Australian Government

Office of the Australian Information Commissioner

December 2016

Data Availability and Use – OAIC submission to Productivity Commission Draft Report

www.oaic.gov.au

Contents

Overview **3**
Establishing trust and a social licence **5**
New 'Comprehensive Right' to access digitally-held data **7**
The *Data Sharing and Release Act* and existing secrecy and privacy provisions **12**
The role of the National Data Custodian **13**
The 'trusted user' model **15**
Accredited Release Authorities (ARAs) **17**
Other specific recommendations **18**

Overview

As the Australian Information Commissioner and Australian Privacy Commissioner (Commissioner), I welcome the opportunity to comment on the Productivity Commission's *Draft Report on Data Availability and Use* (draft report).

As I outlined in my earlier submission on the Commission's *Issues Paper*,[1] I am supportive of initiatives which seek to maximise and enhance the use of data. I appreciate that the Commission is seeking to foster a cultural shift, and to '*take Australia beyond the stage of viewing data availability solely through a privacy lens, in recognition that there is much more than privacy at stake when it comes to data availability and use*'.[2] Since the establishment of the OAIC in 2010, my Office has encouraged Australian Government agencies to view government-held data as a national resource which should be managed strategically, and in a way that benefits the public. In my role as the Information Commissioner, I strongly endorse such an approach to data use and management

At the same time, as the Privacy Commissioner I am also mindful that privacy is a fundamental human right as recognised in the *United Nations Declaration of Human Rights*, and in many other international and regional treaties. Therefore, when considering how data use can be enhanced, it is crucial that a balance is struck between the right to privacy and the interests of entities in carrying out their functions and activities.[3] This is no longer straightforward or two-dimensional. It is a balance that must be struck at the intersection of law, policy, and technology. My agency has helped numerous agencies and organisations, across all sectors within the Australian economy, navigate the line between open data and privacy protection over the past six years.

To ensure the success and sustainability of the Commission's proposed reforms, public support will be essential. Building the social licence for new data-related activities will require well-thought out data governance measures. Such measures will give individuals confidence about how their information will be managed, and give clear guidance to data custodians about how they should handle personal information. Privacy law, underpinned as it is by principles of transparency and accountability, will continue to be an essential component of any successful data governance framework.

The Commission's draft report recommends the development of a centralised model for data governance in Australia. I understand that the proposed new *Data Sharing and Release Act* (new Data Act), the centrepiece of the proposed reforms, is intended to apply to all digitally-held data. The draft report also suggests that the new Data Act is intended to apply as broadly as possible, including to State and Territory government bodies (to some extent), as well as to all private sector entities. To successfully promote maximum participation across all governments and sectors, I encourage the Commission to consult with all affected stakeholders to further refine the details of how the model will apply across the various Australian jurisdictions.

I am broadly supportive of the general direction of the proposed model. I support the proposal to establish a central body (the National Data Custodian, or NDC) with responsibility for implementation of any new data management framework, including the identification and designation of high-value datasets of strategic national importance. I also support the development of a 'trusted user' model, to ensure that appropriate access controls are in place for those who handle certain National Interest Datasets (NIDs).

---

[1] OAIC submission to Commission's Issues Paper 'Data use and Availability', August 2016, available at www.oaic.gov.au.

[2] Draft report, p 12.

[3] See the objects set out in s 2A of the *Privacy Act 1988* (Cth).

As currently drafted the recommendations are very high-level and a significant range of issues will need to be addressed in greater detail to ensure appropriate implementation. I have highlighted some of those issues in this submission, and also make a number of other comments and suggestions in relation to various aspects of the draft report.

In particular, I believe the following recommendations need further refinement:

- **Social licence and uses of data held in NIDs (draft recommendations 9.4, 9.7 and 9.8).** I do not believe that the current draft recommendations adequately address the need to ensure community support for the proposed reforms. At present, the draft report has suggested significant modification of the existing settings contained in the *Privacy Act 1988* (Cth) (Privacy Act), without proposing a principled framework to apply in its place. Most crucially, the draft report does not address what new uses of data should be permissible under the model.

- **New definition of 'consumer data' (draft recommendation 9.1).** I do not support this definition as currently drafted, as I believe it essentially duplicates the definition of personal information already set out in the Privacy Act.

