Australian Government
Attorney-General's Department

17 January 2017

Submission on Draft Report

Productivity Commission inquiry into Data Availability and Use

Contents

General comments

AGD is broadly supportive of the proposals in the Productivity Commission's Draft Report on Data Availability and Use. Appropriate regard appears to have been given to the need to protect personal information and address privacy issues. We raise below issues regarding specific recommendations for further consideration. We also provide information that may be of use to the Commission in finalising its report.

As a general comment, we note that making data accessible to all Australians is not cost neutral. Agencies will need to invest significant resources to increase access at the cost of other activities. The Draft Report would benefit from providing more information on the likely costs for agencies in implementing the Commission's recommendations.

Australia's international human rights obligations

Several of the recommendations in the Draft Report may have implications for Australia's international human rights obligations. Ensuring consistency with Australia's obligations would largely be an exercise when (and if) government sought to implement the recommendations. AGD suggests that it may be useful for the Commission to acknowledge Australia's obligations relevant to regulating access to information (see table below), to pre-empt criticism that may arise in that regard and as relevant context to its work. Also, it may be useful to explain that the *Privacy Act 1988* (Privacy Act) implements the right to privacy under article 17 of the International Covenant on Civil and Political Rights (ICCPR).

Source	International human right obligation	Restrictions permitted
Article 19 ICCPR	Right to freedom of expression, including the freedom to seek, receive and impart information	Freedom of expression may be subject to restrictions provided by law that are necessary for the respect of the rights or reputations of others (for example, the right to privacy, see below) or for the protection of national security or public order or of public health and morals.
Article 17 ICCPR	Prohibits arbitrary or unlawful interferences with privacy.	Australia is obliged to ensure that any such interferences with privacy are both lawful (that is, authorised under domestic law) and non-arbitrary.[1]

In considering issues of availability of data it is important that accessibility also be considered. Universal accessibility requires investment of time, finances and resources, but it is critical to build inclusive communities. Australian Government agencies are required to provide services in a non-discriminatory manner and make reasonable adjustments under the *Disability Discrimination Act 1992* (Cth). One way in which agencies address accessibility issues is through compliance with the Australian Government's commitment to providing accessible web information, content and services to all Australians regardless of disability, culture or environment. For example, the Government adopts the *Web Content Accessibility Guidelines Version 2.0*. The Guidelines set out the minimum standards for government adherence to ensure accessibility. Accessibility is critical for individuals to be able to use the data as proposed in the Draft Report.

[1] In order for an interference with privacy not to be 'arbitrary', the interference must be reasonable in the particular circumstances. The United Nations Human Rights Committee, in its General Comment No 16 on the right to privacy, has acknowledged that the use of personal information by public authorities is permissible where its collection is essential in the interests of society.

Data registers (recommendation 3.1)

The Draft Report applies a 'one-size-fits-all' response to address concerns relating to specific circumstances and/or data sets. AGD considers that greater investigation of the benefits and costs of increasing the availability and improving the use of data is required. A staged approach to implementation, focusing on those data sets with greatest potential to generate economic gain would be preferable, allowing experience to guide implementation across the much broader range of agencies in the government.

Recommendation 3.1 states that all Australian Government agencies should create comprehensive, easy to access data registers (listing both data that is available and that which is not) by 1 October 2017 and publish these registers on data.gov.au. Limited exceptions for high sensitivity datasets would apply.

It would be useful for the Commission to provide guidance in relation to the definition of 'data' for which registers would be required (is it any collection of information, must it be structured, must it be in a particular system which allows for interrogation). Guidelines and tools to assist information custodians to consistently identify data sets of value will need to be developed. A key barrier to the success of data policies is the lack of awareness that information holdings, or even the metadata, could be seen by external parties as a data set of value. The ongoing issue of cost of preparing, extracting and releasing data (particularly where this is not held in a system which allows for this to occur easily), as well as requiring potentially new skills sets to manage this process, will be a significant issue in some instances.

Credit reporting (recommendation 4.1)

The Draft Report recommends that the Australian Government adopt a minimum target for voluntary participation in the comprehensive credit reporting system (CCR) of 40% of accounts and that if this target is not achieved by 30 June 2017, the Government should circulate draft legislation to impose mandatory reporting by 31 December 2017.

The benchmarking of voluntary participation and possible mandating of participation in CCR is primarily a matter for Treasury as it would be likely to involve Australian credit licensees, authorised deposit-taking institutions, or subsets thereof. By contrast a credit provider is defined with broad scope under the Privacy Act to include any entity that provides goods or services on credit for at least 7 days.[2] The broad definition of 'credit provider' in the Privacy Act would make it difficult to assess the participation in CCR of all entities that fall into this definition and would mean that the regulatory cost of any subsequent decision to mandate their participation in CCR would be likely to outweigh any benefits. The Draft Report should clarify the subsets of credit providers with which it is primarily concerned.

However, AGD thinks the recommendation timeframe appears premature given the relatively brief period of time since the commencement of CCR in March 2014, and the subsequent authorisation of the industry code regulating the exchange of information in the credit reporting system (the Principles of Reciprocity and Data Exchange (PRDE)) in December 2015. We note that the Financial Systems Inquiry Final Report commented that Government should review in 2017 industry's participation in CCR to determine whether a regulatory incentive or legislation for mandatory reporting was required. However, the 2008 Australian Law Reform Commission Report 108 recommended a review of CCR five years from commencement[3].

[2] Section 6G(2) of the Privacy Act. Section 6 defines 'credit provider' by reference to sections 6G to s6K of the Act.
[3] ALRC, *For Your Information: Australian Privacy and Practice*, report 108, May 2008, recommendation 54-8.

A review in 2019 (five years after the 2014 commencement) would ensure the new credit reporting provisions and the PRDE are given a chance to be fully implemented by industry, consistent with the Office of the Australian Information commissioner's (the OAIC's) submission to this inquiry.[4] Also, we recommend the Commission consider whether the mandating of participation in CCR may raise constitutional issues around the acquisition of property and, if so, would require the Australian Government to pay compensation on just terms to credit providers for compelling them to disclose valuable commercial information.

