these matters on the face of the primary legislation.[65]

Minister's response

3.69 In response to the first matter, the minister advised that the approach of providing for three types of legislative instruments in the bill 'helps to ensure the scheme can adapt to emerging technologies and future needs over time, while allowing for oversight through the disallowance process'.[66]

3.70 The minister also advised that the approach taken to allowing rules to provide for procedures, requirements and any other matters relating to accreditation

---

62 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

63 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

64 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

65 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

66 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 21.

aligns with the Legislative Handbook issued by the Department of the Prime Minister and Cabinet.[67]

3.71 The minister concluded that he did 'not consider it necessary to include further guidance on accreditation matters on the face of the bill'. He contended that as the weight of the accreditation framework was already located in Part 5.2 of the bill, significant matters would not be left to delegated legislation, and that where the bill does provide for delegated legislation, it is aligned with standard drafting practices to balance legal certainty and flexibility.[68]

3.72 The Scrutiny committee was not satisfied with the responses and reiterated its concerns:

> …noting the importance of ensuring that the accreditation framework only permits accreditation of entities who can safely handle public sector data, from a scrutiny perspective, the committee remains concerned about the extent to which the bill relies on delegated legislation to determine matters related to the accreditation of entities under the scheme.[69]

3.73 As a result, the Scrutiny committee:

- drew its concerns to the attention of the Senate;
- requested an addendum to the EM containing the key information provided by the minister relating to the expected content of the Accreditation Rules be tabled in Parliament as soon as practicable, noting the importance of these explanatory materials as a point of access to understanding the law, and if needed, as extrinsic material to assist with interpretation; and
- drew its concerns to the attention of the Senate Standing Committee for the Scrutiny of Delegated Legislation.[70]

Broad delegation of investigatory powers

Context

3.74 Clauses 109 and 110 of the bill seek to trigger the monitoring and investigation powers under the *Regulatory Powers (Standard Provisions) Act 2014*. Specifically, subclauses 109(4) and 110(3) provide that an authorised person may be

---

[67] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 21.

[68] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 22.

[69] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 23.

[70] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 23.

assisted by 'other persons' in exercising powers or performing functions or duties in relation to monitoring and investigation.[71]

3.75 The EM does not contain any information on the categories of 'other persons' who may be granted such powers, and the bill does not confine who may exercise the powers by reference to any particular expertise or training.[72]

Concerns

3.76 The Scrutiny committee reiterated that its consistent position in relation to the exercise of coercive or investigatory powers is that persons authorised to use such powers should have the appropriate training and expertise.[73]

3.77 It therefore requested the minister's advice as to:

- why it is considered necessary and appropriate to allow any 'other person' to assist an authorised person in exercising monitoring and investigatory powers; and
- whether the bill can be amended to require that any person assisting an authorised person have the knowledge and expertise appropriate to the function or power being carried out.[74]

Minister's response

3.78 In response, the minister advised that the clauses in question adopt the standard suite of provisions under the *Regulatory Powers (Standard Provisions) Act 2014*, and that this is the 'accepted baseline of powers' required for an effective monitoring, investigation or enforcement regulatory regime, while providing adequate safeguards and protecting important common law privileges.[75]

3.79 The minister also advised that staffing provisions in the bill will ensure that 'other persons' at commissioner's disposal will have the appropriate knowledge, training and expertise in the exercise and performance of investigatory powers and functions.[76]

---

[71] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

[72] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

[73] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

[74] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

[75] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 24.

[76] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 24.

3.80 The minister further advised that:

- persons assisting must act under the direction of the commissioner as an authorised person;
- any valid actions of the person assisting will be taken to be those of the commissioner; and
- as persons employed or engaged by an Australian Public Service (APS) department, assisting individuals would be further subject to standard accountability measures (e.g. the APS Code of Conduct for staff and the Commonwealth Procurement Rules for contractors), as well as security clearances and other pre-employment screening procedures.[77]

3.81 The minister explained that, for the stated reasons, the bill and the *Regulatory Powers (Standard Provisions) Act 2014* already give effect to the committee's suggested drafting changes to clauses 109 and 110.[78]

3.82 The Scrutiny committee did not accept this reasoning and concluded:

> ….there is nothing on the face of the bill to limit the use of 'other persons' to assist the Commissioner as set out in the response. In particular, it appears that there is no requirement on the face of the bill that 'other persons' assisting an authorised person must be the staff, consultants or contractors to which clauses 47 to 49 of the bill refer. The committee reiterates its consistent scrutiny view in relation to the exercise of coercive or investigatory powers that persons authorised to use such powers should have appropriate training and experience.[79]

3.83 The Scrutiny committee drew its concerns on the matter to the attention of the Senate.

Reversal of evidential burden of proof

Context

3.84 Clause 136 of the bill establishes the geographic jurisdiction of civil penalty provisions and offences in the bill. It does so by providing that the bill may apply extraterritorially where there is a sufficient link between Australia and the matter in order to establish the commissioner's jurisdiction.[80]

3.85 Subclauses 136(2) and 136(3) limit the geographic scope of the bill by providing defences for foreign entities, modelled on defences in section 15.2(2)

---

77 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 24–25.

78 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 24–25.

79 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 25–26.

80 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 11.

and (4) of the Criminal Code. Under subclause (2), a foreign entity will not be liable for contravening a civil penalty or criminal offence provision if there is no Australian connection (territorial or nationality) and the conduct is lawful in the foreign jurisdiction in which it occurred. Subclause (3) provides the same defence for an ancillary contravention or ancillary offence, where it relates to a primary contravention or offence which occurred outside of Australia.[81]

3.86 Subclause 136(4) sets out that a person that seeks to rely on these defences bears an evidential burden.[82]

Concerns

3.87 The Scrutiny committee observed that at common law it is ordinarily the duty of the prosecution to prove all elements of an offence. It wrote:

> This is an important aspect of the right to be presumed innocent until proven guilty. Provisions that reverse the burden of proof and require a defendant to disprove, or raise evidence to disprove, one or more elements of an offence, interferes with this common law right.[83]

3.88 In light of this, it continued on:

> While in this instance the defendant bears an evidential burden (requiring the defendant to raise evidence about the matter), rather than a legal burden (requiring the defendant to positively prove the matter), the committee expects any such reversal of the evidential burden of proof to be justified. [84]

3.89 The Scrutiny committee observed that the reasons for the reversals of the evidential burden of proof in clause 136 were not addressed in the EM. As a result, it requested the minister's advice as to why the bill proposes to use offence-specific defences (which reverse the evidential burden of proof) in this instance.[85]

Minister's response

3.90 In response, the minister advised that it is appropriate for the defendant to bear the evidential burden in these circumstances because evidence to establish whether:

---

81 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 78.

82 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 78.

83 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 11.

84 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 11.

85 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 11.

- the relevant conduct occurred wholly in a foreign country (but not on board an Australian aircraft or ship); and
- the defendant is not an Australian entity (as defined in clause 9 of the bill) is 'best able to be adduced by, and within the knowledge of, the defendant.' [86]

3.91 The minister also advised that evidence that suggests the reasonable possibility that the conduct in question is lawful in a foreign country is also best raised by the defendant, as:

- the defendant would have knowledge of that foreign jurisdiction; and
- and it would be significantly more difficult or costly for Australian-based prosecutors to bear this burden.[87]

3.92 Furthermore, the minister stated he was 'willing to consider' an addendum to the EM 'at an appropriate time' that incorporates the explanation he provided the Scrutiny committee.

3.93 The Scrutiny committee was satisfied with the minister's response, and therefore made no further comment on the matter. It did, however, request that an addendum to the EM containing the key information from the minister be tabled in the Parliament as soon as practicable.[88]

3.94 It made this request noting the importance of explanatory materials as a point of access to understanding the law, and if needed, as extrinsic material to assist with interpretation.[89]

---

[86] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 26–27.

[87] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 27.

[88] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 27.

[89] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 27.

Chapter 4
Examination by the Parliamentary Joint Committee on Human Rights

4.1 The Parliamentary Joint Committee on Human Rights (joint committee) examined the Data Availability and Transparency Bill 2020 (the bill) in its Report 2 of 2021, where it raised a number of concerns and requested further information from the minister. It further considered the bill in its Report 4 of 2021, taking into account the responses provided by the then minister, the Hon. Stuart Robert MP.

4.2 This chapter will provide an overview of each of the concerns raised by the joint committee, as well as the responses from the minister to those matters.

Right to privacy

4.3 In its Report 2 of 2021, the joint committee noted that the bill seeks to establish a legislative framework that overrides existing laws in order to facilitate the sharing of, and controlled access to public sector data held by Commonwealth bodies with accredited entities.[1]

4.4 It observed that, in doing so, the bill 'engages and limits' the right to privacy, while also noting that this right may be subject to 'permissible limitations' if they are shown to 'reasonable, necessary and proportionate'.[2]

Context

4.5 The joint committee stated that the right to privacy is 'multi-faceted' and comprises respect for informational privacy, including the right to respect for private and confidential information, particularly the storing, use and sharing of such information.[3]

4.6 The right also:

- prohibits arbitrary and unlawful interference with an individual's privacy, family, correspondence or home;
- includes a requirement that the state not arbitrarily interfere with a person's private and home life (meaning that an interference with a person's privacy – including one provided for by law – should be in accordance with the International Covenant on Civil and Political Rights and be reasonable in the particular circumstances);

---

1 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

2 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

3 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 7.

- includes the right to control the dissemination of information about one's private life;
- requires that States Parties take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it; and
- requires that legislation must 'specify in detail the precise circumstances' in which an interference with privacy will be permitted.[4]

4.7 The right to privacy may be subject to permissible limitations where the limitation:

- pursues a legitimate objective;
- is rationally connected to an objective; and
- is a proportionate means of achieving that objective.[5]

Concerns

4.8 The joint committee recognised that the data sharing scheme to be established by the bill is intended to facilitate greater data availability and use which could in turn support economic and research opportunities and streamline government service delivery. It acknowledged that these appear to be important objectives, particularly given the recent pressures on public service delivery following the 2020 bushfire season and COVID-19 pandemic.[6]

4.9 However, it identified that the statement of compatibility with human rights for the bill did not set out what objectives are sought to be achieved by the bill.

4.10 As a result, the joint committee considered that further information was required for it to assess whether the stated objectives constitute a legitimate objective for the purposes of international human rights law.[7]

4.11 It also submitted that while the statement of compatibility provides a list of safeguards with respect to the right to privacy, the extent to which the proposed scheme may limit the right to privacy is not made clear.[8]

4.12 In its Report 2 of 2021, the joint committee indicated that it had not yet formed a concluded view in relation to the matter and required further information to assess the compatibility of the bill with the right to privacy.[9]

4.13 As a result, it sought the minister's advice as to:

---

4 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 7.

5 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

6 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

7 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

8 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

9 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

(a) what is the specific objective the measure seeks to achieve, including what public or social concern the measure seeks to address, which is pressing and substantial enough to warrant limiting the right to privacy;
(b) why the Australian Federal Police (AFP) is not listed as an excluded entity under proposed subclause 11(3), noting that it is a law enforcement body;
(c) in what type of circumstances is it likely that data will be shared, or not shared, for a data sharing purpose (with examples provided as to what is, and is not, likely to be considered to be for 'the delivery of government services'; 'informing government policy and programs'; and 'research and development');
(d) what considerations would be considered relevant (and irrelevant) in an assessment of the 'public interest' for the purpose of proposed subclause 16(2), and why does the bill not specifically reference the need to consider the right to privacy;
(e) in what circumstances, and based on what factors, would it be considered unreasonable or impracticable (under proposed paragraph 16(2)(c)) to seek the consent of individuals whose personal information would be shared, and would the provision of any government service be contingent on the individual giving their consent to the proposed sharing of their data;
(f) whether and in what manner accredited entities would be subject to ongoing monitoring (or auditing) of their continued compliance with the data sharing scheme, and their suitability for continued accreditation;
(g) why the scheme would not permit an individual to complain to the National Data Commissioner (commissioner) about a matter associated with the data sharing scheme, such as to report a suspected breach or data misuse, or to express concerns as to the sharing or use of their data in a specific context;
(h) noting the requirement that the sharing of personal information be minimised as far as possible without compromising the data sharing purpose, in what circumstances would the data sharing purpose be compromised by not sharing personal information;
(i) in what circumstances does the bill provide, and is it intended that the rules will provide, that a data sharing agreement may allow the accredited user to provide shared output data to a third party, and what protections apply to protect personal privacy in such circumstances; and
(j) why other, less rights restrictive alternatives would not be effective to achieve the intended objectives (such as amendments to individual pieces of legislation to invoke this data sharing scheme which take into account the specific data to be shared and the specific circumstances in which it is appropriate to share such data).[10]

[10] Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, pp. 16–17.

Minister's response

4.14 In response to the joint committee's request for additional information, the minister advised that the bill constitutes a 'proportionate limitation on the right to privacy', given that it permits data sharing in a closely controlled, consistent and transparent manner, with a specific regulatory regime to ensure data sharing is undertaken safely.[11]

4.15 The minister addressed each of the joint committee's ten requests separately, with each response summarised briefly below.

(a) What is the specific objective of the bill?

4.16 The minister advised that the bill is designed to facilitate controlled access to public sector data for specific purposes in the public interest, with safeguards in place to mitigate risks. The minister also noted that limitations on data sharing in existing legislation are 'a constraint' that can be only be addressed by further legislation, such as the bill, stating:

> It would be impractical and cumbersome to amend every applicable statutory provision imposing limitations on the use and disclosure of data to achieve the public policy purpose of facilitating the benefits and outcomes of improved data sharing.[12]

(b) Why is the AFP not listed as an excluded entity?

4.17 The minister advised that the bill would enable the sharing, collection and use of public sector data by the AFP only for permitted purposes in the public interest, and that these would be described in publically available data sharing agreements. The minister emphasised that the bill excludes the sharing of the operational data of the AFP to protect the integrity and security of police operations, and provided the following example of how this could operate:

> For example, if it became an accredited user, the AFP could collect and use data to undertake research, or to inform policies and programs that are related to law enforcement (as distinct from policing activities that target particular individuals).[13]

(c) In what type of circumstances is it likely data will be shared or not shared?

4.18 The minister advised that the data sharing purposes set out in clause 15 of the bill reflect 'extensive public consultation' on appropriate uses of public sector data for the scheme and were considered as part of three independent Privacy Impact Assessments. The minister's response provided the following examples of activities that could fall under each of the three data sharing purposes:

---

[11] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 32.

[12] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 32.

[13] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 32.

(i) Delivery of government services

Sharing data for this purpose could enable the provision of better services, such as the delivery of new disaster relief payments, or grants of industry support payments.

(ii) Inform government policy and programs

Sharing for this purpose could help enable the discovery of trends and risks to inform public policymaking, enable modelling of policy and program interventions, and improve the quantity and quality of the data used by governments to inform public policy decisions.

(iii) Research and development

Sharing for this purpose could enable academics, scientists, and innovators in the public and private sectors to access public sector data to gain insights that could enhance Australia's socio-economic wellbeing.[14]

(d) What considerations would be considered relevant (and irrelevant) in an assessment of the public interest?