- **New Comprehensive Right to access digitally held data (draft recommendation 9.2).** I do not support the current drafting of this recommendation as I believe that dividing regulatory responsibility between the ACCC, my Office and other bodies will lead to unnecessary complexity, creating fragmentation. This would not produce a viable model for governing access to consumer data. However, I am broadly supportive of proposals which strengthen individual rights to access information. In my view, the Commission's proposed expansions to existing access rights can be achieved most efficiently through enhancing the existing framework in the Privacy Act.

- **Open publication of NIDs containing personal information (draft recommendation 9.4)**. In my view, it is unlikely that any high-value datasets containing personal information will be able to be sufficiently de-identified to enable general, open publication (in a manner that also preserves the integrity of that data). These types of datasets require additional controls to be in place to prevent re-identification. The 'trusted user' model proposed in the draft report could instead be used to increase the value and availability of these datasets, while maintaining appropriate access controls.

I explain these comments below, and raise some further issues for the Commission's consideration.

Establishing trust and a social licence

Draft Finding 8.1; Draft Recommendations 9.4, 9.7 and 9.8

8.1 - Governments must maintain a social licence for their collection and use of data

9.4 – The Australian Government should develop a process for designating 'National Interest Datasets' (NIDs) and categorising NIDs for release

9.7– The NDC should develop pre-approved uses of NIDs and grant trusted users access to data for specific projects, subject to conditions

9.8 – The NDC, in consultation with data custodians, should develop a list of pre-approved uses for datasets

Draft recommendation 9.4 recommends establishment of a parliamentary committee to ensure community consultation on the identification and designation of high-value datasets. Draft Findings 8.1-8.3 also discuss these matters, and suggest that the new consumer right will assist in building a social licence for the broader reform proposals.

However, while draft recommendation 9.8 states that the NDC will be given responsibility for developing a '*list of pre-approved uses for a dataset*',[4] there are no proposed limits set on the uses of data in the draft report. I believe this is a significant gap which should be addressed in the final report. Public support for the reforms will depend on a number of factors, including the community having a clear understanding of what is proposed, as well as the overall proportionality of those proposals. For example, I expect many Australians would be concerned if they learned that their personal health, Medicare or social security data - collected compulsorily by government in exchange for access to payments or services - was to be made available to private sector organisations, to conduct research in their own commercial interest in circumstances where they have not consented to that disclosure (or even been notified that this will occur). More broadly, many individuals may not support their data being used for purposes which they see as having no clear personal (or public) benefit, particularly where a risk of harm or discrimination is introduced to them by way of that disclosure. As draft finding 5.3 notes, '*individuals expect to remain in control of who data on them is shared with*'.[5]

Data reforms of the scale envisaged by the Commission will therefore require strong community support to be successful. The draft report states that the introduction of the new consumer right will help to build this support. I do not believe that there is necessarily any correlation between public support for the new consumer right, and the public's attitude to broadening access to datasets. While the new consumer right may provide a benefit to individuals, it will not necessarily build support for the government to use and share individuals' data for secondary, unspecified purposes. Most importantly, to build support and trust the Commission must address the intended uses that data will be put to.

[4] Draft report, p 38.

[5] Draft report, p 28.

A social licence for data use will be built on a number of elements. First, governments must be transparent about their intentions, so that individuals actually understand what the data reforms may mean for their personal information. Second, there must be meaningful consultation with individuals, to find out what uses of data the broader community believes are valuable, and reasonable. Third, governments must respond and take public opinion into account when making decisions. This may mean, ultimately, that there is community support for only some proposed uses of data - rather than all those that government and business may desire. However, in a democracy, having broad community support for reforms of this nature is essential.