If the Commission wishes to retain the recommendation, we note that, as currently drafted, the reference in recommendation 4.1 to 'mandatory reporting' is unclear and open to considerable interpretation. AGD's preference would be to replace the reference with 'mandatory participation in Comprehensive Credit Reporting' for greater clarity and consistency.

In addition, consideration should be given to specifying more precisely in recommendation 4.1:

- Which providers each of the requirements (voluntary and mandatory) would apply to
- Which information the requirements would apply to, ie consumer credit liability information only, or repayment history information as well (noting that only credit providers that are licensees can provide and access repayment history information)

Hardship

The Report comments that greater clarity on how hardship provisions should interact with CCR could help pave the way for broader industry participation or alternatively that the inclusion of a hardship flag in credit reports could address the concerns expressed by participants to the inquiry. The treatment of hardship in the credit reporting system is primarily a matter for the Treasury as hardship is provided for in the National Credit Code. AGD will work with the Treasury on any relevant hardship issues.

While the draft report comments that issues around repayment history information and hardship have been identified by participants as discouraging participation in the credit reporting scheme, we note that the retail credit industry has previously stated the issue will not prevent or impact on the transition to comprehensive credit reporting.[5] We note that the inclusion of hardship provisions raises policy issues that need to be explored, particularly from the consumer perspective, and that concerns have been raised that the inclusion of hardship information in the credit reporting system could be a disincentive for hardship applications and may trigger other complications for people trying to resolve financial difficulties.[6]

Trans-Tasman credit reporting

In 2008, the Australian Law Reform Commission report on privacy recommended changes to facilitate the sharing of credit reporting information with New Zealand.[7] AGD notes that sharing of credit reporting information between Australia and NZ has the potential to be beneficial for consumers, by increasing the portability of good credit history, and for industry, by making it harder for consumers to avoid credit obligations.

---

[4] Office of the Australian Information Commissioner, *Submission to Productivity Commission Issues Paper*, page 45.
[5] Australian Retail Credit Association, *Between the flags: Repayment History Information (RHI) for consumers in financial hardship*, page 4.
[6] Financial Rights Legal Centre submission to the Data Availability and Use Issues Paper, page 6.
[7] ALRC, *For Your Information: Australian Privacy Law and Practice*, report 108, Recommendations 54-6 and 54-7.

However, we note that there are some important differences between the Australian and NZ systems that would need to be worked through. Firstly, legislation amendments would be required to adjust the existing prohibitions in the Privacy Act. Currently, the consumer credit reporting system is restricted to information about consumer credit in Australia and access to the credit reporting system is only available to credit providers in Australia.[8] In 2009, the previous government stated an intention that the Privacy Act be amended to allow credit reporting information to be shared between the Australian and NZ consumer credit reporting systems in defined circumstances.[9] This intention is reflected in the Explanatory Memorandum for the legislation that introduced CCR.[10]

Secondly, implementation of a Trans-Tasman credit reporting scheme would require the negotiation of treaty level arrangements to ensure that sufficient safeguards exist to protect information. The Privacy Act cannot regulate conduct that is regulated by New Zealand or beyond Australian jurisdiction under international law. Also, a treaty would ensure consistency in the way that information is used once it has been disclosed (eg NZ currently permits employers to access credit reporting information but Australia does not). A treaty would also support a complaints handling mechanism.

AGD will continue work on this matter.

Proposed role for the OAIC (recommendation 5.1)

AGD considers that the proposal for the OAIC to develop and publish practical guidance on best practice de-identification is consistent with the OAIC's existing guidance related functions under section 28 of the Privacy Act.

However, AGD does not support the recommendation in 5.1 that the OAIC should be afforded power to certify when entities are using best practice de-identification processes. This proposed power is not consistent with the OAIC's existing functions and is not a role for which the OAIC would have the necessary technical expertise. It also sets up a potential conflict if the OAIC were to both endorse the de-identification method used by an entity but then adjudicate any related complaint about a privacy breach in relation to that entity. We suggest this certification role could more appropriately sit with the proposed National Data Custodian, at least in relation to the public sector, as this would complement the existing proposed function of accrediting the Accredited Release Authorities. In the private sector, entities should be encouraged to create their own accreditation approaches.

Data management standards (recommendation 6.1)

The Draft Report recommends that government agencies should adopt data management standards to support increased data availability and use as part of their implementation of the Australian Government's Public Data Policy Statement. Recommendation 6.1 also states that policy documents outlining the standards and how they will be implemented should be available in draft form for consultation by the end of 2017, with standards implemented by the end of 2020.

---

[8] Part IIIA of the Privacy Act prohibits Australian credit reporting bodies from disclosing credit reporting information unless the disclosure is to a credit reporting body that has an 'Australian link'. The credit information that is disclosed must also relate to credit that is or has been provided, or applied for, in Australia.

[9] Former government response to ALRC Report 108, pp 102–3.

[10] Explanatory Memorandum, Privacy Amendment Bill 2012, p 92.