4.19 The minister advised that the question of whether a project can be reasonably expected to serve the public interest must be made on a project-by-project basis, weighing a range of factors for and against sharing. The minister noted that the factors will include:

- the impacts on an individual's right to privacy;
- the potential for serious harm to the public; and
- whether those impacts are 'reasonable, necessary and proportionate'.[15]

4.20 The minister also advised:

> The Bill's holistic approach ensures privacy interests are appropriately balanced with the public interest in a project, and does not explicitly reference privacy to avoid the implication that one most prevail at the expense of the other.[16]

(e) When would it be 'unreasonable or impracticable' to seek consent?

4.21 The minister advised that he proposed to table an addendum to the explanatory memorandum (in response to the observations of the Senate Standing Committee for the Scrutiny of Bills) in the Parliament 'as soon as practicable'. He noted that the addendum will outline 'key information and examples' about the meaning of 'unreasonable or impracticable' to help clarify the interpretation of paragraph 16(2)(c) of the bill, and that it would also direct users to relevant guidance issued by the Australian Information Commissioner (AIC) on the standard of consent.[17]

---

[14] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 33.

[15] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 33.

[16] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 33.

[17] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 34.

(f) Will accredited entities be subject to ongoing monitoring of their continued compliance with and suitability for participation in the data sharing scheme?

4.22 The minister advised that the bill proposes a range of responsibilities on accredited entities, such as complying with conditions of accreditation and reporting relevant changes. The minister noted that a condition of accreditation can be imposed requiring an entity to provide updated evidence at specific intervals to support the criteria for accreditation. The minister also stated that once the data sharing scheme commences, the commissioner will identify annual regulatory priorities in a Regulatory Action Plan, which will reflect areas where uncertainty, complexity or the risk of non-compliance may arise.[18]

(g) Why does the scheme not permit an individual to complain to commissioner about a matter associated with the data sharing scheme?

4.23 The minister advised that the bill's formal complaint mechanism is 'scheme-specific' to supplement existing redress mechanisms and 'reduce duplication and overlap'. He clarified that the complaints process in the bill is a 'highly structured' mechanism designed to resolve concerns held by one data scheme entity about the conduct of another data scheme entity in relation to the scheme.[19]

4.24 The minister further noted that individuals may complain to the commissioner outside of the formal complaints mechanism in the bill, and that the commissioner would respond to such complaints 'as appropriate' which could lead to the commissioner conducting an own-motion investigation or transferring the matter to a more appropriate regulator.[20]

(h) In what circumstances would the data sharing purposes be compromised by not sharing personal information?

4.25 The minister advised that the sharing of personal information will 'generally be reasonably necessary to support delivery of government services to particular individuals'. He also advised that sharing of personal information may also be required 'for some data integration projects for a permitted purpose' as certain personal information may be necessary to support the integration of the data sets. In these circumstances, data custodians would still be required to share only the personal information necessary to facilitate the data integration project, and would be expected to apply appropriate protections to the data.[21]

---

18 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 34.

19 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, pp. 34–35.

20 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 35.

21 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 35.

4.26 The minister further noted that there are 'well-established' conventions for integrated data, including to maintain 'functional separation' of identifying information (e.g. name or date of birth) from content information (e.g. clinical information or benefit details).[22]

(i) In what circumstances does the bill provide (and is it intended that the rules will provide) that a data sharing agreement may allow the accredited user to provide shared output data to a third party? What protections will apply to protect personal privacy in these circumstances?

4.27 The minister advised that outputs containing personal information are protected by a range of safeguards. He noted that the most common circumstances where personal information would be shared by an accredited user with a third party would be to support government agencies providing an enhanced and streamlined service delivery experience to individuals who are entitled to receive current or new services of benefits.[23]

4.28 Additionally, the minister advised that any sharing of output by an accredited user would only be permitted if this were agreed by the data custodian in accordance with the data sharing agreement, and that for sharing to be authorised, the data custodian must have determined that the access is consistent with the purpose test and data sharing principles.[24]

4.29 The minister also drew the joint committee's attention to subclauses 21(1) and (2) of the bill which set out the circumstances in which an accredited user may provide controlled access to an output to third parties.[25]

(j) Why would other 'less rights restrictive alternatives' (such as amendments to individual pieces of legislation) not be effective to achieve the intended objectives of the bill?

4.30 The minister advised that the bill's authorisation to share and its 'limited override' provide a consistent legal framework for sharing that would be supported by an independent regulator. He stated that it would be 'complex and impractical' to amend individual Commonwealth laws to facilitate greater sharing and explained:

> An exercise of this nature would require changes to over 500 secrecy provisions without the benefit of a dedicated regulator to promote best practice and cultural change, and without the guarantee of less rights restrictive outcomes.[26]

---

22 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 35.

23 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, pp. 35–36.

24 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 36.

25 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 36.

26 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, pp. 36–37.

Joint committee's concluding comments

4.31 After considering the additional information provided by the minister, the joint committee acknowledged that the bill 'appears to be directed towards the legitimate objective of facilitating controlled access to public sector data for specific purposes and would appear to be rationally connected to that objective'.[27]

4.32 However, it also stated that it remained concerned that the scheme as drafted may not be a proportionate means by which to achieve the stated objective. It explained:

> The committee considers that the breadth of the Commonwealth public sector data to which the scheme could apply, and the corresponding considerable extent of the potential interference with the right to privacy, means that the measure would need to be shown to be accompanied by stringent safeguards, oversight and review mechanisms.[28]

4.33 The committee continued with its concerns, emphasising that while the bill contained some important safeguards to protect the right of privacy, it had not been clearly established that these safeguards were 'sufficient'. It noted:

> In particular, the committee notes that the bases on which personal data may be shared are broadly framed and would capture a wide range of purposes. The committee is also concerned that there is no legislative guidance as to when data sharing could reasonably be expected to serve the 'public interest', and no requirement that privacy considerations are considered in this process. The committee is also concerned that there is no explicit requirement in the bill that, where it is possible to do so, information is shared only in a way that does not allow for the identification of an individual.[29]

4.34 The joint committee indicated that it was also 'particularly concerned' that under clause 23 of the bill, authorisation under the overarching legislation would override any existing Commonwealth, state or territory law that restricts or prohibits disclosure of personal information.[30]

4.35 It observed that as a result, the data sharing scheme would permit a Commonwealth body to disclose personal data regardless of any law that currently prohibits this, and without parliamentary oversight of the specific privacy implications of sharing that type of data. It noted that this would mean that the value of any future data protection or secrecy provisions in specific legislative contexts (aside from those related to law-enforcement and national

---

27 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 43.

28 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 44.

29 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, pp. 44–45.

30 Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

security) would need to be assessed having regard to the operation of the scheme. [31]

4.36 The joint committee highlighted that while sharing data in some contexts may have limited privacy implications, there may be other data (e.g. health data) which if shared using 'umbrella type legislation' (such as that proposed in the bill) may have 'significant privacy implications'.[32]

4.37 As such, it pointed out that in assessing proportionality, it was necessary to consider if there were 'less rights restrictive alternatives' which would also be effective in achieving the goals of the scheme. In this regard, the joint committee remarked that no information had been provided by the minister to demonstrate that a less rights restrictive mechanism – such as amending individual pieces of legislation to invoke the umbrella data sharing scheme – would not be equally as effective to achieve the scheme's objectives.[33]

4.38 On this matter, it commented that although it appreciated that amending individual pieces of legislation may be a 'complex undertaking', this did not, in itself, indicate that such an alternative would not be effective to achieving the objective of facilitating controlled access to public sector data.[34] The joint committee determined that as a result it had not been established that the data sharing scheme would constitute a permissible limitation on the right to privacy.[35]

4.39 In summing up its examination of the bill, the joint committee concluded:

> The committee considers that consideration should be given to establishing overarching data sharing legislation which does not override existing secrecy provisions but which requires that the data sharing powers must be specifically invoked by individual pieces of legislation, to ensure appropriate regard is had to whether these broad data sharing powers are appropriate in each specific context.
>
> The committee otherwise considers that the proportionality of the measure may be assisted were the bill amended to provide that:
>
> (a) determining if 'the sharing of information can reasonably be expected to serve the public interest', requires consideration of the impact on an individual's right to privacy, the potential for serious harm to the public, and whether those impacts are reasonable, necessary and proportionate, as well as the potential benefits to the community that would arise from the project;

---

[31] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

[32] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

[33] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

[34] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

[35] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 45.

(b) subclause 16(8) specifies that the application of appropriate protections to the data includes, where possible, ensuring personal information is shared in a manner that does not allow for the identification of individuals;
(c) clause 79 requires that it is a condition of accreditation that an entity which is required to provide evidence for accreditation must provide updated evidence at specified intervals to support its continued suitability for accreditation; and
(d) Part 5.3 makes clear that the Commissioner may consider complaints from individuals with respect to the scheme, and establish a mechanism for dealing with such complaints.

The committee recommends that consideration be given to updating the statement of compatibility with human rights to reflect the information which has been provided by the minister.[36]

4.40 The joint committee drew its human rights concerns to the attention of the minister and the Parliament. [37]

[36] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, pp. 45–46.

[37] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 46.

Chapter 5
Key issues

5.1 This chapter will briefly set out the range of views the committee received from submitters regarding the Data Availability and Transparency Bill 2020 (the bill) and the Data Availability and Transparency (Consequential Amendments) Bill 2020 (the consequential amendments bill).

5.2 It will then examine a number of key issues in greater detail, including:

- the views and recommendations put forward by the Office of the Australian Information Commissioner (OAIC);
- security concerns relating to the participation of foreign entities in the data sharing scheme; national security risks in the higher education and research sector, and cyber-security;
- the standard of consent for sharing and the lack of definition of 'unreasonable or impracticable' in the context of paragraph 16(2)(c);
- the lack of definition of 'public interest' in the context of paragraph 16(2)(a);
- the reliance on delegated legislation for key aspects of the accreditation framework;
- the reliance on guidelines (i.e. non-legislative instruments) to convey core aspects of the data sharing scheme;
- the definition of 'other persons' in clauses 109 and 110;
- the dual roles of the Office of the National Data Commissioner (ONDC);
- concerns relating to the sharing of particular kinds of data;
- the treatment of legal professional privilege; and
- Indigenous considerations.

5.3 The chapter will then conclude with the committee's views and final recommendations.

Views on the bills

5.4 As noted in Chapter 1 of this report, the committee received 31 submissions to its inquiry. Stakeholder views ranged from:

- support for the bills and the proposed data sharing scheme;
- support for the general intent of the data sharing scheme coupled with specific concerns and recommendations designed to improve the drafting of the bills and operation of the scheme; and
- opposition to the bills and the broader concept of public sector data sharing.

Support for the data sharing scheme

5.5 A number of submitters to the inquiry supported the two bills and the policy outcomes the data sharing scheme seeks to achieve.

5.6 For example, Research Australia stated that it believed the framework for data availability to be established by the bills was 'a robust and effective mechanism' for utilising data for research purposes while mitigating the risk of privacy or data breaches.[1]

5.7 Research Australia also commented that its support for the bill was driven by a belief that the new data sharing framework would improve the consistency and timeliness of the consideration of requests for access to data by Commonwealth government departments and agencies. It noted that this outcome would improve the conduct of research in Australia and ultimately lead to better health, social and economic outcomes.[2]

5.8 A submission from Data Republic, an Australian technology company, argued that the bill was a 'critical productivity driver' for both government and improved citizen outcomes.[3]

5.9 Data Republic also supported the 'principles-based' approach of the bill, noting that this approach offered a 'longevity advantage' over a highly codified piece of legislation. It highlighted that it was to be expected that practitioners would require some ongoing guidance (to be provided by the ONDC) in light of the increasing rate of change in data and technology spheres.[4]

5.10 BSA | The Software Alliance (BSA), an advocate for the global software industry, noted that government-generated data is an important asset that can serve as a 'powerful engine' for creating new jobs, promoting economic growth, driving productivity and enabling innovation. It indicated it was 'very supportive' of the bills and asserted that the bills establish a 'promising model' for encouraging the sharing of sensitive, but high-impact data.[5]

5.11 It noted:

> BSA is highly supportive of the Australian Government's intent to enhance the collective benefits of data by advancing responsible policies that facilitate greater sharing, collaboration, and experimentation with data resources while protecting privacy.[6]

5.12 GovHack Australia is an organisation that runs community hackathon events aimed at allowing all levels of government to engage directly with hackers in order to solve civic challenges using government agency open data. It

---

1 Research Australia, *Submission 5*, p. 5.

2 Research Australia, *Submission 5*, p. 9.

3 Data Republic, *Submission 4*, [p. 1].

4 Data Republic, *Submission 4*, [p. 1].

5 BSA | The Software Alliance, *Submission 3*, pp. 1–2.

6 BSA | The Software Alliance, *Submission 3*, p. 1.

informed the committee it believed the Commonwealth Government was taking 'the right steps' to facilitate data sharing and strongly supported the bills.[7]

5.13 The George Institute for Global Health Australia, an independent global medical research institute, set out its support for the bills and highlighted that the bills would not only create opportunities for Australian health and medical researchers, but also mitigate risks relating to the storing, accessing and sharing of data.[8]

5.14 The Population Health Research Network (PHRN), a national data linkage infrastructure network, indicated it supported the passage of the bills as they would embed existing good data sharing practices in legislation. It acknowledged the extensive stakeholder consultation that had taken place during the development of the bills, and stated that it believed that 'overall' the bills deliver 'an effective balance between minimising individual privacy risks and maximising the benefits from the sharing of data'.[9]

Opposition to the bills

5.15 A small number of submitters expressed dissatisfaction with the bills and opposed the proposed data sharing scheme.

5.16 For example, the Australian Privacy Foundation (APF) asserted that the scheme lacked transparency and adequate safeguards for data protection.[10]

5.17 Dr Bruce Baer Arnold, Vice Chair of the APF expressed the view that the bill represents an erosion of Australian privacy law, which itself is considered inadequate and is subject to a review. The new ONDC, sitting alongside the OAIC, was considered by Dr Baer Arnold to be 'balkanising' current responsibilities. Additionally, the OAIC was seen as under-resourced to regulate both privacy and freedom of information law.[11]

5.18 Digital Rights Watch stated that it was concerned that the bills were moving ahead in parallel to the review of the *Privacy Act 1988* (Privacy Act) and asserted:

> Given the topical overlap and potential for new privacy reforms to fundamentally impact the way data protection and ownership is viewed in Australian legislation, it should remain a priority to anticipate an updated

---

7 GovHack Australia Limited, *Submission 12*, [pp. 2–4].

8 The George Institute for Global Health, *Submission 11*, [pp. 1–2].

9 Population Health Research Network, *Submission 17*, [pp. 3–4].

10 See for example: Australian Privacy Foundation, *Submission 28*, pp. 1–5.

11 Dr Bruce Baer Arnold, Vice Chair, Australian Privacy Foundation, *Proof Committee Hansard*, 20 April 2021, pp. 16, 20.