A number of salient international examples illustrate this point. For example, as the Commission outlined in its draft report, in January 2014 in the United Kingdom, the National Health Service (NHS) launched care.data—an initiative to extract data from NHS primary care medical records, for research and other purposes, unless a patient was to opt out. There was a lack of patient awareness of the program, and a lack of clarity around how to opt out, which resulted in intense public concern. This public concern caused the program to be suspended, and ultimately it was wound up in July 2016, following two negative reviews. One such review found that "*there needs to be a much more extensive dialogue with the public about how their information will be used, and the benefits of data sharing for their own care, for the health and social care system and for research*".[6] The failed program also incurred significant costs for the UK government.[7]

In summary, I recommend that the Commission:

- Consider how meaningful community consultation can be undertaken on what uses of data should be permissible, with the government or NDC ensuring that this feedback is taken into account when developing the list of 'pre-approved' uses (see Draft Recommendation 9.8). In my view, the establishment of a parliamentary committee alone will not be enough to ensure adequate consultation for reforms of this scale.

- Consider how the proposed model can otherwise address the 'use' question, in a way that is commensurate with community expectations. For example, the NSW Data Analytics Centre's enabling legislation[8] provides that it can only collect information where this is in accordance with the relevant agency's legislative obligations, or where information has been de-identified. I am broadly supportive the NSW model, and recommend that the Commission consider whether aspects of this model could be implemented in the federal context.

[6] Care Quality Commission, 'Review of Data Security, Consent and Opt-Outs' (July 2016). A further example can be found in a New Zealand case. When the NZ government first announced its intentions to engage in wider use and sharing of government-held data, there was an intense public backlash, particularly in relation to a proposed observational study of 60,000 children, to try to identify those at risk of abuse. Momentum for the reforms stalled in the wake of a loss of public confidence (see, eg, Jones, N (30 July 2015) 'Anne Tolley scraps 'lab rat' study on children' *nzHerald*. Retrieved from www.nzherald.co.nz). The NZ government has learned from this experience, with a much more sophisticated campaign now having been established by the Data Futures Partnership. The Data Futures Partnership is a cross-sector group of influential people, working together to drive high-trust and high-value data use for all New Zealanders. More information about the Data Futures Partnership is set out at www.datafutures.co.nz. In summary, it has taken the New Zealand government many years to engage with and convince the public that its data reforms are worth pursuing.

[7] See, eg, Shah, S (27 September 2016), 'Scrapped NHS care.data ballsup cost taxpayer almost 8 million pounds', *The Register*, retrieved from www.theregister.co.uk.

[8] *Data Sharing (Government Sector) Act 2015* (NSW).

New 'Comprehensive Right' to access digitally-held data

Draft Recommendations 9.1, 9.2 and 9.3

9.1 - The Australian Government should introduce a new definition of consumer data to apply across all Commonwealth legislation

The new definition of consumer data purports to encompass the current definition of personal information contained in the Privacy Act, while expanding and defining the scope of that definition to ensure that there is a clear benefit for consumers. I understand that the new definition of consumer data is intended to apply to all digitally-held data, whether held by a private sector organisation (regardless of annual turnover) or an Australian Government entity, and that the intention is for this definition to apply, at least to some extent, to data held by State and Territory bodies.

However, I note that as currently drafted, the definition essentially duplicates the existing definition of personal information set out in the Privacy Act. I consider that this new definition would likely introduce significant confusion and result in an increased regulatory burden, for minimal (if any) benefit. I therefore do not support the new definition of consumer data as currently drafted.

Personal information is currently defined in the Privacy Act as information or an opinion about an identified or 'reasonably identifiable' individual.[9] It extends to *any* information or opinion about a person from which they can be identified or reasonably identifiable, including information deduced about an individual from their activities. I note that '*All files posted online by the consumer*' is undoubtedly personal information for the purposes of the Privacy Act. '*All data derived from consumers' online transactions or internet-connected activity*', and '*Other data associated with transactions or activities that is relevant to the transfer of data to a nominated third party*' are also likely to be personal information, though it is not clear exactly what type of information these aspects of the draft definition refer to. Draft recommendation 9.1 attempts to define the boundaries of the proposed consumer data definition, by stating that '*data that is transformed to a significant extent, such that it is demonstrably not able to be re-identified as being related to an individual, should not, for the purposes of defining and implementing any Comprehensive Right, be defined as consumer data*'.[10] In my view, this statement merely reformulates the test for personal information, in slightly different language.