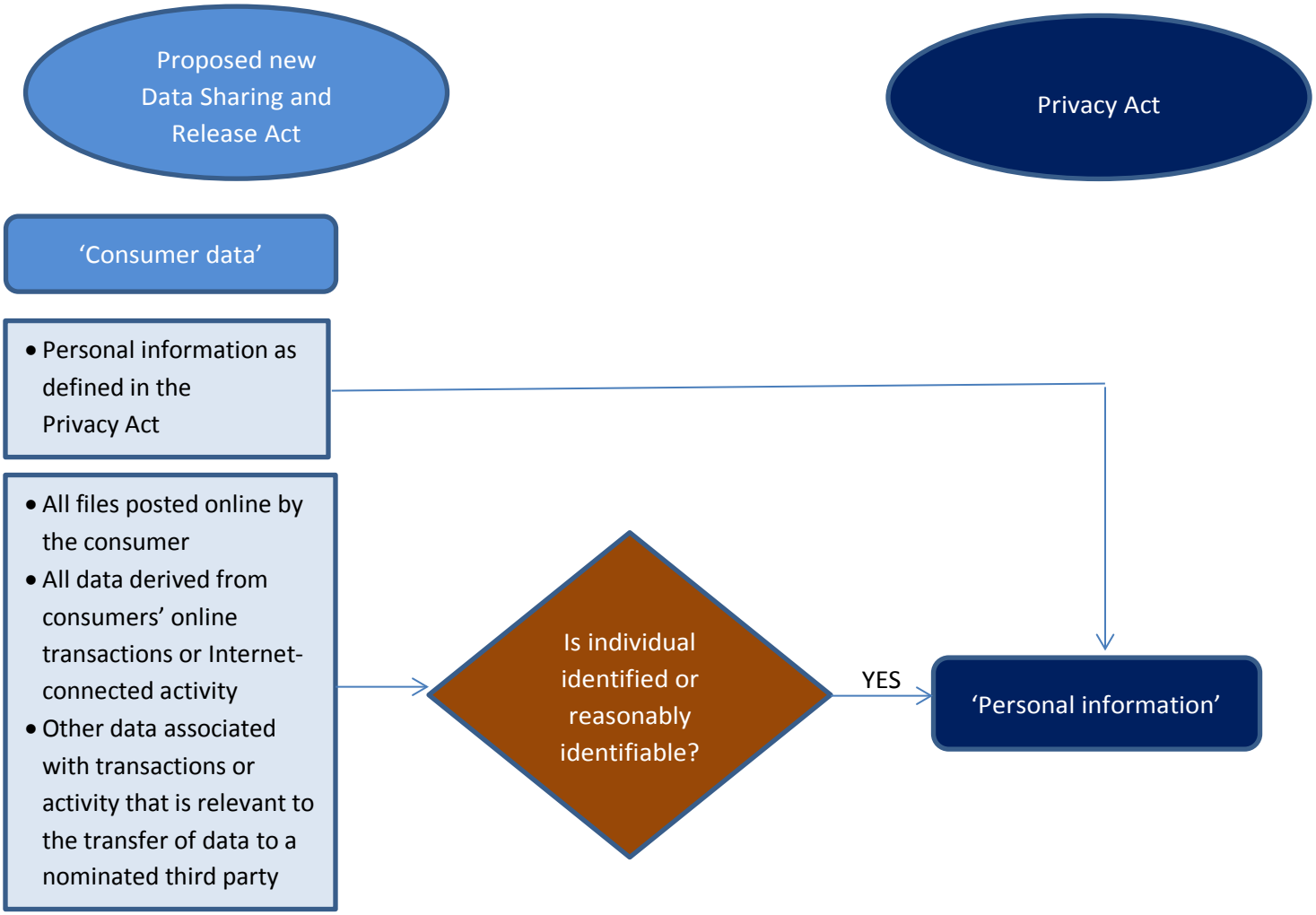
Under Recommendation 6.1, agencies that do not meet sector-specific standards would be noted as not fully implementing the Australian Government's Public Data Policy and would be required to work under a nominated Accredited Release Authority to improve the quality of their data holdings.

AGD's view is that the ongoing costs and complexity of developing and maintaining data management standards should be further considered, particularly in the context of Machinery of Government changes. Where data collections are commenced under one standard there may be complexities if transferred to another agency with significantly different, or non-complementary, standards.

Definition of consumer data (recommendation 9.1)

The interaction of the proposed definition of 'consumer data' with the existing definition of 'personal information' in the Privacy Act should be further explored. The Privacy Act is technology neutral with a broad definition of 'personal information'. It is clear that the proposed new definition of 'consumer data' would encompass data that is also 'personal information' under the Privacy Act (the following **Diagram** sets out our understanding of the proposed definition).

Diagram



The definition of 'consumer data' also appears to include a wide range of data and information, apparently including any information that is available electronically. Some, or all, of this information may also be personal information for the purposes of the Privacy Act, depending on the way the information is collected and held by an agency or organisation. For example, the question of whether telecommunications metadata is personal information is currently the subject of a matter before the courts.

This means that there is not necessarily ever going to be a clear distinction between 'personal information' and 'consumer data', nor is it necessarily the case that the category called 'consumer data' will always be broader than the category called 'personal information'.

The term 'consumer' may also be unhelpful. Many of the activities and transactions which people undertake online would not be thought of by them as 'consumer' acts, such as interactions with government departments or social media activities.

Finally, we note the OAIC commented in its submission that the proposed restriction of consumer data to 'digitally-held' information may also lead to an anomalous situation where different rights may attach to the same piece of information, on the basis of whether it is stored on a hard drive or on a sheet of paper.

We therefore support the OAIC's view that this new definition would likely introduce significant confusion and result in an increased regulatory burden, for minimal (if any) benefit. Accordingly, we encourage the Commission to reconsider whether it is necessary to create a new definition of 'consumer data'.

We also note that the Draft Report recommends that a definition of 'consumer data' be inserted in the *Acts Interpretation Act 1901* (Cth). This is not a term that is currently used in legislation, but placing the definition in the Acts Interpretation Act is an option should there be a demonstrable need. If it is expected that the term 'consumer data' would be used widely in legislation then specific examples of where it would be used, including how frequently, would be useful to support this proposal. Inserting this definition in the Acts Interpretation Act is not currently under active consideration as it is not an issue that stakeholders have raised with the department.

Comprehensive Right (recommendation 9.2) – Interaction between proposed Data Sharing and Release Act and Privacy Act (recommendation 9.11)

AGD considers that the proposed 'Comprehensive Right' is a positive privacy-protecting measure. The proposed 'Data Sharing and Release Act' considers some privacy issues, but additional consideration on the following matters would assist to clarify the scope and operation of the new right.