> Privacy Act before proceeding with any other fundamental changes to the way that personal data of Australians is treated.[12]

5.19 Mr Jonathan Gadir, a member of the New South Wales Council for Civil Liberties (NSWCCL) also echoed this concern.[13]

5.20 The Public Interest Advocacy Centre (PIAC) noted that while it does not oppose 'appropriate, secure and informed consent-based sharing of public sector data for the purposes of improving socio-economic outcomes',[14] it believed that the bill did not provide 'sufficient safeguards for a data-sharing scheme which represents a fundamental reform to the way in which public sector data is shared and used'.[15]

Recommendations for improvement

5.21 A larger cohort of submitters expressed general support for the broad intent of the data sharing scheme and acknowledged the oversight and safeguard mechanisms already embedded in the bills.

5.22 However, some of these submitters also raised significant concerns with the practical operation and potential consequences of the bills, and put forward specific recommendations designed to improve the proposed data sharing scheme.[16]

5.23 Many of these concerns centred on privacy risks and safeguards and echoed those raised by the Senate Standing Committee for the Scrutiny of Bills (Scrutiny committee) and the Parliament Joint Committee on Human Rights (joint committee).

5.24 For example, the Law Council of Australia (Law Council) acknowledged the importance of fostering and facilitating data sharing arrangements and the need for the continued development and improvement of robust policies to govern these arrangements. It expressed its support for the removal of 'unnecessary barriers' to government data sharing and the development of a single, unified approach to improve the current 'fragmented and often unclear' data sharing approach.[17] However, the Law Council also stated that it

---

[12] Digital Rights Watch, *Submission 25*, p. 1.

[13] Mr Jonathan Gadir, Member, New South Wales Council for Civil Liberties, *Proof Committee Hansard*, 20 April 2021, p. 15.

[14] Public Interest Advocacy Centre, *Submission 6*, p. 3.

[15] Mr Chadwick Wong, Senior Solicitor, Public Interest Advocacy Centre, *Proof Committee Hansard*, 20 April 2021, p. 15

[16] See for example: Verifier, *Submission 14*; University of Sydney, *Submission 18*; Australian Research Data Commons, *Submission 8*; Group of Eight Australia, *Submission 9*; Population Health Research Network, *Submission 17*; Australian Academy of Science; *Submission 7*; Law Council of Australia, *Submission 30*.

[17] Law Council of Australia, *Submission 30*, pp. 7–8.

appreciated the 'delicate balance' that must be struck between collecting and sharing data, and the right to privacy and the need for appropriate safeguards.[18]

5.25 In many cases submitters informed the committee that they had raised their concerns with the ONDC during the consultation process for the exposure draft of the bill, but that the issues had not been addressed or adequately clarified in the final bill.[19]

5.26 For example, a submission from privacy practitioners Ms Melanie Marks, Ms Anna Johnston and other commercial, public sector and academic professionals acknowledged the significant consultation and review that had informed the development of the bill; however, they emphasised that the concerns they had raised with the ONDC during the consultation had not been addressed in the drafting of the bill.

5.27 They argued that although effective data sharing may assist with achieving enhanced productivity, better service delivery and improved research outcomes, there was 'overarching underappreciation' that the data sharing scheme proposed by the bill constituted an exemption 'authorised by or under an Australian law' from the general principle that personal information must not be used for secondary purposes as set out in Australian Privacy Principle (APP) 6 contained in Privacy Act.[20]

5.28 The committee also received a submission from the OAIC, the independent Commonwealth regulator overseeing privacy functions, freedom of information functions, and information management.[21]

5.29 The OAIC informed the committee that it had engaged with the ONDC throughout the development of the bills to 'help ensure that privacy and security play a central role in the legislative framework'.[22]

5.30 The views and recommendations put forward by the OAIC will be examined in greater detail in the next section.

Views of the Office of the Australian Information Commissioner

5.31 The OAIC noted that two of its key strategic priorities include upholding information access rights and supporting the proactive release of government-

---

18 Law Council of Australia, *Submission 30*, p. 9.

19 University of Sydney, *Submission 18*; National Aboriginal Community Controlled Health Organisation, *Submission 23*; Universities Australia, *Submission 15;* Australian Urban Research Infrastructure Network (AURIN), *Submission 1*; Electronic Frontiers Australia, *Submission 21*; Public Interest Advocacy Centre, *Submission 6*;

20 Ms Melanie Marks, Ms Anna Johnston and other interested parties, *Submission 2*, p. 4.

21 Office of the Australian Information Commissioner, *Submission 16*, p. 3.

22 Office of the Australian Information Commissioner, *Submission 16*, p. 3.

held data, in recognition that data held by the Australian Government is a 'national resource' which can 'yield significant benefits for the Australian people when handled appropriately, and in the public interest'.[23]

5.32 While identifying that the data sharing scheme is one of several Commonwealth government initiatives that reflect this policy objective, the OAIC also noted that proposals to share data containing personal information will necessarily carry certain privacy risks, including:

- the loss of control by individuals; and
- the potential for the mishandling of personal information.[24]

5.33 It observed:

> Privacy risks can be heightened in relation to Government-held information, which is often collected on a compulsory basis to enable individuals to receive a service or benefit or is otherwise required by law. Such data is often sensitive or can become sensitive when it is linked with other government data sets. [25]

5.34 The OAIC informed the committee that it supports the measures included in the bills that are designed to build on the existing privacy framework to minimise the privacy impacts of the data sharing scheme, including:

- Requiring all data scheme entities to be covered by the Privacy Act or a law of a state or territory that provides a commensurate level of privacy protection, monitoring of compliance with the law, and a means for an individual to seek recourse if their personal information is shared.
- Requiring consent to be obtained if the personal information of individuals is to be shared, unless it is unreasonable or impractical to seek their consent.
- Requiring entities to outline how the public interest is served by the sharing in a data sharing agreement.[26]

5.35 However, in addition to this statement of support, the OAIC also recommended the inclusion of additional privacy measures that will provide 'further protections' for individuals and clarity for data scheme entities about their privacy obligations.[27]

5.36 It emphasised:

> The OAIC considers that these additional measures are necessary to ensure the proportionality of the scheme and to achieve the trust and confidence

---

[23] Office of the Australian Information Commissioner, *Submission 16*, p. 2.

[24] Office of the Australian Information Commissioner, *Submission 16*, p. 2.

[25] Office of the Australian Information Commissioner, *Submission 16*, p. 2.

[26] Office of the Australian Information Commissioner, *Submission 16*, p. 3.

[27] Office of the Australian Information Commissioner, *Submission 16*, p. 3.

> of the community, which is vital to the success of the DAT [data availability and transparency] scheme.[28]

5.37 Additionally, the OAIC voiced concerns about the proposal to exempt agencies from the *Freedom of Information Act 1982* (FOI Act).

5.38 These matters will be addressed in further detail below.

Recommendations for additional safeguards

5.39 The OAIC acknowledged the numerous privacy safeguards included in the bill; however, it identified further key privacy protective measures that it deemed should be included to further mitigate the risks posed by sharing personal information.[29]

5.40 These additional measures revolve around:

- the de-identification of data;
- the use of exit mechanisms; and
- the accreditation of Commonwealth entities as users.

5.41 Each of these additional recommended measures will be examined below.

De-identification of data

5.42 Subclause 16(7) of the bill establishes the 'data principle'. This principle focusses on the nature of the data and whether any technical or statistical treatments are necessary to control the risks of the sharing, while still delivering the data needed to achieve the purpose of sharing.[30]

5.43 Specifically, subclause 16(8) states that the 'data principle' includes (but is not limited to) the following elements:

- only the data reasonably necessary to achieve the applicable data sharing purpose is shared; and
- the sharing of personal information is 'minimised' as far as possible without compromising the data sharing purposes.[31]

5.44 The OAIC noted that it supported the decision of the ONDC following consultation on the exposure draft of the bill to elevate the requirement to 'minimise' the amount of personal information shared from guidance material into primary legislation.[32]

---

[28] Office of the Australian Information Commissioner, *Submission 16*, pp. 3–4.

[29] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[30] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 23.

[31] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 23.

[32] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

5.45 However, the OAIC also indicated that it shared the concerns of Scrutiny committee[33] in that while the data sharing principles set out in clause 16 of the bill contemplate minimising the sharing of personal information as far as possible and sharing only the data reasonably necessary to achieve an applicable purpose, there are no requirements for sharing only de-identified data contained in the principles or elsewhere in the bill.[34]

5.46 The OAIC explained:

> This [concern] is consistent with the OAIC's position throughout the development of the DAT [data availability and transparency] scheme, that data sharing should occur on a de-identified basis where possible, to minimise the privacy impacts of the scheme for individuals.[35]

5.47 As a result, the OAIC recommended that the bill include a requirement that data custodians must not share personal information where the data sharing purpose can reasonably by met by sharing de-identified information.[36]

5.48 The OAIC made clear that any definition of 'de-identified' included in the bill should align with the definition set out in section 6(1) in the Privacy Act – that personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.[37]

5.49 It explained the benefits of this 'technology neutral' approach:

> Such an approach is technology neutral and would enable the data custodian to apply the most appropriate de-identification technique to the data to ensure that personal information is protected and that the information will still be useful for its intended purpose after the de-identification process.[38]

5.50 Additionally, the OAIC recommended that clause 19 of the bill should be amended to require data sharing agreements to outline when personal information is being shared as part of a project. It noted that this amendment would create an additional transparency and accountability requirement that supports a data minimisation approach.[39]

---

[33] Note: Further information on the Scrutiny committee's concerns can be found in Chapter 3 of this report.

[34] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[35] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[36] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[37] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[38] Office of the Australian Information Commissioner, *Submission 16*, p. 5.

[39] Office of the Australian Information Commissioner, *Submission 16*, p. 6.

Exit mechanism

5.51 Subclause 21(1) of the bill establishes the limited circumstances in which an output may be provided to third parties as an authorised use of data under subclause 13(3). Subsequent to the process established in this clause, the output 'exits' the scheme and is no longer considered 'scheme data' regulated by the bill.[40]

5.52 'Output' is defined in subclause 10(4) of the bill as 'data that is the result or product of the use, by an accredited user, of public sector shared data shared with the accredited user under subsection [subclause] 13(1).'[41]

5.53 Under subclause 21(1), an accredited user may provide individuals and businesses with outputs containing data about themselves to check the data is accurate by validating or correcting it. Subclause 21(2) clarifies the point at which an output exits the data sharing scheme and ceases to be scheme data regulated by the bill – under paragraph 21(2)(a), that point is the time the output is validated or corrected by the entity with which it is shared.[42]

5.54 The explanatory memorandum (EM) noted that the exit mechanism contained in subclause 21(1) is intended to support the use of outputs created for permitted data sharing purposes, in particular 'government service delivery for which accurate, up-to-date information is essential'. The EM illustrated a potential use of the exit mechanism by noting that the clause supports pre-filling forms (to be validated by the individual or business) and a single point-of-contact to engage with multiple government agencies.[43] In regards to this statement in the EM, the OAIC observed that this data is likely to contain personal information.[44]

5.55 The exit mechanism provided for in subclause 21(3) of the bill allows an accredited user to 'release' output in circumstances that are specified in the data sharing agreement for the project, provided that the release does not contravene a law of the Commonwealth, state or territory.[45]

5.56 The OAIC pointed out that 'release' is defined in clause 9 of the bill as 'provide open access' to data – which is distinct from 'share', which means 'provide controlled access' to data.[46]

---

40 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 29.

41 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 14.

42 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 29–30.

43 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 30.

44 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

45 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 30.

46 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

5.57 The EM noted that subclause 21(3) does not create a new authorisation to release data, and instead provides that entities must rely on release mechanisms in other legislative and policy frameworks.[47] In regard to this, the OAIC observed that if an output contained personal information it could only be disclosed by an accredited user if that disclosure is permitted by the Privacy Act.[48]

5.58 In examining these matters, the OAIC acknowledged that to maximise the benefits and utility of the data sharing framework, it may be necessary for outputs to exit the scheme in certain circumstances.[49]

5.59 However, it recommended that additional protections be included in the bill to ensure that this exit mechanism minimises the risks to individual's privacy and is only used in 'specific and confined' circumstances.[50]

5.60 It recommended that only output that has been shared for the purpose of delivery of government services should be permitted to exit the data sharing scheme for validation or correction under subclause 21(1), unless the ONDC could identify a clear use case prior to the introduction of the legislation that reasonably necessitates data exiting the scheme for broader purposes.[51]

5.61 The OAIC further recommended that the bill 'should explicitly require the accredited user to take reasonable steps to ensure that the output is being shared with the entity or individual (or the individual's responsible person) that the output is about'.[52]

5.62 Additionally, the OAIC recommended that outputs that include personal information should not be permitted to be released from the scheme under subclause 21(3). It explained the rationale behind this recommendation:

> An accredited user will have collected the personal information from a data custodian and not directly from an individual. The individual will therefore have had no ability to consent to the information being disclosed outside the DAT [data availability and transparency] scheme (which could include publication), or to decide to withhold their consent. Given the most likely scenario for data release under cl 21(3) will be sharing research or policy outcomes, it seems unlikely that personal information will be required to meet this purpose and should therefore be explicitly prohibited from release.[53]

---

47 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 30.

48 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

49 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

50 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

51 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

52 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

53 Office of the Australian Information Commissioner, *Submission 16*, p. 6.

Accreditation of Commonwealth entities as users

5.63 Subclause 74(3) of the bill requires the commissioner to automatically accredit non-corporate Commonwealth entities and other Commonwealth bodies as prescribed in the rules if they apply for accreditation as an accredited user under clause 76.[54]

5.64 The OAIC observed that this constituted a 'significant change' to the accreditation framework for the scheme which had not been previously consulted on.[55]

5.65 In making this observation, the OAIC highlighted that accreditation plays an important role in ensuring that entities have appropriate processes, systems and procedures in place to support safe handling of personal information.[56]

5.66 It noted:

> The effectiveness of an accreditation framework rests on the accreditation criteria being set at an appropriate level and accreditation standards and processes being applied consistently across the scheme. A light touch or inconsistent approach to accreditation risks undermining the level of assurance that the framework is designed to provide. A robust accreditation process would provide a strong trust mark for the scheme.[57]

5.67 The OAIC acknowledged the accreditation criteria set out in clause 77 of the bill, as well as the explanation in the EM which noted that non-corporate Commonwealth bodies already meet these accreditation criteria as they are subject to relevant government policies, frameworks, and ministerial oversight.[58]

5.68 However, the OAIC still considered that it was important that the accreditation framework also include an upfront assessment of each entity that wishes to be accredited under the data sharing scheme, and that the assessment is 'undertaken consistently' in relation to all potential accredited entities.[59]

5.69 It explained:

> Compliance with the DAT [data availability and transparency] scheme accreditation criteria could be demonstrated by drawing on the policies and processes, governance arrangements, training programs and data management protocols that an entity already has in place to comply with its existing obligations under other frameworks. However, an individual

---

54 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 47.