I appreciate that the definition of personal information does not provide a bright line test, and that what is personal information may not always be entirely clear. However, the current definition was specifically drafted this way so that it would be flexible, technologically-neutral, and able to evolve over time. Further, while there is no centralised definition of personal information internationally, the current Australian definition is also consistent with the definitions used around the world, including in the APEC and OECD fora, as well as the European Union, Canada, and New Zealand.[11] The proposed definition of consumer data would not only be unclear and duplicative, but would lock in a prescriptive,

[9] See s 6(1) of the Privacy Act.

[10] Draft report, p 34.

[11] See the definitions of 'personal information' or 'personal data' in international instruments relating to the protection of privacy, such as the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of* Personal Data, the *Asia-Pacific Economic Cooperation Privacy Framework*, and the data protection laws of many other countries including the *Canadian Personal Information Protection and Electronic Documents Act 2000*, the *New Zealand Privacy Act 1993*, and the EU's *General Data Protection Regulation*.

point-in-time approach that would be inconsistent with international practice. In an increasingly globalised marketplace, there is also a particular benefit for Australian businesses in having a definition of personal information that is consistent with the data protection laws of other comparable jurisdictions, and particularly the EU definition.[12]

The justification for introducing a new definition of consumer data appears to be that an updated definition will help to strengthen consumer rights to data, by ensuring that Australian Government agencies and businesses can shift away from seeing data through a more limited, compliance-based 'privacy lens'.[13] It is important to note that good privacy practice is not merely a 'compliance' or regulatory issue. Privacy is a fundamental human right, with the Privacy Act giving individuals control over their personal information, and requiring entities which handle personal information to do so in a transparent and accountable manner. Nevertheless, if the data reforms are aimed at encouraging entities to take a different, more 'positive' approach to their management of data, in my view a legislative amendment is not necessary to effect such a change. Rather, entrenched cultural practices and mindsets can be overcome more effectively through a clear communications strategy. Such a strategy could seek to educate individuals about the rights that they have over their personal information under the Privacy Act, and help data custodians to see personal information as a valuable commodity which can be cultivated through good data governance, rather than a liability or a risk to be managed.

Lastly, I understand that the proposed restriction of consumer data to 'digitally-held' information has arisen due to certain constitutional limitations.[14] However, I note that the proposed restriction may also lead to the somewhat 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. The practical implications of this may be limited, given that in the current age, most information is digitally held. However, the Commission may wish to consider whether this issue can be addressed in implementation, to ensure that the coverage of the new Data Act is as consistent as possible.

I therefore recommend that:

- The Commission reconsider whether it is necessary to create a new definition of 'consumer data'. My Office would be pleased to work with the Commission in developing a clear communications strategy, and to provide further guidance to entities (particularly businesses) on what types of data constitute personal information.

9.2 - Individuals to have a Comprehensive Right to access digitally-held data about themselves (and to opt-out of certain collections)

I am broadly supportive of initiatives which enhance the ability of individuals to access their personal information. I note that this draft recommendation largely emulates the current system for accessing personal information as set out in APPs 12 and 13,[15] with certain expansions. For example, the draft recommendation would give individuals:

[12] The GDPR will apply to certain businesses that provide goods and services to EU customers. See articles 22 and 24 of the GDPR.

[13] Draft report, p 12.

[14] Draft report, p 20.

[15] I note that the draft recommendations will also affect the regime which allows individuals to access their personal information (from Australian Government agencies) under the FOI Act, which I also administer.

- an express right to direct data holders to copy data in a machine-readable form, and provide this either directly to the individual or to a nominated third party
- the right to appeal against any automated decision-making, and
- the right to be informed about a data custodian's intention to disclose or sell data about them to third parties.[16]

In principle, I would support these expansions to the access and correction rights currently available through APPs 12 and 13.[17] I note that these share some similarities with article 22 of the European Union's new data protection law, though I understand the new Comprehensive Right is intended to be broader than the EU provision.[18] However, the draft report does not currently provide sufficient detail about how aspects of the new Comprehensive Right will operate in practice, or the problem that the new measures are intended to solve. I suggest that the Final Report do this - for example, by explaining how the new Comprehensive Right will address the problem of consumers being unaware of '*who is holding what information on them and for what purposes*'.[19]

However, I strongly recommend that the arrangements for accessing personal information remain within the existing Privacy Act framework. In my view, there is no compelling reason why the Privacy Act could not simply be amended to incorporate any of the new aspects proposed in draft recommendation 9.2. The scheme proposed for the new Comprehensive Right would run parallel to the Privacy Act access scheme and, for information held by government agencies, the scheme provided by the *Freedom of Information Act 1982* (Cth) (FOI Act). I question whether having two or three parallel access schemes providing substantially similar rights is efficient.