In particular, AGD suggests the Commission may wish to consider options to ensure that there is minimal duplication and confusion with multiple pieces of legislation regulating the same issues, and greater clarity around regulatory responsibilities. AGD's preference would be to maintain the Privacy Act as the primary framework relating to personal information. However, page 366 of the Draft Report states the intended approach is for issues around data access to be viewed via an alternative lens (data as an asset) rather than that provided by existing legislation such as the Privacy Act. We encourage the Commission to consider whether elements of the Comprehensive Right may be achieved by amendments to the Privacy Act, to maintain a consistent scheme for handling personal information with minimal regulatory impact on business and individuals

Small business, journalism and other exemptions

AGD considers it would be useful for the Commission to clarify whether the proposed Comprehensive Right requirements would apply to organisations which are in exemption categories under the Privacy Act, such as the small business[11], journalism[12] and employee records[13] exemptions.

If so, the Commission could also consider whether such organisations (exempt from the Privacy Act) should be subject to Privacy Act (or similar) requirements around data quality, security[14] and cross-border[15] disclosure restrictions, particularly regarding the data transfer aspect of the Comprehensive Right. We note that extending the Privacy Act to these currently exempt entities would impose considerable regulatory costs.

State and territory authorities

A similar issue arises in relation to state and territory authorities. AGD notes that the Commission's aim is for the Data Sharing and Release Act to apply as part of a consistent scheme across jurisdictions and separate state and territory legislation may be required to cover state governments and instrumentalities.[16]

AGD considers it would be useful for the Commission to consider whether state and territory authorities, exempt from the Privacy Act but proposed to be subject to the Comprehensive Right under State-based legislation, should be subject to the type of requirements around data quality and security found in the Privacy Act (or similar).

---

[11] The Privacy Act generally exempts small businesses and not-for-profit organisations with an annual turnover of $3 million or more). We note that the OAIC has indicated it may be timely to re-examine the application of the small business exemption in the context of the Privacy Act: OAIC Submission to Issues Paper, pp 12-13.

[12] Media organisations acting in the course of journalism are exempt from the Privacy Act if the organisation is publicly committed to observing published privacy standards.

[13] In some circumstances, the handling of employee records by an organisation may be exempt from the Privacy Act in relation to current and former employee relationships.

[14] The Privacy Act sets out the obligations of APP entities around data quality and data security through Australian Privacy Principles (APPs) 10 and 11 respectively. With regard to data quality, APP entities must take reasonable steps to ensure personal information they collect is 'accurate, up-to-date and complete'. An APP entity has the same qualitative obligations concerning the use or disclosure of personal information, with the additional requirement that the use or disclosure be 'relevant'. Regarding data security, APP entities must take reasonable steps to protect personal information from 'misuse, interference and loss', as well as from 'unauthorised access, modification or disclosure'. Further, APP entities must destroy or de-identify personal information they no longer need (with limited exceptions).

[15] The Privacy Act imposes strict rules on APP entities governing the overseas disclosure of personal information held in Australia. APP 8 generally requires an APP entity, before disclosing personal information to an overseas recipient, to take reasonable steps to ensure that overseas recipient will handle the personal information in accordance with the APPs. Importantly, the APPs include a requirement for businesses to take reasonable steps to protect personal information from unauthorised access or disclosure (APP 11). Section 16C of the Privacy Act makes the APP entity responsible for personal information disclosed to an overseas recipient, unless an exception applies. This means the APP entity will be accountable if the overseas entity mishandles the information.

[16] Page 366.

Access, edits and corrections of data

As currently drafted, the proposed Data Sharing and Release Act would create a second regime for access, edits and corrections to data, operating in parallel to the Privacy Act,[17] with a second set of regulators (**Appendix A**). This situation arises due to overlaps between the proposed new definition of 'consumer data' and the Privacy Act definition of 'personal information' as mentioned above. Also, for data held by government agencies, the *Freedom of Information Act 1982* (Cth) provides another, third, access scheme.

AGD considers it would be useful for the Final Report to clarify how access, edits and corrections to data will operate differently under the proposed Comprehensive Right to existing Privacy Act provisions, including the categories of exceptions that may apply to limit the right.

We also note that as part of the Open Government Partnership National Action Plan,[18] the Government will consider and consult on options to develop a simpler and more coherent framework for managing and accessing government information that better reflects the digital era. This commitment recognises that the core frameworks underpinning Australia's information access law (in particular the FOI Act and the Archives Act) have not been substantially altered since their commencement in the early 1980s, when government operated in a paper-based environment. It is therefore timely to consider opportunities for new technologies to facilitate more efficient and effective management and access of government information. At the same time, the public has an increasing expectation of access to government information in the digital environment. The project will provide an opportunity for a holistic assessment of government information frameworks and provide a strong driver to progress reforms across policy, technology and culture. The National Action Plan follows a number of reviews, notably Dr Allan Hawke's review of the FOI Act in 2013[19] and the *Belcher Red Tape Review* in 2015.[20]

Format of data

The Draft Report refers to comments by the ACCC and the Financial System Inquiry that the Privacy Act does not provide guidance on the format in which personal information is to be provided to consumers.

By way of background, the Privacy Act was designed to be technologically neutral. By using high level principles, the Privacy Act regulates agencies and organisations in a flexible way. They can tailor personal information handling practices to their diverse needs and business models, and to the equally diverse needs of their clients.[21]

---

[17] Individuals can request access to personal information (including digital data) about themselves, in the form they wish, and organisations are required to give individuals access as requested unless exceptions apply (APP 12). Individuals can request edits and corrections to personal information where it is inaccurate, out-of-date, incomplete, irrelevant or misleading. Organisations are required to make edits and corrections unless exceptions apply (APP 13).

[18] Commitment 3.1, <http://ogpau.pmc.gov.au/2016/12/07/australias-first-national-action-plan-submitted>

[19] Dr Allan Hawke AC, Review of the *Freedom of Information Act 1982* and *Australian Information Commissioner Act 2010*, 2013, < https://www.ag.gov.au/consultations/pages/reviewoffoilaws.aspx>

[20] Barbara Belcher, Independent Review of Whole-of-Government Internal Regulation, August 2015, <https://www.finance.gov.au/publications/reducingredtape/>. The Belcher review made a number of recommendations relating to information frameworks, including in areas of ICT, planning and reporting, publishing and tabling, senate continuing orders, FOI and PSPF. Notably, the review found there was duplication, inconsistency and a lack of coherence in the operation between information access schemes under the FOI Act, the Privacy Act and the Archives Act.