55 Office of the Australian Information Commissioner, *Submission 16*, p. 7.

56 Office of the Australian Information Commissioner, *Submission 16*, p. 7.

57 Office of the Australian Information Commissioner, *Submission 16*, p. 7.

58 Office of the Australian Information Commissioner, *Submission 16*, p. 8.

59 Office of the Australian Information Commissioner, *Submission 16*, p. 8.

> assessment of each application for accreditation by the National Data Commissioner would enable important oversight of how these obligations will be applied in the context of the DAT scheme. The OAIC considers that this should be the case even for Commonwealth bodies, who should still be subject to the same rigorous accreditation process, regardless of their broader privacy and security obligations.[60]

5.70 Subsequently, the OAIC recommended that all accredited users (including Commonwealth bodies) be subject to the same rigorous accreditation processes and criteria as other entities seeking to become accredited under the data sharing scheme.[61]

Proposal to exempt agencies from the FOI Act

5.71 The OAIC raised concerns regarding the proposed exemption of scheme data from the FOI Act contained in the consequential amendments bill, noting that it considered this exemption 'runs counter' to the objects of both the FOI Act and the principal bill.[62]

5.72 The OAIC explained its core concerns as follows:

> The OAIC is concerned that the proposal is unnecessarily broad and risks misalignment with the objects of the FOI Act to provide a fundamental legal right to access documents. The OAIC is also concerned that this proposal reduces the information access rights of individuals, impacting on their ability to seek access to their own personal information and understand how agencies are using this information.[63]

5.73 The OAIC recommended that consideration be given to removing the proposed consequential amendment to the FOI Act so that data that is shared by agencies under the data sharing scheme remains subject to the usual FOI processes and potential exemptions under the FOI Act.[64]

5.74 It submitted that through building on existing transfer mechanisms in the FOI Act, data custodians and accredited users could be supported to deal with such FOI requests through the inclusion of specific provisions in the FOI Act that would:

- allow for the transfer of data back to the data custodian in the event an FOI request is received by an agency with which the data was shared as an accredited user; or

---

60 Office of the Australian Information Commissioner, *Submission 16*, p. 8.

61 Office of the Australian Information Commissioner, *Submission 16*, p. 8.

62 Office of the Australian Information Commissioner, *Submission 16*, p. 4.

63 Office of the Australian Information Commissioner, *Submission 16*, p. 4.

64 Office of the Australian Information Commissioner, *Submission 16*, p. 4.

- require the accredited user to consult with the original data custodian if data that had been shared with them under the data sharing scheme is requested through the FOI Act.[65]

Security concerns around foreign entities

5.75 The committee received evidence relating to the participation of foreign entities in the data sharing scheme.

5.76 For example, a joint submission from the Allens Hub for Technology Law and Innovation (Allens Hub), the Australian Society for Computers and Law (ASCL) and University of New South Wales Institute for Cyber Security (UNSWICS) highlighted that it was not clear how exactly the ONDC would enforce the protection of data released offshore to a foreign entity in the case of a breach of a data sharing agreement.[66]

5.77 The three organisations stated that they had raised this concern with the ONDC during a consultation roundtable in October 2020 and set out the response they received:

> … it was suggested [by the ONDC] that if the foreign entity breached its agreement, then Australia would have recourse to send information about the breach to authorities in the foreign jurisdiction for prosecution under its own laws. [67]

5.78 However, they emphasised that this proposed approach would only work if the entity has data protection laws 'at least on par' with those in Australia.[68]

5.79 The three organisations argued that the status of the data protection laws in the foreign country should be a 'determining factor' in the accreditation of a foreign entity and the approval of a data sharing agreement. They contended that if the domestic laws for the foreign entity are insufficient, then no accreditation should be given and no data should be shared.[69]

5.80 They also noted that subclauses 136(2) and (3) in the bill raised concerns that if a breach occurs outside of Australia, then it may not contravene a civil penalty provision. They explained:

> Although Australia may not have jurisdiction to pursue matters which occur offshore, it is not clear why it is necessary to remove the civil

---

65 Office of the Australian Information Commissioner, *Submission 16*, pp. 4–5.

66 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 4].

67 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 5].

68 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 5].

69 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 5].

> penalty. Even so, given the non-application of penalties against foreign entities, it is questionable whether such entities would be compelled to comply with many of the safeguard mechanisms once accredited.[70]

5.81 The committee queried Ms Deborah Anton, the Interim National Data Commissioner, as whether the ONDC had consulted with the Australian Security Intelligence Organisation (ASIO) and other security agencies regarding the bill.

5.82 The committee noted that the Parliamentary Joint Committee on Intelligence and Security (PJCIS) is currently inquiring into the national security risks affecting the Australian higher education and research sector, with a report due in July 2021.

5.83 The committee drew Ms Anton's attention to evidence received in March 2021 by the PJCIS, where Mr Mike Burgess, the Director-General of Security for ASIO, stated :

> Foreign intelligence services and their proxies are all too willing to take advantage of the openness that is integral to our universities and research institutions to steal intellectual property and cutting-edge technologies.[71]

5.84 Ms Anton advised the committee that the ONDC had significant engagements and consultations with the Australian intelligence agencies during the development of the bill. Further, she noted that input and feedback had been critical to ensure the bill establishes protections to prevent Australian Government data from being used inappropriately by foreign entities. Ms Anton stated that while the bill contemplates the sharing of data with foreign entities, a 'series of controls' was also built in to manage the risks associated with international data sharing,[72] including that the bill has extraterritorial operation (as set out in clause 7).[73]

5.85 Ms Anton provided further detail on those controls:

> More particularly, I do note that opening point that data cannot be shared for a purpose that relates to a prejudice of national security as per [subclause] 15(2).
>
> In accrediting entities other than Commonwealth government entities, essentially, our criteria for accreditation is that the entity's participation in

---

[70] Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 5].

[71] Mr Mike Burgess, Director-General of Security, Australian Security Intelligence Organisation, *Parliamentary Joint Committee on Intelligence and Security Hansard*, 11 March 2021, p. 27.

[72] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 3.

[73] Office of the National Data Commissioner, additional information received 22 April 2021, p. 1.

> the data-sharing scheme would pose no concerns for reasons of national security as per section 77.
>
> The commissioner can suspend or cancel accreditation for reasons of security as per clause 81.
>
> As I noted in my opening statement, it's not expected that foreign entities, which are not covered by Australian privacy law, will be able to access personal data as they can't satisfy the privacy coverage test under clause 28.
>
> Data-sharing agreements which may involve working with research or government policy purposes and engaging with the research community which you allude to do have a requirement for an accredited user who accesses the data.

5.86 With regard to ASIO's involvement in accreditation Ms Anton advised:

> Data can only be shared under the scheme with entities that are accredited as users by the Commissioner. Any foreign entity seeking accreditation must meet the criteria which include that "the entity's participation in the data sharing scheme would not pose concerns for reasons of national security (within the meaning of *the Australian Security Intelligence Organisation Act 1979*)" (clause 77(1)(g) of the Bill). When assessing whether this criterion is met, the Commissioner will rely upon advice from ASIO in the form of a security assessment. If an entity is not accredited because of an ASIO recommendation, it will not be able to receive any data under the scheme. ASIO recommendations can also result in the imposition of conditions of accreditation on a foreign entity for security reasons, including constraints on data or the individuals who can access shared data.
>
> Importantly, decisions by the Commissioner to suspend, cancel or impose a condition on the accreditation of a foreign entity for security reasons are not reviewable by the Administrative Appeals Tribunal (clause 118 of the Bill).[74]

5.87 Ms Anton concluded that there are multiple layers of control present in the bill:

> From my point of view, those are quite a few layers of control—the creation of an accreditation scheme that works with the research sector in terms of accessing data that links back into the work being done by ASIO. Those are new controls designed specifically for this scheme.[75]

5.88 The committee requested information from the ONDC as to what ongoing oversight security agencies will have under the bill to ensure that access to government data is not being used, even inadvertently, to the advantage of foreign powers. Ms Anton advised that the security review is an ongoing process that will continue past the accreditation stage. Ms Anton noted that:

---

[74] Office of the National Data Commissioner, additional information received 22 April 2021, pp. 1–2.

[75] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 3.

> ASIO will have access to the names of accredited entities and the data sharing agreements these entities have entered into. If, at any time, ASIO has security concerns they can make a recommendation to the commissioner.[76]

5.89 Additionally, Mr Paul Menzies-McVey, Assistant-Secretary for ONDC, noted that the commissioner would have the powers to take appropriate action in response to a security recommendation, including:

- suspending or cancelling the accreditation (therefore preventing any further data sharing); or
- imposing conditions on the accreditation (e.g. requiring that people of concern no longer have access to the data).[77]

5.90 He further noted that the commissioner would have the regulatory powers to ensure that any conditions on the accreditation were being complied with.[78]

5.91 The ONDC advised that it will enter into a memorandum of understanding with ASIO and the OAIC to document the everyday working relationship in relation to the accreditation process and other matters, if the bill is enacted.[79]

5.92 The committee also inquired about the ability of universities participating in data-sharing agreements to protect data from cybersecurity breaches. Dr Adele Haythornthwaite from the University of Sydney advised:

> We have a concerted program that is addressing cybersecurity risk, as all other research institutions in Australia are doing. We are in a constant state of improving those. We are taking part in the review of critical infrastructure that's currently underway at the moment, with the legislation there, to put in even more robust risk governance frameworks to address cybersecurity risks. We have a dedicated information security officer and a team of cybersecurity analysts who stay abreast of the current developments in the cyberworld. As you're aware, it's a current state of escalation and there are always new threats to be identified. To date we have managed to have very good cybersecurity governance of our systems; that includes our administrative systems as well as our research systems.[80]

5.93 Mr Tim Payne from the University of Sydney added:

> I can add that we have reported in detail on our efforts in these areas in another submission recently, in relation to foreign interference. The university is also required to report through its compact agreement with

---

[76] Office of the National Data Commissioner, additional information received 22 April 2021, p. 2.

[77] Mr Paul Menzies-McVey, Assistant Secretary, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 4.

[78] Mr Paul Menzies-McVey, Assistant Secretary, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 4.

[79] Office of the National Data Commissioner, additional information received 22 April 2021, p. 1.

[80] Dr Adele Haythornthwaite, Research Data Consulting Lead, Sydney Informatics Hub, University of Sydney, *Proof Committee Hansard*, 20 April 2021, p. 22.

> the federal government, as are all universities about their approaches to foreign interference, as part of that cybersecurity.[81]

5.94 Ms Anton highlighted the Government's ongoing efforts to ensure strong cyber-security standards and to protect data from unauthorised use, drawing particular attention to Australia's Cyber Security Strategy 2020 and the Government's own approach to secure data storage. With regard to ability of the commissioner to ensure those using the scheme took these factors into account she noted:

> As Australian Government policies evolve over time, data custodians will be expected to apply the updated policies, as applicable, to entities receiving data shared under the scheme.
>
> This expectation will be included in guidance to be issued by the Commissioner, and if necessary, in a data code issued by the Commissioner.
>
> Security requirements on the accredited user must be included in the data sharing agreement, which is legally binding on the accredited user and which will be published by the Commissioner.[82]

5.95 Ms Anton also noted the particular role that accredited data service providers (ADSPs) will can play to ensure strong security standards are met:

> Where accredited users cannot meet the security standards required by the data custodian, consideration can be given to sharing the data with the accredited user using a secure facility operated by an accredited data service provider.[83]

Standard of consent (definition of 'unreasonable or impracticable')

5.96 A number of submitters echoed the concerns of the Scrutiny committee in regard to the paragraph 16(2)(c) of the bill, which requires that any sharing of the personal information of individuals 'is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent'.[84] Specifically, submitters were concerned that the bill does not contain a clear definition of 'unreasonable or impracticable'.

5.97 The Law Council highlighted the Scrutiny committee's concern with the breadth of the 'unreasonable or impracticable' exception, and drew attention to the minister's advice that privacy interests will not be given priority in the public interest test.[85] It concluded:

---

[81] Mr Tim Payne, Director, Higher Education Policy and Projects, Office of the Vice-Chancellor and Principal, University of Sydney, *Proof Committee Hansard*, 20 April 2021, p. 23.

[82] Office of the National Data Commissioner, additional information received 22 April 2021, p. 1.

[83] Office of the National Data Commissioner, additional information received 22 April 2021, p. 1.

[84] See Chapter 3 of this report for further detail on the Scrutiny committee's concerns.

[85] Law Council of Australia, *Submission 30*, p. 23.

> Further guidance is needed in relation to the scope of practical application of the 'unreasonable or impracticable' exception as it applies to securing consent, noting that this should be a high threshold to obtain and that many of the data sets collected are collected based on existing legal requirements or notices (not consents).[86]

5.98 Dr Megan Prictor and Associate Professor Mark Taylor from the Melbourne Law School (who submitted in their private capacities) considered that there was 'significant risk of confusion' in regard to the interpretation of the terms with reference to the OAIC guidelines, given that the guidelines that apply to section 16A of the Privacy Act on when it is unreasonable or impracticable to obtain consent 'are not an obvious fit for the use of these terms' in the bill.[87]

5.99 They explained that this was because section 16A is specific to circumstances where an entity is collecting, using or disclosing personal information in the context of necessity to 'lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety', and that this constituted a 'narrower context' than that envisaged in the data sharing scheme to be established under the bill, which will permit sharing for a very wide range of purposes.[88]

5.100 Dr Prictor and Associate Professor Taylor stated that a reliance upon the OAIC guidelines relating only to section 16A of the Privacy Act (as appears to be indicated in the EM to the bill) would be 'insufficient' as a basis for interpretation of those terms in the new legislative context. They noted that additional OAIC guidance on consent is available in relation to other provisions of the Privacy Act, such as section 16B in relation to research relevant to public health or public safety, which they considered may be of greater relevance to the bill.[89]

5.101 Dr Prictor and Associate Professor Taylor recommended that 'as a minimum' the commissioner should be 'required' (rather than simply 'permitted' under clause 127 of the bill) to make written guidelines on the interpretation of the 'unreasonable or impracticable' exemption. They also further recommended:

> …considering that there is a substantial risk that lack of clarity relating to data sharing principles will ultimately undermine the Government's policy goal of promoting data sharing, we would suggest a better path to certainty for those subject to the scheme would be for the Commissioner to issue codes of practice with the status of legislative instruments, rather than guidelines, to address these issues.[90]

---

86 Law Council of Australia, *Submission 30*, p. 24.

87 Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [p. 2].

88 Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [p. 2].

89 Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [pp. 2–3.].

90 Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [p. 3].