I also note that the scope of the new Comprehensive Right will differ significantly to that of the Privacy Act, as the Privacy Act generally applies only to private sector organisations with an annual turnover of $3 million or more. [20] The practical result of this would be that small businesses would have to comply with the full range of Comprehensive Right obligations in relation to consumer data, while not having any other obligations at all under the Privacy Act in relation to the remainder of their information-handling practices in relation to one 'subset' of consumer data – personal information. The Commission should therefore be aware that creating tiered levels of obligations for businesses in this way may result in some confusion.[21] I therefore recommend that the Commission consider how this issue could be addressed in implementation, to ensure that the framework is as efficient as possible.

Finally, in my view the inclusion of the right to opt-out of data collection processes may be in need of further refinement. While I generally support initiatives which give individuals greater control over which collections of their personal information they consent to (and which they do not), in my view the breadth of the proposed exceptions to this new Right may render the opt-out provisions of limited utility to many consumers. For example, generally speaking Australian Privacy Principle (APP) 3 permits entities to collect personal information only where it is 'reasonably necessary' for their business purposes. Entities must also generally collect personal information about an individual directly from that

[16] Draft report, p 36. I note that this element of the proposed right may also relate to the substance of other APPs, for example APP 5, which relates to the *Notification of the collection of personal information*.

[17] There is also a right of access to personal information contained in the FOI Act, which I also administer.

[18] See article 22 of the *General Data Protection Regulation*, Regulation (EU) 2016/679.

[19] See p 347 of the draft report.

[20] The Privacy Act provisions currently apply to private sector organisations only where they have an annual turnover of $3 million or more. See s 6D of the Privacy Act.

[21] The draft report recommends that all private sector organisations, including small businesses, should be subject to the new Comprehensive Right provisions. At present small businesses are generally excluded from the operation of the Privacy Act.

individual, unless it is unreasonable or impracticable to do so.[22] Therefore, in the majority of situations where an entity collects information directly from an individual because this is necessary for the provision of a product or service, the opt-out right will be of limited practical utility. Further, I would be concerned to ensure that the new opt-out right does not undermine APP 3, by encouraging entities to collect more information than they need for their business purposes, with the intention of relying on the opt-out provision if individuals object.

On the other hand, I consider that the proposed opt-out right may be beneficial for consumers in some situations, for example where their information is collected by third parties, and there is no direct relationship (i.e. no service delivery) between the data custodian and the individual. In these situations, the opt-out right may provide individuals with greater choice and control over how their personal information is to be used. The Commission should therefore consider how best to design the new opt-out right, to ensure that the best outcome for individuals is achieved.

I therefore recommend that the Commission:

- include any expanded access framework within the Privacy Act, rather than locating it in the new Data Act (or elsewhere)
- consider how the new Comprehensive Right can be implemented efficiently and in a way that ensures minimal confusion for business (having regard to whether the entities which are to be covered by the new Right already have obligations under the Privacy Act), and
- further refine the new opt-out right provisions, to ensure that individuals receive the maximum benefit from any new Comprehensive Right.

I will comment further on the regulatory model proposed for the new Comprehensive Right in the following section.

9.3 – Oversight and complaints functions for the new Comprehensive Right to be shared by the ACCC, OAIC and others

As outlined above, I do not support the new definition of consumer data, and believe that certain aspects of the new Comprehensive Right need further refinement. Further, I do not support draft recommendation 9.3 as currently formulated, which would divide regulatory responsibility for the new Comprehensive Right between a range of bodies, including the Australian Competition and Consumer Commission (ACCC), my Office, and existing industry ombudsmen.