[21] Explanatory memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52. This principles-based approach to privacy law is comparable to international regulatory models in jurisdictions such as Canada, New Zealand and the United Kingdom.

Individuals can request access to personal information (including digital data) about themselves in the manner they wish, for example by email, by phone, in person, hard copy or an electronic record. Entities must provide the information in the requested manner where it is reasonable and practicable to do so.[22]

That said, AGD acknowledges there may be benefit in providing guidance on the format in which personal information is to be provided to consumers, such as by allowing for the prescription by legislative instrument of standards or format requirements for specific types of data.

Complaints handling – Proposed role for Industry Ombudsman and external dispute resolution (EDR) schemes (recommendation 9.3)

In addition to issues raised above about regulatory overlaps between the proposed Data Sharing and Release Act and the Privacy Act, the proposed regulatory regime presents other issues. The Draft Report proposes that complaints handling and dispute resolution would be by existing industry ombudsman or external dispute resolution (EDR) schemes in various sectors.

The Draft Report states that at present there is a range of industry-specific regulators that exercise their powers jointly with the OAIC where those industries involve collection, disclosure or use of personal information. These other regulators have various enforcement powers relating to their respective regulatory responsibilities. For example, the Financial Ombudsman Scheme (FOS) and the Credit and Investment Ombudsman (CIO) scheme in the finance sector; ACMA and the Telecommunication Industry Ombudsman (TIO) in the telecommunication sector; ASIC as corporate regulator, APRA as prudential regulator and Commonwealth Ombudsman as Private Health Insurance Ombudsman.

This proposal raises a number of issues that merit further consideration by the Commission:

- *Significant new functions* - Other than the Privacy Act recognised EDR schemes[23], these Industry Ombudsmen do not currently provide dispute resolution, or enforce powers, for individuals' data issues in a way that is comparable to the proposed complaints handling role. Their role over individuals' data is incidental. Instead, their functions are more in the nature of consumer protection in their respective regulatory areas.
  Also, for Privacy Act EDR Schemes, their functions are limited to handling complaints about credit providers and credit reporting bodies and not organisations more broadly. **Appendix A** compares the proposed role with the existing situation under the Privacy Act.

- *Funding* – Existing Industry Ombudsmen and EDR scheme operators would need funding to provide the proposed new functions. Specifically, EDR schemes within the Attorney-General's portfolio would require a significant injection of funding before they could provide a sufficiently solid structure to support the proposed new complaints handling role.

---

[22] If an APP refuses to give access in the manner requested by the individual, the entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual. This should be done within 30 calendar days where practicable: OAIC, APP Guidelines, paras [12.68]-[12.71]. Also, the APP entity is expected to consult the individual to satisfy their request: Explanatory memorandum to Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 52.

[23] Under s21D(2)(a)(i) of the Privacy Act, credit providers are required to be members of an external dispute resolution (EDR) scheme recognised by the Australian Information Commissioner in order to disclose credit information about an individual to a credit reporting body and thereby participate in the credit reporting system.

Options for the Commission to consider include funding from industry member contributions, as with the two banking schemes (Financial Ombudsman Scheme (FOS) and the Credit and Investment Ombudsman (CIO)). The costs of running these schemes are met by members as a result of the licensing obligations to which participants in the finance sector are subject.[24] However, funding options for the existing subset of State-based utility and transport schemes would require a different approach.

Complaints handling – Proposed role for OAIC

The Draft Report proposes that the OAIC would act as a backup where no Industry Ombudsman/EDR scheme already exists. The OAIC would require funding for its backup role, and particularly until the industry ombudsman/EDR schemes are set up for the new role.

Datasets of national interest (Ch 9 Information request)

Family law services data provided by non-government service providers and held by the Department of Social Services is potentially of great value to researchers, especially when aggregated with other datasets held by agencies such as the Australian Institute of Family Studies and the Department of Human Services. AGD would be supportive of designating these data holdings as National Interest Databases, and of a trial of their release to accredited trusted users.

Requirement on government agencies to share and release data (recommendation 9.11)

The Draft Report recommends that the Data sharing and Release Act would include provisions requiring government agencies to share and release data with other government agencies, and requiring sharing between government agencies and other sectors. These provisions would operate regardless of all restrictions on data sharing or release contained in other legislation, policies or guidelines. However, the provisions may be waived in limited exceptional circumstances, to be specified in the Data Sharing and Release Act.

AGD agrees there is scope to promote better sharing and release of data for public purposes and supports the aims of recommendation 9.11 in this regard. However, AGD does not support the proposed requirement on government agencies to share and release data with other government agencies. On its current wording, we consider the requirement is too broad in its scope. It risks the unintended release of government data which could compromise the public interest. Also, the requirement does not appropriately balance the intrusion on individuals' privacy with the stated policy objectives, as the least intrusive option available. Such a balance is required to comply with Australia's international human rights obligations under Article 17 of the ICCPR.

AGD also considers that further consideration is required of the greater security risks associated with an exponential increase in data sharing and release, as proposed. The presence of more data in a wider set of agencies (such as data originally held by one agency now being held in other agencies) involves a greater risk of inappropriate access or release by agencies.

[24] For example, Australian Credit Licensees are obliged to be a member of an ASIC approved EDR scheme (FOS or CIO) under s47(1)(i) of the *National Consumer Credit Protection Act 2009*.

We encourage the Commission to give further consideration to appropriate limitations on the proposed requirement to share and release government data, considered below. Also, governments have a responsibility to the community to ensure that individuals' personal information is shared and release in accordance with accepted standards and subject to appropriate accountability and oversight arrangements.