5.102 Ms Johnston and Ms Marks contended that it was not clear how the consent model could be implemented and maintained, particularly for the sharing of datasets containing personal information already held by a data custodian. Their submission stated that as such it was likely to be considered 'impracticable' for a data custodian to seek individual consent for any substantial dataset that had already been collected.[91]

5.103 The joint submission from the Allens Hub, the ASCL and the NSWICS also recognised that the bill does not provide definitions or examples on when it is unreasonable or impracticable to seek individuals' consent.[92]

5.104 The three organisations identified that different data custodians (i.e. government agencies) have different rules and policies in place, and therefore what may be unreasonable to one custodian to seek consent may not be unreasonable to another. The submission explained:

> In our view, it is important to promote consistency across agencies where possible and provide clarity on when it is unreasonable and impracticable to seek consent, or at least provide certain threshold examples or guidelines.[93]

5.105 The submission recommended that the threshold for circumstances when it is unreasonable or impracticable to seek consent should be incorporated as part of the ethics function governed by the National Data Advisory Council.[94]

5.106 Verifier, a regulatory technology company, submitted that the proposed consent requirements in the bill 'lag community expectations' about individuals' privacy and the right to control how their data is shared, used and disclosed. It suggested that guidance issued by the commissioner should address the 'unreasonable or impracticable' exception to seeking consent to ensure that it is only applicable in 'limited and clearly defined circumstances'.[95]

5.107 PIAC also echoed the concerns of the Scrutiny committee. While it acknowledged that the inclusion of consent in the 'project principle' was an improvement on earlier versions of the bill where consent was not intended to be required, it stated that in its view paragraph 16(2)(c) remained an area of

---

91 Ms Melanie Marks, Ms Anna Johnston and other interested parties, *Submission 2*, p. 7.

92 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 7].

93 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 7].

94 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security, *Submission 22*, [p. 7].

95 Verifier, *Submission 14*, p. 3.

concern as the concepts of 'unreasonable or impracticable' are not defined in the bill or in the Privacy Act:[96]

> Guidance on this phrase, as issued by the 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.[97]

5.108 Continuing on, PIAC submitted that this lack of clarity would limit the scheme's transparency and accountability:

> 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.[98]

5.109 PIAC identified that the issue would affect marginalised communities disproportionately, given their greater interaction with government services. It observed that people who rely on government services may not be in a position to provide informed consent, given the inherent power imbalance when requesting services.[99]

5.110 PIAC asserted that for the government to build confidence in the community that data is being shared appropriately, 'consent of those least empowered must not be bypassed'.[100] It set out a number of potential situations that it considered would not be sufficient to satisfy the 'unreasonable or impracticable' exception, including:

> … 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.[101]

5.111 To mitigate its concerns, PIAC recommended that the bill be amended to strengthen the requirement for consent by better defining the circumstances in which it will be 'unreasonable or impracticable' to seek consent of an individual, including by identifying relevant factors to be taken into account in making that decision.[102]

---

96 Public Interest Advocacy Centre, *Submission 6*, pp. 4–5.

97 Public Interest Advocacy Centre, *Submission 6*, p. 5.

98 Public Interest Advocacy Centre, *Submission 6*, p. 5.

99 Public Interest Advocacy Centre, *Submission 6*, p. 5.

100 Public Interest Advocacy Centre, *Submission 6*, p. 6.

101 Public Interest Advocacy Centre, *Submission 6*, p. 6.

102 Public Interest Advocacy Centre, *Submission 6*, pp. 6–7.

5.112 PIAC further recommended the bill incorporate a requirement that where personal information is shared by data custodians without consent on the basis that it is 'unreasonable or impracticable', the data custodian must publish (in such a way that does not identify individuals) the efforts undertaken to seek that consent and the subsequent reasons for dispensing with consent. It argued that this would allow for increased scrutiny and accountability of decisions made by data custodians. [103]

5.113 As set out in Chapter 3 and Chapter 4 of this report, the then minister responded to the concerns of the Scrutiny committee and joint committee on this matter. He advised that he proposed to table an addendum to the EM 'as soon as practicable' which would outline 'key information and examples' about the meaning of 'unreasonable or impracticable' to assist to clarify the interpretation of paragraph 16(2)(c) of the bill. He also noted that the proposed addendum would direct users to relevant guidance issued by the Australian Information Commissioner on the standard of consent.[104]

Definition of 'public interest'

5.114 Several submitters flagged similar concerns to those raised by the Scrutiny committee and the joint committee about the lack of a definition of 'public interest'.

5.115 The Scrutiny committee noted that paragraph 16(2)(a) of the bill requires a judgement to be made about whether the sharing can be reasonably expected to serve the public interest. It highlighted that 'public interest' is not defined in the bill, and that the EM does not provide guidance about the factors that might be considered when evaluating public interest for the purposes of data sharing.[105]

5.116 PHRN informed the committee that it shared the concerns of the Scrutiny committee in regard to the evaluation of the public interest. It commented that although there was a strong emphasis on the concept of public interest during the ONDC consultation process for the bill, it considered that the concept was 'significantly diluted' in the final text of the bill.[106]

5.117 PHRN highlighted that although the bill requires a description of how the public interest is served by sharing to be included in a data sharing agreement, there is no requirement for any independent assessment of public interest before the requested data is shared. It asserted that this could prove challenging, particularly in the case of sharing with private sector entities:

---

[103] Public Interest Advocacy Centre, *Submission 6*, pp. 6–7.

[104] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 34.

[105] See Chapter 3 of this report for further detail on the Scrutiny committee's concerns.

[106] Population Health Research Network, *Submission 17*, p. 2.

> The data custodian and other entity entering into the data sharing agreement will need substantial support and guidance to be able to assess and describe the public interest in the data sharing agreement. This will be particularly important when considering sharing data with private companies. The legal obligations of private companies to their shareholders must take precedent over the public interest and therefore whether data sharing with private industry is in the public interest will require careful consideration.[107]

5.118 The Minderoo Tech & Policy Lab at the University of Western Australian Law School argued that the bill as currently drafted only requires that sharing be expected to serve the public interest generally and does not require specific testing against competing public interest claims, such as to privacy or autonomy.[108]

5.119 Although welcoming the inclusion of a public interest test, the submission from privacy practitioners Ms Marks and Ms Johnston noted that there remained questions about the threshold of what is and is not in the public interest. They asserted that the requirement found in paragraph 19(7)(a) of the bill for data sharing agreements to include a description of how the public interest is to be served by the sharing did not constitute a 'robust enough' test.[109]

5.120 They recommended that a detailed formulation of the public interest test be modelled from the joint National Health and Medical Research Council (NHMRC)/OAIC guidelines (issued under the Privacy Act), and that a 'no harm' test be included where the sharing includes personal information, in order to ensure that individual harm is considered as well as broad public interest.[110]

5.121 Dr Prictor and Associate Professor Taylor also echoed the concerns of the Scrutiny committee and flagged that the lack of definition of 'public interest' may permit the operation of a public interest test that cannot be appropriately reconciled with reasonable expectations of privacy. They suggested that, as a minimum and in line with the objective of the bill, it should be made clear that an assessment of a reasonable expectation of public interest should incorporate assessment from the perspective of data subjects and community expectations and norms:[111]

> …it should be critically significant whether those whose data may be shared (when relevant factors have been 'weighed') have reason to expect

---

[107] Population Health Research Network, *Submission 17*, p. 2.

[108] Minderoo Tech & Policy Lab – University of Western Australian Law School, *Submission 26*, p. 2.

[109] Ms Melanie Marks, Ms Anna Johnston and other interested parties, *Submission 2*, p. 9.

[110] Ms Melanie Marks, Ms Anna Johnston and other interested parties, *Submission 2*, p. 9.

[111] Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [p. 2].

> and accept the privacy interference that sharing represents and that it not be to their unjustified disadvantage. Adopting a principle that data sharing only take place under conditions that persons have reason to both expect and accept may enable privacy interests to be appropriately reconciled with the public interest in data sharing (rather than overridden for commercial or economic interests that data subjects personally may have no reason to think justify privacy intrusion.[112]

5.122 As set out in Chapter 3 and Chapter 4 of this report, the then minister responded to the concerns of the Scrutiny committee and joint committee on this matter, advising that the question of whether a project can be reasonably expected to serve the public interest must be made on a project-by-project basis, weighing a range of factors for and against sharing.

5.123 The minister noted that the factors will include:

- the impacts on an individual's right to privacy;
- the potential for serious harm to the public; and
- whether those impacts are 'reasonable, necessary and proportionate'. [113]

5.124 He also advised that the bill's intended approach is to ensure privacy interests are appropriately balanced with the public interest of a project, rather than assuming that one must prevail at the expense of the other. He emphasised that this approach is consistent with the objectives of the Privacy Act.[114]

Reliance on delegated legislation for accreditation

5.125 Submitters to the inquiry raised concerns with the reliance on delegated legislation to set out the accreditation framework.

5.126 For example, the Law Council advised that it shared the Scrutiny committee's concerns about the proposed reliance on delegated legislation to provide for procedures, requirements and matters relating to the accreditation of entities for the purpose of the data sharing scheme.[115]

5.127 The Law Council recommended that Part 5.2 of the bill (relating to the accreditation framework) be amended to provide greater detail in regard to the procedures, requirements and matters relating to the accreditation of entities for the purpose of the data sharing scheme.[116]

5.128 The Australian Research Data Commons (ARDC) and Universities Australia also raised concern with the reliance on delegated legislation, with the ARDC

---

[112] Dr Megan Prictor and Associate Professor Mark Taylor, *Submission 19*, [p. 2].

[113] Parliamentary Joint Committee on Human Rights, *Report 4 of 2021*, 31 March 2021, p. 33.

[114] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 16.

[115] Law Council of Australia, *Submission 30*, p. 24.

[116] Law Council of Australia, *Submission 30*, p. 24.

recommending that key matters of the accreditation framework should be explicit in legislation.[117]

5.129 Universities Australia commented that leaving a range of significant matters to legislative instruments without significant guidance in the primary legislation does not support certainty, while the University of Sydney also noted that the likely impact of the implementation of the bills on universities and their research is 'hard to gauge while the legislative instruments are not yet defined'.[118]

5.130 As set out in Chapter 3 of this report, the then minister responded to the Scrutiny committee's concerns around this matter. He advised that the approach of providing for three types of legislative instruments in the bill will ensure the scheme can adapt to emerging technologies and future needs while still allowing for oversight through the disallowance process.[119]

5.131 The minister stated that he did 'not consider it necessary to include further guidance on accreditation matters on the face of the bill'. He reiterated that as the weight of the accreditation framework was already located in Part 5.2 of the bill, significant matters would not be left to delegated legislation. He also explained that where the bill does provide for delegated legislation, it is aligned with standard drafting practices to balance legal certainty and flexibility.[120]

Reliance on guidelines

5.132 Clause 127 of the bill empowers the commissioner to make guidelines with respect to matters relating to their functions and powers under the data sharing scheme.[121]

5.133 Subclause 127(2) provides that these guidelines may include principles and processes relating to:

- any aspect of the data sharing scheme; and
- any matters incidental to the data sharing scheme, including:
  - data release;
  - data management and curation;
  - technical matters and standards; and
  - emerging technologies.[122]

---

117 Australian Research Data Commons, *Submission 8*, [p. 2].

118 Universities Australia, *Submission 15*, [p. 2]; University of Sydney, *Submission 18*, [p. 2].

119 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p.21.

120 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 22.

121 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 73.

5.134 Subclause 127(4) provides that a guideline is not a legislative instrument.[123]

5.135 The Law Council expressed reservations about this subclause given the importance of the guidelines in setting the parameters of the data sharing scheme, and the fact that non-legislative instruments are not subject to parliamentary scrutiny.[124]

5.136 It recommended that the subclause be removed and instead a requirement inserted that guidelines made by the commissioner are a legislative instrument and therefore subject to parliamentary scrutiny and potential disallowance.[125]

5.137 As set out in Chapter 3 of this report, the then minister responded to the Scrutiny committee's concern in regard to this matter, emphasising that the approach taken by the bill is consistent with that of other principles-based legislative schemes. He advised that the bill establishes a framework of resources 'of scaled legal weight' to assist in interpretation and application, and that he considered this scaled approach to be reasonable and necessary to support best practice data sharing and a graduated approach to enforcing compliance.[126]

5.138 The minister also noted that while guidelines do not alter the law, they provide 'clear guidance from the commissioner about their view of law applied and better practice', and that it was 'not appropriate' for such guidance to be disallowable.[127]

'Other persons'

5.139 Clauses 109 and 110 of the bill relate to monitoring and investigation powers respectively. Specifically, subclauses 109(4) and 110(3) provide that an authorised person may be assisted by 'other persons' in exercising powers or performing functions or duties in relation to monitoring and investigation.[128]

5.140 As set out in Chapter 3 of this report, the Scrutiny committee raised concerns with these clauses, given that the EM does not contain any information on the categories of 'other persons' who may be granted such powers and the bill

---

122 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 73.

123 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 74.

124 Law Council of Australia, *Submission 30*, p. 23.

125 Law Council of Australia, *Submission 30*, p. 23.

126 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5 of 2021*, 17 March 2021, p. 36.

127 Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 5 of 2021*, 17 March 2021, p. 37.

128 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 63.

does not confine who may exercise the powers by reference to any particular expertise or training.[129]

5.141 Despite receiving further information from the then minister on the matter, the Scrutiny committee remained concerned with the clauses and reiterated that its consistent position in relation to the exercise of coercive or investigatory powers is that persons authorised to use such powers should have the appropriate training and expertise.[130]

5.142 The Law Council echoed these concerns and affirmed its support of the view of the Scrutiny committee. It recommended that the bill be amended to include minimum thresholds of training or experience for 'other persons' assisting the commissioner in the exercise of their monitoring and investigation powers.[131]

5.143 As set out in Chapter 3 of this report, the then minister addressed this matter and clarified that the staffing provisions in the bill will ensure that 'other persons' at the commissioner's disposal will have the appropriate knowledge, training and expertise in the exercise and performance of investigatory powers and functions.[132]

Dual roles of the Office of the National Data Commissioner

5.144 As set out in Chapter 3 of this report, the Scrutiny committee noted the possibility of tension between the dual roles of the commissioner as both regulator and champion of the data sharing scheme.

5.145 A number of submitters flagged similar concerns with the possible tensions that could arise from the dual roles of the commissioner.

5.146 For example, the submission authored by privacy practitioners Ms Marks and Ms Johnston stated that 'at a fundamental level' it was not appropriate for the commissioner to have powers to investigate or suspend activities given that the role also included advocating for the sharing and release of public sector data. The submission concluded:

> We see the dual roles of promoting and maximising sharing whilst protecting privacy to be at odds, and a conflict of interest.[133]

---

[129] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 10.

[130] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, pp. 25–26.

[131] Law Council of Australia, *Submission 30*, pp. 10–11.

[132] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 3 of 2021*, 17 February 2021, p. 24.

[133] Ms Melanie Marks, Ms Anna Johnston and other interested parties, *Submission 2*, p. 10.

5.147 The Australian Medical Association (AMA) also expressed concern about the potential conflict between the commissioner's two roles:

> If an agency seeks advice from the Data Commissioner prior to entering into a data sharing agreement, there is potential conflict at the point of providing advice between the Data Commissioner's role of promoting safety and their role of promoting sharing. Moreover, if the data is subsequently re-identified or a complaint is made, the Data Commissioner will be investigating a data sharing agreement that they advised on.[134]

5.148 In order to mitigate this potential conflict, the AMA recommended that that OAIC be provided with a greater role in the oversight of the scheme.[135]

5.149 The NSWCCL, Electronic Frontiers Australia (Electronic Frontiers) and the APF also suggested that there was an inherent conflict of interest in having the commissioner as both the regulator and champion of data sharing. The NSWCCL and Electronic Frontiers both recommended that as an alternative the OAIC be funded to perform the oversight and regulatory functions for the scheme, leaving the commissioner to focus on advocacy, education and advice.[136]

Concerns with the sharing of particular kinds of data

5.150 A number of submitters raised concerns regarding the sharing of particular kinds of data, including:

- health data (including immigration detention health records);
- commercially sensitive data; and
- biometric data.

5.151 Each of these matters will be addressed further below.

5.152 In its submission the ONDC highlighted that data sharing will not be authorised if it is for a precluded purpose, or another exclusion applies. In addition, the minister may also prescribe additional precluded purposes in rules.[137]

5.153 Specifically, the EM clarified that:

> Clause 17 of the bill outlines when sharing of data is excluded from the scheme, and clause 17(4) allows further exclusions to be prescribed by regulations. Exclusions detailed in this clause include contravention or infringement of rights such as commercial-in-confidence, contracts, international law and evidence before the court.

---

[134] Australian Medical Association, *Submission 13*, p. 7.

[135] Australian Medical Association, *Submission 13*, p. 7.

[136] See New South Wales Council of Civil Liberties, *Submission 27*, p. 5; Electronic Frontiers Australia, *Submission 21*, pp. 8–9; Australian Privacy Foundation, *Submission 28*, p. 1.

[137] Office of the National Data Commissioner, *Submission 20*, p. 5.

> Clause 17 works in conjunction with other limitations on data sharing to ensure data is not authorised to be shared where it would be inappropriate to do so. Clause 13 ensures that all other controls in the bill, as outlined in clauses 15 to 18 are met, and that data sharing is in the public interest.[138]

5.154 Draft regulations, released alongside the exposure draft of the bill, exclude types of entities from sharing data and also data collected under specific legislation.[139] Ms Anton advised the committee:

> I understand that the Minister's intention is to make available another version of the draft regulations before the Bill is debated in the House of Representatives.[140]

Health data

5.155 The AMA submitted that clause 15 of the bill allows individuals' health information to be shared with private sector organisations for profit.[141] The AMA cited the EM to the bill, which states:

> Sharing for purposes that are consistent with clause 15(1) but have other applications may be permissible. For instance, a research project to improve pharmaceutical treatments for heart disease may deliver both profit for a researcher as well as serving the public interest.[142]

5.156 In light of this, the AMA emphasised that it was concerned for the potential for non-admitted primary healthcare data, including Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data, to be shared with health funds for their own purposes. It explained:

> Currently this [the sharing of non-admitted primary healthcare data] is prohibited by the *National Health Act 1953*, the *Health Insurance Act 1973* and the *My Health Records Act 2012*. It makes no sense to preclude My Health Record data from the data sharing scheme, but then permit the same MBS/PBS data to be directly shared with private health insurers. This is not consistent with the public's expectations and has the potential to undermine the community-rated private health insurance system.[143]

5.157 To mitigate this concern, the AMA recommended that rules created under paragraph 15(2)(c) specify that the use of MBS and PBS data by health funds is a precluded purpose for data sharing.[144]

---

138 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 23.

139 Note: The draft Data Availability Regulations 2020 are available at www.datacommissioner.gov.au/resources/exposure-draft

140 Office of the National Data Commissioner, additional information received 22 April 2021, p. 2.

141 Australian Medical Association, *Submission 13*, p. 9.

142 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 20.

143 Australian Medical Association, *Submission 13*, p. 9.

144 Australian Medical Association, *Submission 13*, p. 10.

5.158 Additionally, PIAC raised 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. It explained:

> 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.[145]

5.159 It noted that while the exposure draft of the Data Availability and Transparency Regulations 2020 proposed to exclude other types of especially sensitive data (such as My Health Record information) from the data sharing scheme (pursuant to clause 17(4)(a) of the bill), there was no mention of immigration detention health record information also being excluded. PIAC recommended that immigration detention records held by the Department of Home Affairs be excluded from the data sharing scheme.[146]

Commercially sensitive data

5.160 The Australian Banking Association (ABA) strongly recommended that business regulation and commercially sensitive data obtained from the private sector (but held by the public sector) be excluded from the data sharing scheme.[147]

5.161 The ABA explained that it had raised its concerns with the ONDC during consultation on the exposure draft of the bill, but stated that it was not satisfied with the proposed solution.[148]

5.162 The ABA explained its position:

> Data held by banks can reveal confidential information provided under, or contained in, commercial contracts. Even where data is anonymised or used in aggregate form, it can reveal commercial information about certain entities or their customers in specific sectors or geographical regions. As it is currently drafted, the DAT Bill creates the real risk of on-sharing this data to third parties who may lack full understanding of the implications of further sharing the information. Further, the proposed individual contractual agreements between individual regulators and third parties cannot fully ensure the adherence of third parties to protect the confidentiality of commercially sensitive data.[149]

---

145 Public Information Advocacy Centre, *Submission 6*, pp. 8.

146 Public Information Advocacy Centre, *Submission 6*, pp. 7–8.

147 Australian Banking Association, *Submission 29*, p. 1.

148 Australian Banking Association, *Submission 29*, p. 1.

149 Australian Banking Association, *Submission 29*, p. 1.

5.163 The ABA also noted that its understanding was that the ONDC intends to use regulations to exempt data from the Australian Prudential Regulation Authority (APRA) and the Reserve Bank of Australia (RBA) from the bill. The ABA argued that such an exemption would need to be extended to other business regulators like the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) in order to protect commercially sensitive data.[150]

Biometric data

5.164 The Law Council drew attention to the potential sharing of biometric data – that is, data that can be described as an individual's physical characteristics (such as fingerprints) which can be used to verify their identity. It highlighted the 'immutable nature' of biometric data and noted that under the Privacy Act, biometric information is defined and treated as a class of 'sensitive information' which requires a higher standard of care, specifically where use of the information is a secondary use of such information.[151]

5.165 The Law Council commented that it was unclear whether biometric data was intended to be specifically dealt with in the bill, and observed that the 'apparent lack of specific reference' to this type of data in the bill raised questions about privacy safeguards. It flagged that this may be problematic, given:

> The data sharing regime is subject to other legislation, however, if biometric data is not so covered, then it is reliant on this regime, which is a risk management regime and relies largely on good will. [152]

5.166 In relation to this, the Law Council raised the matter of consent:

> The Law Council considers the issue of consent, or lack thereof, in relation to the obtaining and subsequent sharing of such data to be a primary concern. In circumstances where biometrics are the only means of access to technology and buildings, and the data is subsequently available to be shared under this regime, the Law Council queries whether the persons subject to the biometric analysis are aware of the uses that may be made of their intimate data. This gives rise to a critical question as to whether the individual has provided meaningful consent to the use of their biometric data for external purposes, despite the fact that the purposes may be in the public interest.[153]

---

150 Australian Banking Association, *Submission 29*, p. 2.

151 Law Council of Australia, *Submission 30*, pp. 20–21.

152 Law Council of Australia, *Submission 30*, p. 21.

153 Law Council of Australia, *Submission 30*, p. 21.

5.167 It continued:

> The Law Council expresses concern at the perceived creation of 'mandatory consent' in these circumstances in the form of an agreement to share personal data in order to engage with an agency. Such situations render consent functionally meaningless.[154]

5.168 To mitigate this concern, the Law Council recommended that the bill be amended to provide that where privacy interests that involve biometric data may be affected by the data sharing scheme, all sharing of such data must be based on prior express consent.

Treatment of legal professional privilege

5.169 The Law Council argued against the proposed abrogation of legal professional privilege. It suggested the bill does not provide strong justification for why this is necessary in this instance and may impact on the willingness of participants to seek legal advice before entering into a data sharing agreement.

5.170 The Law Council proposed that section 105 of the bill be omitted, or the bill be amended to include additional controls.[155]

Indigenous considerations

5.171 The Indigenous Data Network (IDN) and the National Aboriginal Community Controlled Health Organisation (NACCHO) both raised concerns regarding the lack of specific regard given to Indigenous Australians and Indigenous public sector data in the bills. [156]

5.172 Both organisations recommended that the National Data Advisory Council established by the bill include at least one Aboriginal or Torres Strait Islander representative.[157] NACCHO noted that this would ensure considerations relating to Aboriginal and Torres Strait Islander data will be included in the advice provided to the commissioner.[158]

Committee view

5.173 The committee recognises the Australian Government's commitment to reforming public sector data sharing in response to the Productivity Commission's 2017 *Data Availability and Use* report.

---

[154] Law Council of Australia, *Submission 30*, p. 21.

[155] Mr Ian Bloemendal, Chair, Privileges and Immunities Committee, Federal Litigation and Dispute Resolution Sector, Law Council of Australia, *Proof Committee Hansard*, 20 April 2021, p. 17

[156] See for example: National Aboriginal Community Controlled Health Organisation, *Submission 23*, [p. 4]; Indigenous Data Network, *Submission 24*, [p. 4].

[157] National Aboriginal Community Controlled Health Organisation, *Submission 23*, [p. 6]; Indigenous Data Network, *Submission 24*, [p. 4].

[158] National Aboriginal Community Controlled Health Organisation, *Submission 23*, [p. 6].

5.174 It is of the view that a proportionate and balanced data sharing scheme with appropriate privacy and security safeguards would help bring Australia into line with international best practice for data sharing in regard to government service delivery, policy and program development, and research purposes.

5.175 In particular, the committee is cognisant that a well-developed data-sharing scheme has the potential to unlock benefits for the Australian community, as agreed by the majority of submitters to the inquiry.

5.176 However, the committee is mindful that for a data sharing scheme to be successful and trusted by the community it must be underpinned by strong and effective safeguards and protections for privacy and security.

Security concerns

5.177 The committee considers that it is imperative that national security concerns related to access to data have been fully considered and appropriately managed, particularly given the current concerns about cyber security and the covert influence of foreign actors in the university and research sector.

5.178 The committee recognises that a number of security safeguards are already present in the bill and welcomes the advice from the ONDC that they intend to establish memorandums of understanding with ASIO and the OAIC to clearly document the working relationship between the agencies in relation to this scheme.

5.179 The committee anticipates that the Australian Government and the Parliament will wish to be assured that in addition to upfront security assessments for data sharing participants which are already embedded in the bill, appropriate ongoing oversight is in place to manage and, wherever possible, mitigate security risks. The committee appreciates the advice of the ONDC that such mechanisms are under development.

5.180 The committee notes that the PJCIS is currently conducting an important inquiry into the national security risks affecting the Australian higher education and research sector, and is due to report to the Parliament in July 2021.

5.181 Given that universities and the research sector are expected to be one of the core participants in the proposed data sharing scheme, the committee notes the possibility that the findings of the PJCIS inquiry into national security risks in the higher education and research sector may be relevant to the ongoing management of data sharing agreements and may need to inform the development of additional data codes and guidance material.

Recommendation 1

5.182 The committee recommends that assurances are provided to Parliament regarding appropriate ongoing oversight by security agencies of data sharing agreements and potential security risks.

Recommendation 2

5.183 The committee recommends that any relevant findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector are taken into account as part of the development of any additional data codes and guidance material and inform continued engagement with the national security community.

Privacy issues

5.184 The committee notes the issues raised by stakeholders regarding privacy considerations.

5.185 The committee is of the view that, in drafting the bill and the proposed framework for data sharing, the ONDC has made substantial effort to address privacy concerns and strike an appropriate balance.

5.186 The committee notes that the bill has been designed to work with, and to be supported by, the Privacy Act (as it may be in force from time to time) rather than the bill replicating any particular point-in-time provisions from the Act. If the Privacy Act is amended in the future (for example, following the current review), the provisions of the bill will continue to operate in the context of those amended provisions.

5.187 The committee notes that the intention of the bill is to provide a high-level, principles-based framework to facilitate the sharing of government data, and that in addition to the proposed legislative privacy protections in the bill, many other potential privacy concerns would be addressed through further protections prescribed in regulation and guidance material, and in the exercise of appropriate judgement and controls by scheme users.

5.188 However, despite these layers of protection, it is evident that some stakeholders believe further privacy protections should be prescribed in legislation or specifically addressed in the EM to the bill.

Recommendation 3

5.189 The committee recommends that consideration is given to whether amendments could be made to the bill, or further clarification added to the explanatory memorandum to provide additional guidance regarding privacy protections, particularly in relation to the de-identifying of personal data that may be provided under the bill's data-sharing scheme.

Senator Claire Chandler
Chair

Labor Senators' Dissenting Report

1.1 The *Data Availability and Transparency Bill 2020* and the *Data Availability and Transparency (Consequential Amendments) Bill 2020* seeks to establish a new data sharing scheme which will serve as a pathway and regulatory framework for sharing public sector data. The bill would enable data custodians (Commonwealth bodies which control the relevant data and have a right to deal with it) to share data with accredited users, either directly or via an intermediary termed an 'accredited data service'. The bill defines data broadly to mean 'any information in a form capable of being communicated, analysed or processed (whether by an individual or by a computer or other automated means).'[1]

1.2 The bill would establish a National Data Commissioner (the Commissioner), who would serve as statutory regulator for the scheme and whose role would include advocating for the sharing and release of data more generally. The Commissioner would enforce the scheme through assessing, monitoring and investigating data scheme entities. The Commissioner would have enforcement powers, including suspension or cancellation of accreditation, injunctions, giving binding directions and seeking civil and criminal penalties where appropriate. [2]

1.3 Interactions with government services creates thousands of points of data, many of them deeply personal and sensitive. The capacity for that information to be stored, shared, processed and, in some cases, abused is greatly expanding through the development of technologies such as Artificial Intelligence. By expanding the ability for citizen's data to be shared across the public service and some third parties, the measures proposed in this bill engages and limits the right to privacy. The right to privacy may be subject to limitations where the limitation:

(a) Pursues a legitimate objective;
(b) Is rationally connected to that objective; and
(c) Is a proportionate means of achieving that objective[3]

1.4 Labor Senators are of the view that the bill is deeply flawed. While there is a clear need for an effective scheme for the management and regulation of public data, and clear public benefits from using such data, the measures outlined in this bill do not represent a proportionate means of achieving that objective. If passed, the scheme outlined in the bill would undermine current privacy

---

1 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 5.

2 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 7.

3 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, pp. 7–8.

protections, most notably the *Privacy Act 1988*. The regulatory structure designed to oversee the scheme is weak, poorly designed and subject to abuse. This bill violates community standards about the protection of private data and, if passed, would erode public trust in the government's ability to protect the privacy of its citizens.