Social licence and openness

As stated at page 2 of AGD's original submission, we consider that governments should be open about the practices and policies they apply to data. They should clearly articulate why they collect data and for what purposes that data is retained, used and shared. While this is particularly important for personal information covered by the Privacy Act, openness also applies to other types of data. Openness promotes community understanding and acceptance of Government's approach to data and allows for early feedback when community expectations are not being met. Openness also promotes cultural change within government agencies. AGD encourages the Commission to consider ways to reconcile the requirement to share and release government data with other initiatives, including the Draft Report's recommendations 9.2 and 9.11, giving individuals greater control over their data. For example, the My Health Record initiative gives individuals the ability to set access controls to restrict who sees their health information.

Secrecy review

AGD notes that, in addition to recommendation 9.11, draft finding 5.2 states that:

> A wide range of more than 500 secrecy and privacy provisions in Commonwealth legislation plus other policies and guidelines impose considerable limitations on the availability and use of identifiable data. While some may remain valid, they are rarely reviewed or modified. Many will no longer be fit for purpose. Incremental change to data management frameworks is unlikely to be either effective or timely, given the proliferation of these restrictions.

The Productivity Commission's report serves as an important reminder to Government of the need to comprehensively assess secrecy provisions. However, we are concerned that the report may be too narrow a vehicle to comprehensively assess secrecy provisions with the appropriate input from across government. The development and implementation of an Australian Government response on secrecy would be a major law reform project, requiring the revision and re-design of an entire field of law, including the amendment of several hundred provisions of Commonwealth legislation spanning all portfolios. This would require extensive whole-of-government consultation and agreement on legislative and policy reforms. The lack of uniformity in the elements, penalties and policy rationales applying to existing secrecy offences is likely to make consensus within the Commonwealth difficult to attain in the short term.

Further, as reflected in recent experience in making targeted amendments to secrecy offences in the 2014 security legislation amendments, secrecy law reform attracts significant public debate and controversy, particularly from the media, which could impact on the success of any proposed amendments. A careful public consultation and stakeholder management strategy would therefore be vital, and would also be highly resource intensive.

Consequently we agree with the Department of Prime Minister and Cabinet position[25] that legislative reform is required to identify whether secrecy laws can be streamlined and modernised.

[25] Public Sector Data Management, July 2015, p 36, quoted at page 202 of the Draft Report.

We note there is no impediment to individual agencies assessing the secrecy provisions which they administer to determine on a case by case basis whether they remain appropriate, including in the context of data availability and use.

Privacy and secrecy restrictions

AGD's view is that legislation relating to the sharing and release of personal information, particularly sensitive personal information, should be drafted narrowly and clearly defined in legislation to ensure minimal interference with an individual's privacy. However, draft recommendation 9.11 proposes that the Data Sharing and Release Act would positively require sharing and release of personal information and override all restrictions in legislation such as the Privacy Act.

The Draft Report does not provide guidance on the exceptions which may limit the government sharing and release requirement. AGD encourages the Commission to give further consideration to the nature of any exceptions, as these will be significant in determining the scope of the requirement and whether the new Act would contain adequate privacy safeguards to protect personal information. We address suggested exceptions further below.

For example, on the current wording, recommendation 9.11 would positively require a government agency (eg ABS) to share or release:

- personal information, including sensitive information such as religious beliefs or affiliations
- which it collects for one or more purposes (primary purpose or purposes) *specified* in legislation (eg Census)[26]
- with all other government agencies, at both the federal and State level, for *unspecified* purposes (secondary purposes).

By contrast, the Privacy Act prohibits secondary disclosures (unless the individual consents or specified exceptions apply) and contains additional restrictions governing sensitive information.

Also, there is a legitimate public interest in maintaining the confidentiality of certain information. As administrator of Commonwealth secrecy policy, we see secrecy override provisions in practice only in rare circumstances, for example in the *Inspector-General of Intelligence and Security Act 1986* where there is a strong justification such as an independent oversight body requiring access to all information. In this context, the public interest in override has been specifically considered and consequently balanced with the public interest of open government.

Other, less intrusive models

As we noted in our original submission, AGD considers that the complexity of the existing government data regime can lead to a perception that the law is more restrictive than it is in reality. At the same time, we recognise this complexity does also give rise to genuine barriers to sharing of data across government.[27]

A less intrusive approach to promote greater sharing of information is legislation that authorises, rather than requires, the sharing of government data as adopted in New Zealand[28] and, within Australia, in New South Wales and South Australia.[29]

---

[26] Under the agency's governing legislation or under a Privacy Act exception.
[27] Pages 1, 5-6.

As detailed in AGD's original submission, the department suggests a tiered approach to improving data use and availability in the diagram below. The three tiers are intended to operate in a cascading fashion. If information can be shared at the highest level of the framework (broad based data sharing legislation or personal information sharing agreements) then you do not need to proceed to the next level and so on.

[28] NZ's *Privacy Act 1993* contains a mechanism for the approval of information sharing agreements: Part 9A.
[29] *Data Sharing (Government Sector) Act 2015* (NSW), *Public Sector (Data Sharing) Act 2016* (SA), due to commence on a day to be fixed by proclamation.

This permissive model would be similar to that adopted in NSW, SA and NZ, where data sharing legislation:

- specifies the purposes for which data may be shared (eg in NSW and SA: data analytics work, public sector agency policy making, program management and service planning and delivery)[30]
- limits data sharing to the government sector (NSW) or sets out additional requirements where sharing extends to non-government sector bodies (NZ and SA: data sharing agreements)[31]
- sets out exceptions or data sharing safeguards to protect privacy (NSW, NZ)[32] or to protect data that is subject to secrecy provisions (NSW), or is confidential or commercially sensitive data[33] (NSW and SA).
- specifies that government data that is shared is maintained and managed in compliance with any legal requirements and government data security policies concerning its custody and control (NSW and SA),[34] and
- provides a role for an oversight body (NSW Privacy Commissioner, NZ Privacy Commissioner).

Any equivalent legislation at the Commonwealth level would provide an opportunity to consider what protections and oversight mechanisms should apply to data use and sharing activities. This might include allowing for data to be used and shared in cases that might otherwise be prevented by restrictions in other legislation, though noting again that in many cases it would likely be appropriate to maintain secrecy, non-disclosure and confidentiality restrictions.