Privacy Act 1988* and *Australian Privacy Principles

1.5 Labor Senators have concerns about the way that this bill would interact with existing privacy legislation, specifically the *Privacy Act 1988* and the *Australian Privacy Principles* (APPs). In their testimony to the committee, the Office of the National Data Commission insisted that the bill was designed to complement and not to duplicate the *Privacy Act*. The Interim National Data Commissioner described the bill's relation to the *Privacy Act* as follows:

> **Ms Anton:** The bill relates to an express authorisation to disclose, collect and to use personal information, where the requirements DAT bill are met. Basically, it's an authorised exemption, an expressed authorisation to use the bill under the Privacy Act. The Privacy Act provides for, essentially, secondary use frameworks to be met, and this bill creates a very complex set of controls about what is reasonable and practical in those instances.[4]

1.6 The Privacy Impact Assessment commissioned by the Office of the National Data Commission argues that the provisions of existing legislation will continue to provide substantial privacy protections. Chapter 5.1 provides this description of how the proposed bill will interact with the *Privacy Act*:

> When reviewing the privacy impacts of the DATB, it is important to understand that the Data Sharing Scheme will not operate in a vacuum. Existing protections provided by the Privacy Act and its APPs continue to apply. The DATB makes clear that all entities participating in the Data Sharing Scheme must 'maintain privacy coverage' either under the Privacy Act or comparable state or territory law.[5]

1.7 One particular aspect of the bill that raised concerns in both submissions and the public hearing relates to regulation of consent. In his Second Reading speech introducing the *Data Availability and Transparency Bill* to the House of Representatives, Minister Roberts emphasised that 'the bill's approach to consent mirrors the approach in the Privacy Act, requiring consent be sought for the sharing of personal information, unless unreasonable and objectionable'. [6]

1.8 The Minister's words reflect paragraph 16(2)(c) of the bill, which states that the sharing of personal information is to be done with the consent of the

---

[4] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, pp. 6–7.

[5] Information Integrity Solutions, *Privacy Impact Assessment – Data Availability and Transparency Bill 2020*, 8 March 2021, p. 26.

[6] The Hon. Stuart Robert MP, *House of Representatives Hansard*, 9 December 2020, p. 11025.

individuals concerned, unless it is 'unreasonable or impracticable' to do so. This language was criticized in the Parliamentary Joint Committee on Human Right's report on the bill, which argued that the bill is not clear about how broadly such an exception would be applied.[7]

1.9 The explanatory memorandum states that 'the question of whether seeking consent is reasonable or impracticable may depend on the amount, nature and sensitivity of the data involved, and whether individuals gave informed consent for uses including the proposed sharing at the point the data was originally collected.[8] The PJCHR Report found:

> (I)t is questionable whether an individual could be said to have voluntarily consented to the onward sharing of their data under this scheme if their original consent had been provided to meet their basic needs (for example, providing personal information to Medicare or Services Australia)… In addition, no comprehensive guidance is provided as to the circumstances in which it may be deemed unreasonable and impracticable to seek the consent of affected individuals in order to share their personal information.[9]

1.10 Similar concerns about consent in relation to data created through the provision of public services were raised by the Australian Privacy Foundation Submission:

> Australians dealing with governments typically have no choice. They are often legally obligated to provide data and to ensure that the data is correct. They are increasingly forced to provide that data through portals such as MyGov that are badly designed, badly supported and coercive. It is, at best, naïve for government representatives to state that if you don't want benefits you don't need to use those portals and you don't need to share your private lives with government.[10]

1.11 Whether this bill adequately reflects the consent protocols in existing legislation is complicated by the review of the *Privacy Act* currently being conducted by the Attorney General's Department. The review was a recommendation of the Australian Consumer Commission's (ACCC) Digital Platforms Inquiry and announced on 12 December 2019. Submissions for the review have closed – and a discussion paper is expected to be released this year. The inquiry's Terms of Reference clearly relate to matters that are of direct concern to this bill, including:

- The scope and application of the Privacy Act including in relation to:
  - The definition of 'personal information'
  - Current exemptions, and

---

7 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 11.

8 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 24.

9 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 12.

10 Australian Privacy Foundation, *Submission 28*, p. 4.

  - General permitted situations for the collection, use and disclosure of personal information.
- Whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices including in relation to:
  - Notification requirements
  - Consent requirements including default privacy settings
- The effectiveness of enforcement powers and mechanisms under the Privacy Act and the interaction with other Commonwealth regulatory frameworks.[11]

1.12 It is unusual that a bill that relies on the mechanisms outlined in the *Privacy Act* would be developed and introduced to the Parliament before a major review of the *Privacy Act* is completed. During the public hearing, a number of witnesses commented on these circumstances:

> **Mr Gadir:** This bill is a really big carve-out from the protections of the Privacy Act applying to a very high-risk activity of data sharing. This is happening at the same time that another arm of the government is telling us that they want to strengthen the Privacy Act.[12]
>
> …
>
> **Dr Arnold:** With respect, I think the bill should not be passed until we've looked at and, ultimately, fixed the existing weak regime.[13]
>
> …
>
> **Ms Ganopolsky:** There is a risk that you are putting the cart before the horse. What is contemplated under this bill is a very large data-sharing arrangement that is systemic in nature. What is contemplated under the review of the Privacy Act is, potentially, an overhaul of the regime… So, from the point of view of building a series of infrastructure, you are, potentially, putting the cart before the horse in that it will have to respond to a brand new regime.[14]
>
> …
>
> **Ms Krahulcova:** It does not make I think policy sense to be passing this legislation while money is being spent reviewing the Privacy Act,

---

[11] Attorney-General's Department, *Review of the Privacy Act 1988 – Terms of Reference, 30 October 2020*, www.ag.gov.au/integrity/publications/review-privacy-act-1988-terms-reference (accessed 28 April 2021).

[12] Mr Jonathan Gadir, Member, New South Wales Council for Civil Liberties, *Proof Committee Hansard*, 20 April 2021, p. 15.

[13] Dr Bruce Baer Arnold, Vice Chair, Australian Privacy Foundation, *Proof Committee Hansard*, 20 April 2021, p. 19.

[14] Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia, *Proof Committee Hansard*, 20 April 2021, pp. 19–20.

> especially if this legislation as primary legislation will be exempt from the resulting rules and standards in that review.[15]

1.13 The *Privacy Act's* approach to consent appears to be a subject of the Privacy Act Review. The Issues Paper for the review, released in October 2020, includes several references to consent and includes an outline of the way consent operates under the Act. It describes *Australian Privacy Principle (APP) 6* – which outlines the use or disclosure of personal information – as follows:

> APP 6 permits an entity to use or disclose the collected personal information without obtaining consent provided it is for the primary purpose for which it was collected, or for a secondary purpose if the individual would reasonably expect the entity to use or disclose their personal information was collected.[16]

1.14 Question 42 of the Review's questions for consideration is: 'Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?'.[17]

1.15 It is concerning that the bill pre-empts the Privacy Act Review because it is precisely those consent protocols regarding personal information, outlined in the *Privacy Act 1988* and *APP 6* in particular, that are contested by the bill's critics:

> **Mr Gadir:** Earlier, the witnesses from the government were explaining how the Privacy Act would continue to apply, but that is not correct. The fundamental disclosure from the government agency to some private company that would be enabled by this bill is actually a carve-out from Australian Privacy Principle 6… It says you can only use or disclose personal information where it's reasonably expected by the individual and it's related to the primary purpose of collection.[18]
>
> …
>
> **Ms Krahulcova:** In our submission we brought up the fact that privacy principle 6 is essentially being rewritten, and that the primary [inaudible] definition. There are exceptions to that in the existing privacy principles, but this is a top-down override of privacy principle 6 and it is a blunt

---

[15] Ms Lucie Krahulcova, Executive Director, Digital Rights Watch Inc, *Proof Committee Hansard*, 20 April 2021, p. 26.

[16] Attorney-General's Department, *Review of the Privacy Act 1988 – Issues Paper*, 30 October 2020, www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper, p. 41 (accessed 28 April 2021).

[17] Attorney-General's Department, *Review of the Privacy Act 1988 – Issues Paper*, 30 October 2020, www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper, p. 11 (accessed 28 April 2021).

[18] Mr Jonathan Gadir, Member, New South Wales Council for Civil Liberties, *Proof Committee Hansard*, 20 April 2021, p. 19.

> approach that dilutes legal protections and remedies currently available to Australians, and there are not many to begin with.[19]

1.16 Labor Senators note that there are substantial problems in the way the bill interacts with the *Privacy Act 1988*, most notably with regard to *Australian Privacy Principle 6* as it relates to the treatment of consent in the collection and distribution of personal information. Further, it is the view of Labor Senators that attempting to pass such measures before the completion of the Attorney General's review of the *Privacy Act* is reckless, and undermines claims that the bill was developed through a 'privacy-by-design' process.

Inadequate Regulation of Data Matching

1.17 Labor Senators are concerned that the regulatory mechanism outlined by this bill is insufficient for the scope of the data-matching scheme it creates. Datasets created through government data-matching are highly valuable, and the practice of data sharing is considered high risk. As the bill's Privacy Impact Assessment outlines – the DATB's expansion of such practices requires stronger controls:

> What is significant are changes to processes and scale. Also significant is the social and technological environment in which the DATB's Data Sharing Scheme would operate. The advent of new technologies like data analytics, artificial intelligence, face recognition – and indeed the combination of these technologies – as well as increased inherent security risks when sharing data must also be considered.[20]

1.18 The bill provides for the establishment of the National Data Commissioner as a statutory regulator for the scheme, while at the same time 'advocating for the sharing and release of data more generally'. The Commissioner would be empowered to enforce the scheme, including by assessing, monitoring and investigating data scheme entities. Their enforcement powers would include the ability to suspend, cancel or impose conditions on an entity's accreditation; issue written directions to a data scheme entity; impose a civil penalty; issue infringement notices; accept and enter into enforceable undertakings and apply for injunctions.[21]

1.19 The Commissioner's dual role as both 'advocate' and 'regulator' is an immediate weakness in the scheme's regulatory structure. The PJCHR report on the bill raised concerns about whether the Commissioner could provide

---

[19] Ms Lucie Krahulcova, Executive Director, Digital Rights Watch Inc, *Proof Committee Hansard*, 20 April 2021, p. 26.

[20] Information Integrity Solutions, *Privacy Impact Assessment – Data Availability and Transparency Bill 2020*, 8 March 2021, p. 85.

[21] Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 7.

genuine independent regulatory oversight of the scheme.[22] As the Electronic Frontiers Australia submission states:

> 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 those roles effectively, but not both.[23]

1.20 The Australian Privacy Foundation raised concerns about the relationship of the National Data Commissioner to existing regulatory bodies:

> **Dr Arnold:** The bills are not accompanied by a strengthening of the Office of the Australian Information Commissioner, our regrettably inward looking and grossly under-resourced privacy and FOI watchdog. The bills obfuscate recurrent civil society requests for privacy protection. They do that by Balkanising responsibility, with the new Data Commissioner sitting alongside the information commissioner and other agencies.[24]

1.21 The regulatory role of the Commissioner is further complicated by the limited scope to review and overturn its decisions. The bill's Explanatory Memorandum states that regulatory decisions by the Commissioner may be reviewed for their merits or legality through standard administrative review processes.[25] However, the EM also outlines how a number of the Commissioner's decisions will not be subject to such a review:

> Decisions made under the Commissioner's advice, guidance, advocacy, and incidental functions are not appropriate for merits review… Delegation decisions are also unsuitable for merits review… Decisions to appoint persons to undertake specified functions, such as to appoint members of the National Data Advisory Council, are also generally not appropriate for review.[26]

1.22 The central role of the Commissioner in the regulation of this scheme, including the power to delegate concerns to other regulators, while having significant exclusions to judicial review, ultimately means that critical decisions about privacy rights will be delegated to senior public servants, overseen by an appointed commissioner rather than any judicial process. Those public servants, referred to in the bill as 'data custodians', will also be responsible for designing and implementing data matching schemes. Despite this clear conflict of interest, the regulator maintains that they are capable of making informed and appropriate decisions:

---

22 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 14.

23 Electronic Frontiers Australia, *Submission 21*, p. 8.

24 Dr Bruce Baer Arnold, Vice Chair, Australian Privacy Foundation, *Proof Committee Hansard*, 20 April 2021, p. 16.

25 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 10.

26 Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, pp. 70–71.

> **Ms Anton:** So, while we haven't imported the Privacy Act into the bill, those really important links under 28 and the capacity to refer things out to the Privacy Commissioner do maintain the importance of privacy in the work that we're doing and still rest that control, where it's most appropriately dealt by with the Privacy Commissioner, with her.
>
> **Senator AYRES:** It does put a lot of power in the hands of the Data Commissioner, many of whose decisions will be non-reviewable.
>
> **Ms Anton:** I would just note that the decisions to share the data are ultimately left with the data custodians. So they're left with senior public servants. Our view was that, in terms of sharing, they are in the best position to make an appropriate risk assessment.[27]

1.23 While the regulator is relying on the judgement of senior public servants to make decisions about data sharing in line with community expectations and their legal responsibilities under the *Privacy Act* and the *Australian Privacy Principles*, the Explanatory Memorandum of the bill indicates that those critical decisions will be exempt from judicial review:

> Data sharing decisions by data custodians will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data.[28]

1.24 The scheme's emphasis on allowing senior public servants to make critical decisions about the appropriateness of data-matching was criticised by several witnesses during the public hearing:

> **Mr Wong:** Ms Anton also emphasized the role of data custodian and for clarification that really means the Commonwealth government agency who holds that information. They have outsized power and a level of discretion in determining who gets access to what data, what data can be shared, what data falls within the purposes, whether the data can fall within the purpose of improving government policy or research and development, which can be very broadly interpreted, as well as whether it is unreasonable or impracticable for them to obtain consent and, then, the circumstances in which the data is shared and to what agencies they may share this information… There isn't really any form of oversight in that sharing and there are no merits review processes.[29]
>
> **…**
>
> **Dr Arnold:** We have nice language that government agencies will be custodians… They regard this data as their data: 'It's government data. We

---

[27] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 7.

[28] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 10.

[29] Mr Chadwick Wong, Senior Solicitor, Public Interest Advocacy Centre, *Proof Committee Hansard*, 20 April 2021, p. 18.

> can do with it what we like.' We will in practice have very weak oversight of what's happening.[30]
>
> …
>
> **Mr Payne:** A key concern to the university is the absence of a definition for the term 'public benefit' in the main bill, even though data custodians across the Commonwealth will be required to apply this test each time they consider a request for data.[31]

1.25 Further, there are concerns that the bill lacks substantial enforcement mechanisms. Considering the value of the datasets being created and the sensitive nature of the data being shared, the civil and criminal penalties included in the bill are relatively small:

> **Mr Menzies-McVey:** For breach of the mandatory terms of a data sharing agreement, which include the requirement to only use it for the agreed purpose, it's a civil penalty of 300 penalty units… there are general penalties applying for if the sharing or use was purporting to rely on the authorization in the bill and the bill doesn't cover that, in fact. There are both civil penalties, which are the 300 penalty units, and criminal penalties, which is imprisonment for two years, for intentional reckless breaches.[32]

1.26 The civil penalties included in this bill are not proportional to the value of the data, the probity risks that such a scheme would create nor the harm that a breach of such sensitive data would have. As the Electronic Frontiers Australia witness said:

> **Mr Warren:** … data privacy, like life, once it's gone, it's lost forever. Intent is the difference between murder and manslaughter: the victim is still dead. In this case, our privacy has still been invaded; it's still been lost. We can't ever get that back, and what we see here are things like civil penalties of 300 penalty rates, which at the current rate works out at around $66 000. Personal information is extremely valuable. If I managed to get hold of a data leak of every Australian's medical record, 66 grand sounds like a pretty fair fee. You can pay more than that to various brokers to get access to datasets… we need to have a system that deals with bad intents and bad outcomes.[33]

---

[30] Dr Bruce Baer Arnold, Vice Chair, Australian Privacy Foundation, *Proof Committee Hansard*, 20 April 2021, p. 18.