This model would provide a high-level commitment to data sharing. This could then be supplemented by a legislated scheme for personal information sharing agreements. The Department of the Prime Minister and Cabinet's Public Data Management Report discussed the difficulties agencies can face in establishing agreements to share data.[35] There may be value in considering whether data sharing legislation should include a formalised mechanism to support the sharing of personal information for specific activities deemed to be in the public interest, for example to facilitate service delivery improvements or for identity verification purposes. Such agreements would provide agencies with certainty about sharing data with other agencies, and could include appropriate safeguards reflecting existing privacy or other legislative controls. These safeguards could include appropriate approval and oversight mechanisms, most notably through the OAIC, and possibly also through other regulators or bodies where desirable.

An example of such agreements can be found in New Zealand. Part 9A of the *Privacy Act 1993* (NZ) contains an 'approved information sharing agreement' mechanism which allows New Zealand Government agencies and other entities to share personal information for service delivery purposes. Elements of the New Zealand model that could underpin such agreements here include the focus on considering each data sharing proposal on its own merits, being transparent about data sharing activities and providing a role for the privacy regulator.[36]

---

[30] And such other purposes as may be prescribed by the regulations NSW: s6; SA: s7.
[31] In SA, data sharing agreements are required for data sharing between government agencies and private sector bodies. In NZ, information sharing agreements can operate between both public and private sector bodies.
[32] NZ's data sharing provisions are contained, and subject to safeguards within, the Privacy Act.
[33] For example because of a contractual or equitable obligation. NZ's data sharing provisions are contained, and subject to safeguards within, the Privacy Act.
[34] NSW: s14; SA: s10. At the Commonwealth level, government sector data would be subject to the Protective Security Policy Framework and Privacy Act requirements relating to data storage and security, including proposed mandatory data breach notification and re-identification amendments.
[35] Department of the Prime Minister and Cabinet, 2015, *Public Sector Data Management*, p 18.
[36] *Privacy Act 1993* (NZ), ss 96O, 96S.

Other elements, such as the status of approved information sharing agreements as legislative instruments requiring Cabinet approval, would likely not be appropriate in the Australian context as they would not be flexible enough to facilitate the dating sharing activities that will occur under the Australian Government Public Data Policy Statement.

Exclusion of security data and criminal and financial intelligence

AGD recommends that recommendation 9.11 specifically exempt 'security data' (which encompasses law enforcement data), criminal and financial intelligence for clarity.

We note that the scope of the inquiry excludes 'security data', defined broadly to mean 'data where national security or other compelling public interest considerations tell against its release' (section 1.1, p43). Further, the report notes: 'as such, security data is only referenced for clarity — that is, where we believe it may appear to be captured by our draft recommendations, we clarify that it is not'. On this broad definition of 'security data' we consider that information held by law enforcement agencies would fall outside the scope of the Productivity Commission's draft recommendations. However we consider that Recommendation 9.11 (proposing the introduction of a new Commonwealth Data Sharing and Release Act) is not clear on this point. It could be misinterpreted to capture all public sector data including security data. Also, it is not clear whether the term 'security data' includes criminal and financial intelligence.

Definition of security data

The Draft Report recommends that the requirement to share and release government data would operate regardless of all restrictions on data sharing or release contained in other legislation, policies or guidelines. It also proposes that the provisions may be waived in limited exceptional circumstances, and the Act should specify what these circumstances are.

AGD has concerns regarding potential impact of these requirements on the sharing and release of classified information under the Australian Government's Protective Security Policy Framework (PSPF).

We recommend that the existing definition of security data in Part 1.1 (page 43) be amended as follows (suggested text in bold):

- *security data — data where* **its release could have an impact on Australia's national security as defined in the *National Security Information (Criminal and Civil Proceedings) Act 2004,****or where other compelling public interest considerations tell against its release.*

The *National Security Information (Criminal and Civil Proceedings) Act 2004* definition of national security captures Australia's defence, security, international relations or law enforcement interests.[37]

[37] Section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (NSI Act). 'Security' is defined in section 9 of the NSI Act to have the same meaning as in the *Australian Security Intelligence Organisation Act 1979* (Cth):

- the protection of, and of the people of, the Commonwealth and the several States and Territories from:
    - espionage;
    - sabotage;
    - politically motivated violence;

References to 'confidential/protected' information

The proposed framework for accessibility on pages 14 and 344 proposed allowing 'confidential/protected' data to be released if decided by the data custodian. It is not clear what the term 'confidential/protected' data is intended to cover. It appears that the Draft Report intends for the terms 'confidential' and 'protected' to be given their ordinary meaning. We note page 13 refers to 'near real time data that identifies individual persons or businesses carries the highest risks to privacy and security.' However, AGD notes that the term 'confidential information' has a specific meaning under law. We also note the terms 'Confidential' and 'Protected' carry specific meanings, relating to security classifications, under the Australian Government's Protective Security Policy Framework. AGD suggests providing clarification on the definition of 'confidential/protected' data and providing more information on how such data would be released and in what circumstances. AGD understands that the report is not proposing to release classified information under the proposed new framework. However, this needs to be more clearly articulated in the report.

Proposed role for the AAT (p 16 and pp 366-367, recommendation 9.11)

The Draft Report[38] proposes a new role for the AAT in the reformed data management system to assess disputes and appeals regarding data sharing and release. While as a general principle we consider that merits review should be available for administrative decisions that will, or are likely to, affect the interests of a person, it is not clear what the Productivity Commission is proposing in this instance.

The proposed function is significantly different to the existing functions of the AAT and would fundamentally change the nature of the AAT's role, which is to reconsider administrative decisions. The AAT may affirm, vary or set aside the initial decision or remit the decision to the original decision maker for reconsideration.

  - promotion of communal violence (activities that are directed to promoting violence between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth).
  - attacks on Australia's defence system; or
  - acts of foreign interference;
  - whether directed from, or committed within, Australia or not; and
- the protection of Australia's territorial and border integrity from serious threats; and
- the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

'International relations' means political, military and economic relations with foreign governments and international organisations: section 10 of the NSI Act.

'Law enforcement interests' includes interests in the following:

- avoiding disruption to national and international efforts relating to law enforcement, criminal intelligence, criminal investigation, foreign intelligence and security intelligence;
- protecting the technologies and methods used to collect, analyse, secure or otherwise deal with, criminal intelligence, foreign intelligence or security intelligence;
- the protection and safety of informants and of persons associated with informants;
- ensuring that intelligence and law enforcement agencies are not discouraged from giving information to a nation's government and government agencies.

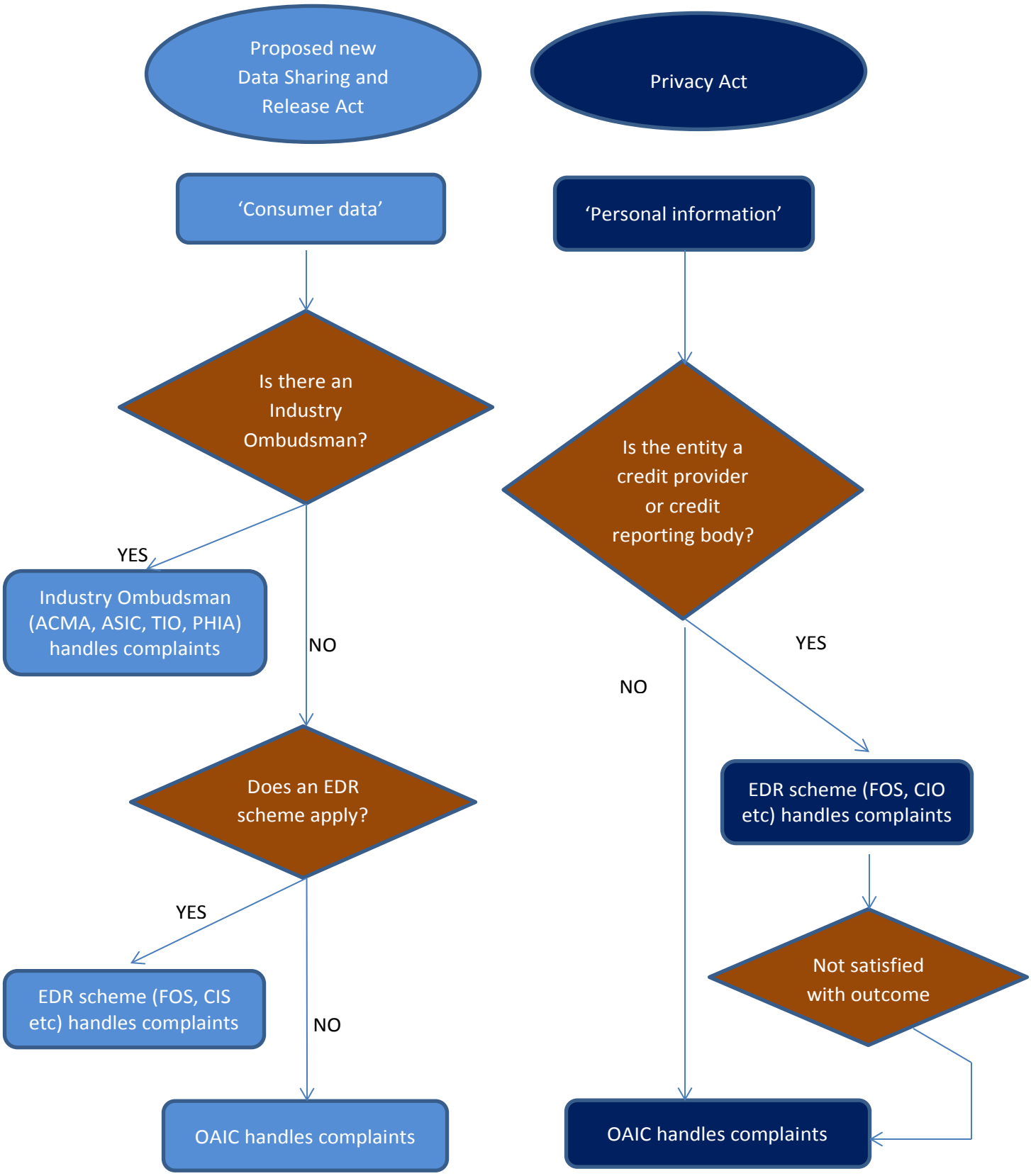
[38] Overview, Box 2, p16; Chapter 9, box 9.6, at page 366 and Table 9.1, page 367.

The AAT currently does not assess or resolve disputes, as recommended by the Report. An expansion of the function of the AAT to include assessing disputes and appeals would require significant resourcing and legislative change.

The Draft Report also recommends establishing Accredited Release Authorities (ARAs), who would decide whether a dataset is available for public release or limited sharing with trusted users. The Report suggests that ARAs may be state/territory (state) entities, and would not be limited to public entities. The AAT only reviews decisions of state and non-government entities in limited circumstances. If the AAT were to review these decisions, there would need to be agreement with states, and the Department would need to seek constitutional advice could be necessary.

The department would prefer a recommendation which confers on the AAT jurisdiction to undertake administrative review of decisions by Commonwealth entitles related to data sharing and release, as this would not change the function of the AAT. However, further resourcing for the AAT to undertake this new caseload and to implement legislative changes would still be required.

APPENDIX A


Proposed new Data Sharing and Release Act
Privacy Act
'Consumer data'
'Personal information'
Is there an Industry Ombudsman?
Is the entity a credit provider or credit reporting body?
YES
Industry Ombudsman (ACMA, ASIC, TIO, PHIA) handles complaints
NO
NO
YES
Does an EDR scheme apply?
EDR scheme (FOS, CIO etc) handles complaints
YES
Not satisfied with outcome
EDR scheme (FOS, CIS etc) handles complaints
NO
OAIC handles complaints
OAIC handles complaints