[31] Mr Tim Payne, Director, Higher Education Policy and Projects, Office of the Vice-Chancellor and Principal, University of Sydney, *Proof Committee Hansard*, 20 April 2021, p. 22.

[32] Mr Paul Menzies-McVey, Assistant Secretary, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 6.

[33] Mr Justin Warren, Board Member Electronic Frontiers Australia, *Proof Committee Hansard*, 20 April 2021, p. 28.

1.27 Labor Senators agree with the findings of the Parliamentary Joint Committee for the Scrutiny of Bills that the Explanatory Memorandum lacks a comprehensive justification for the penalties outlined in the bill.[34]

1.28 Labor Senators are of the view that 300 penalty units (currently $66 000) is an insufficient disincentive for breaching the law. Effective penalties for the misuse of data should be a substantial order of magnitude higher than the value of the data shared.

1.29 It is the view of Labor Senators that the regulatory scheme outlined in this bill is weak, poorly designed and ultimately unable to protect the right to privacy under this scheme. Both the National Data Commissioner and the data custodians they are entrusted to regulate have substantial conflicts of interest by design. Excluding the decisions of senior public servants entrusted with valuable personal data from judicial review is of particular concern. Such a scheme is inadequate to the scale of its exemptions to the *Privacy Act* and the *Australian Privacy Principles*.

Robodebt, Compliance and the National Disability Insurance Scheme

1.30 Labor Senators have concerns that the data-sharing scheme created by this legislation could be abused to create new forms of inequity and neglect. The recent 'Robodebt' scandal, in which the government attempted to recover 'overpayments' made to social security recipients through its *Online Compliance Initiative (OCI)*, provides a clear example. The scheme was found to be unlawful - and resulted in the largest class action settlement in Australian history. It is currently the subject of another Senate Inquiry, which is due to report in 2021.

1.31 As outlined in the 2017 report of the Senate Standing Committee on Community Affairs, the 'debts' were calculated from the cross-referencing of Centrelink recipient data with records from the Australian Tax Office. Cross-referencing using Tax File Numbers (TFNs) had been longstanding practise in Centrelink - having been facilitated by *the Data-matching Program (Assistance and Tax) Act 1990 (Data-matching Act)*. This act allowed the Officer of the Australian Information Commissioner (OAIC) to make legally binding rulings on how such data can be matched.[35]

1.32 However, as part of the introduction of the *Online Compliance Initiative (OCI)* program in 2016, the Department of Human Services stopped the practice of using TFNs to make their calculations, meaning that the program was not legally bound by the Data-matching Program Act. Instead, they were subject to

---

[34] Senate Standing Committee for the Scrutiny of Bills, *Scrutiny Digest 1 of 2021*, 29 January 2021, p. 9.

[35] Senate Community Affairs References Committee, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*, June 2017, Chapter 2.

voluntary, non-binding guidelines issued by the OAIC on data-matching, which allow for greater flexibility as to how data-matching activities may be conducted and did not restrict the volume of data matching activity. The increased volume of data matching - particularly through full automation – and the loosened restrictions on the quality of the data used created the basis of the Robodebt scheme.[36]

1.33 Robodebt represented a failure to appropriately regulate data sharing between government departments, and its example has implications for the *Data Availability and Transparency Bill 2020*. It was noted in the hearings that the bill nominally precludes sharing data for compliance purposes in Clause 15. As the Explanatory Memorandum states:

> … subclause (3)(b) precludes sharing for the purpose of detecting, investigating or addressing (a compendious phrase) deliberate actions that are detrimental to public revenue, like fraud. While enforcement related activities are legitimate functions of government, they are best carried out under dedicated laws.[37]

1.34 The bill as drafted does not resolve issues of data matching across agencies in existing legislation, such as the *Data Matching Program Act 1990*. As the chart tabled by the National Data Commissioner indicates,[38] data that can be shared under existing authority can be shared through existing processes. *The Data Availability and Transparency Bill 2020* is only implemented when those existing authorities and processes do not apply. It therefore fails to improve the management of current privacy risks.

1.35 Further, there is concern that the protections against the use of the bill for compliance purposes are weak given the broadly-framed purposes for which data can be shared under the scheme. These concerns were raised in clause 1.23 of the Parliamentary Joint Committee on Human Rights report on the legislation:

> (I)t is unclear whether the 'delivery of government services would encompass the sharing of data for purposes related to the withholding of government services (such as identifying ways in which to reduce certain social security payments).[39]

1.36 During the public hearing the example of the National Disability Insurance Scheme was raised. Recent press reports have indicated that the National

---

[36] Office of the Australian Information Commissioner, *Submission 10* to the Senate Community Affairs References Committee, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*, June 2017.

[37] Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p. 23.

[38] Office of the National Data Commissioner, *How will the Data Availability and Transparency Act work?*, April 2021, p. 1 (tabled 20 April 2021).

[39] Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, pp. 9–10.

Disability Insurance Agency is planning to use 'data matching and analytics' to 'identify high-risk activities, non-compliant participant plan usage and other potential areas of risk.' [40]The question was put to the Office of the National Data Commissioner whether information shared through the bill would be able to be used in such a process.

> **Ms Anton:** I don't see how enforcement action under NDIS would be supported by the bill as drafted.[41]

1.37 However, through questioning it was established that the breadth of information that can be collected would allow data to be used to determine the appropriate level of support a NDIS recipient would receive. As the PJCHR report indicates,[42] there is a close relationship between this information and the potential for enforcing a compliance regime – creating a loophole in the bill's stated protections.

> **Senator AYRES:** Is it possible for the NDIA to use this framework to collect data that is then used to make assessments about the level of support that's provided to individuals?
>
> **Ms Anton:** I think that goes to individual identified information. The bill contemplates that, where individual information is provided, it's also relevant to make reference to probably the exit clause, which does include a step where individuals are importantly required to validate that the information there is correct for that to go on and be used for other purposes. So, yes.[43]

1.38 Concern about the role data collected through the scheme could play in the proposed NDIS compliance scheme were also raised by the Public Interest Advocacy Centre:

> **Mr Wong:** What we've seen proposed, for example, in the NDIS is around clawing back funds that have been used by participants in ways that the agency considers to be inappropriate… that is an example of something which may not be in contravention of the law and may not be captured by the exclusions in the act.[44]

1.39 It is the opinion of Labor Senators that given the recent example of the Robodebt scheme, the potential for data-matching collected under this bill to

---

[40] Rick Morton, 'Robo-debt public servants now shaping the NDIS', *The Saturday Paper*, 10 April 2021, www.thesaturdaypaper.com.au/news/politics/2021/04/10/robo-debt-public-servants-now-shaping-the-ndis/161797680011420 (accessed 28 April 2021).

[41] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 8.

[42] Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 10.

[43] Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, pp. 8–9.

[44] Mr Chadwick Wong, Senior Solicitor, Public Interest Advocacy Centre, *Proof Committee Hansard*, 20 April 2021, pp. 17–18.

be misused in a compliance function by the NDIA is of great concern. It is a practice that would disproportionately harm the most vulnerable in our society, and potentially deny them the government services they need to live with dignity. The stated protections against the use of the data collected by this act are ultimately negated by its broad scope.

Conclusion

1.40 Labor Senators agree with the findings of the Parliamentary Joint Committee for Human Rights that the bill seeks to establish a framework that overrides existing laws to facilitate the sharing of, and controlled access to, public sector data held by Commonwealth bodies with accredited entities.[45] Labor Senators agree with the findings of the PJCHR that, in doing so, the measure engages and limits the right to privacy and notes that this right may be subject to permissible limitations if they are shown to be reasonable, necessary and proportionate.[46]

1.41 Labor Senators do not believe that the measures outlined in this bill represent a reasonable, necessary or proportionate limitation on the right to privacy. The failures of this legislation can be effectively summarised by a single exchange from the public hearing:

> **Senator AYRES:** Who do you think owns the data?
>
> **Ms Anton:** My general sense is we, the government, hold the data in trust for the public. They do provide that information, and it's a responsibility, as with many functions of the government, to hold that in good faith for the public.[47]

1.42 Citizens are entitled to trust their government with the data they provide, often without their consent. They are entitled to believe that their data will be appropriately respected and protected, and that any scheme that holds or shares their data would be subject to appropriate judicial review. The scheme outlined in this bill does not deserve their confidence. This bill would undermine the existing privacy protections in favour of a poorly regulated system that is widely open for abuse. It amounts to a reckless treatment of public trust.

---

45 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, pp. 17–18.

46 Parliamentary Joint Committee on Human Rights, *Report 2 of 2021*, 24 February 2021, p. 18.

47 Ms Deborah Anton, Interim National Data Commissioner, Department of the Prime Minister and Cabinet, *Proof Committee Hansard*, 20 April 2021, p. 6.

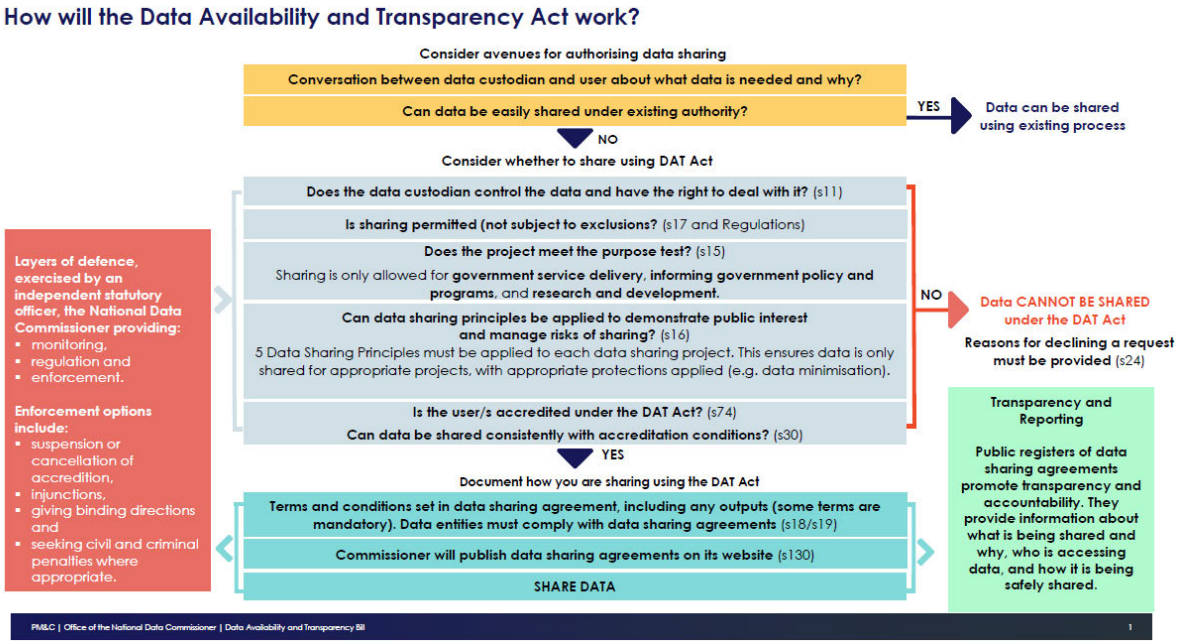
Recommendation 1

1.43 That the bill not be passed.

Senator Tim Ayres
Deputy Chair

Appendix 1
How will the Data Availability and Transparency Act work?

Figure 1.1 How will the Data Availability and Transparency Act work?



[Source: Office of the National Data Commissioner, How will the Data Availability and Transparency Act work?, tabled 20 April 2021.]

Appendix 2
Submissions and additional information received by the committee

Submissions

1 Australian Urban Research Infrastructure Network (AURIN)
2 Ms Melanie Marks, Ms Anna Johnston and other interested parties
3 BSA | The Software Alliance
4 Data Republic
5 Research Australia
6 Public Interest Advocacy Centre
7 Australian Academy of Science
8 Australian Research Data Commons
9 Group of Eight
10 National Archives of Australia
11 The George Institute for Global Health
12 GovHack Australia Limited
13 Australian Medical Association
14 Verifier
15 Universities Australia
16 Office of the Australian Information Commissioner
17 Population Health Research Network
18 University of Sydney
19 Dr Megan Prictor and Associate Professor Mark Taylor
20 Office of the National Data Commissioner
21 Electronic Frontiers Australia
22 Allens Hub for Technology Law and Innovation, Australian Society for Computers and Law, UNSW Institute for Cyber Security
23 National Aboriginal Community Controlled Health Organisation
24 Indigenous Data Network
25 Digital Rights Watch Inc.
26 Minderoo Tech & Policy Lab – University of Western Australian Law School
27 NSW Council for Civil Liberties
28 Australian Privacy Foundation
29 Australian Banking Association
30 Law Council of Australia
- 30.1 Supplementary to submission 30

31 *Name Withheld*

Additional Information

1 Additional information from the Office of the National Data Commissioner; received 22 April 2021.

Answer to Question on Notice

1 Answer to a question taken on notice by the Office of the National Data Commissioner at a public hearing on 20 April 2021; received 22 April 2021.

Tabled Documents

1 Office of the National Data Commissioner – 'Opening statement' – tabled at a public hearing in Canberra, 20 April 2021

2 Office of the National Data Commissioner – 'How will the Data Availability and Transparency Act work?' – tabled at a public hearing in Canberra, 20 April 2021

Appendix 3
Public hearings

Tuesday, 20 April 2021

Committee Room 2S1
Parliament House
Canberra

Office of the National Data Commissioner

- Ms Deborah Anton, Interim National Data Commissioner
- Mr Paul Menzies-McVey, Assistant Secretary

Public Interest Advocacy Centre

- Mr Chadwick Wong, Senior Solicitor (via videoconference)

NSW Council for Civil Liberties

- Mr Jonathan Gadir, Committee Member (via videoconference)

Australian Privacy Foundation

- Dr Bruce Baer Arnold, Vice-Chair

Law Council of Australia

- Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section (via videoconference)
- Mr Ian Bloemendal, Chair, Privileges and Immunities Committee, Federal Litigation and Dispute Resolution Service (via videoconference)
- Mr Nathan MacDonald, Principal Policy Lawyer (via videoconference)

University of Sydney

- Mr Tim Payne, Director, Higher Education Policy and Projects, Office of the Vice Chancellor and Principal (via videoconference)
- Dr Adele Haythornthwaite, Research Data Consulting Lead, Sydney Informatics Hub (via videoconference)

Digital Rights Watch Inc.

- Ms Lucie Krahulcova, Executive Director (via videoconference)

Electronic Frontiers Australia

- Mr Justin Warren, Board Member (via videoconference)