I understand that the intention is for the OAIC to regulate access to 'ordinary' personal information (in the first dot point of draft recommendation 9.1), and either industry ombudsmen or the ACCC will regulate access to the other types of information included in the proposed definition of consumer data.[23] However, the draft recommendation is very high-level, and it is not clear how the framework is intended to operate. Certain unspecified regulatory aspects will be performed by the ACCC (such as determining a framework for access charges). The remainder of the regulatory responsibilities, including 'general' APP 12 access to personal information issues and complaints, would continue to be dealt with by the OAIC. I believe that this model would be confusing and duplicative. Further, the definitional issues I raised in relation to the definition of consumer data would, at this stage, preclude any clear delineation of regulatory responsibilities.

[22] See APP 3, Schedule 1 of the Privacy Act.

[23] Draft report, p 34.

Instead, I strongly recommend that the OAIC remain the regulator for all types of personal information, including consumer data. The Privacy Act provides a comprehensive, overarching framework for the oversight of personal information-handling practices. This includes my powers to conciliate complaints from individual members of the public, and where conciliation is not achievable, to formally determine matters and impose a range of remedies. I also have comprehensive assessment and investigation powers which I can exercise on my own initiative, where alleged breaches of the APPs have occurred. These powers are reinforced by my powers to issue binding determinations, seek court-enforceable injunctions, and seek civil penalties of up to $1.8 million. When taking into account the experience of the OAIC's predecessor (the Office of the Privacy Commissioner), my Office has had a total of over 28 years' experience in resolving privacy complaints which relate to access to personal information, across all areas of government policy, as well as the private sector. Additionally, my Office has had significant experience in dealing with requests to access personal information under the concurrent regime set out in the FOI Act, which I also administer.

In addition to the OAIC's long-standing expertise in this field, there would be many additional advantages to retaining the single regulator framework. Principally, having multiple regulators could lead to increased and unnecessary complexity, resulting in fragmentation and inconsistency of decision-making. Further, the existing framework is one that both business and government are familiar with. My Office has also had significant experience determining appropriate access charges - there is no reason why this function would need to be determined by another body, such as the ACCC, under an expanded access regime. A single regulator model would therefore reduce duplication, increase efficiency and ensure the smooth implementation of any new aspects of an expanded right of access to personal information.

I believe the model currently proposed would also be confusing for individuals, who will have to determine which regulator they should go to when making a complaint about access to consumer data. Further, as the OAIC will remain the only regulatory body with a broad jurisdiction to deal with other APP issues, individuals may lodge a complaint with another body only to find that the issues raised by their complaint extend beyond access issues, raising other issues in relation to the entity's personal information-handling practices. In my experience, access and correction requests are often complex, and require a wholistic assessment of other aspects of an entity's personal information handling-practices, which only the OAIC will be well-placed to provide.

I therefore recommend:

- that the framework for accessing personal information, including the framework underpinning any new 'Comprehensive Right' to access digitally held data, continue to be administered under the Privacy Act and by my Office. I would be very happy to work further with the Commission to refine this recommendation, to ensure an effective framework for oversight of any new expanded access right.

The *Data Sharing and Release Act* and existing secrecy and privacy provisions

Draft Finding 5.2 and Draft Recommendation 9.11

5.2 – There are over 500 secrecy and privacy provisions in Commonwealth legislation. These place considerable limitations on the use of data and many may no longer be fit for purpose

9.11 – A new Data Sharing and Release Act (new Data Act) should be introduced, which will override all current restrictions on data sharing or release, with only limited exceptions

The draft report states that there are too many restrictions currently in place on the use of identifiable data, and that many of these, including privacy protections, may no longer be 'fit for purpose'.[24] However, the draft report does not clearly specify which elements of privacy law may need to be 'streamlined or modernised'.[25]

I am supportive of the overall aims of the draft report, and broadly supportive of draft recommendation 9.11 to introduce a new Data Act. This will become the central legislative framework for the use and sharing of data. I also understand that the new Data Act is intended to modify the application of some provisions of the Privacy Act. However, the draft report does not yet explain how. This will need to be subject to greater consideration and consultation with affected stakeholders, including my Office.

The Commission will need to consider what overall legislative model should be adopted for the National Data Custodian in the new Data Act. A number of jurisdictions have implemented legislative frameworks which allow for a centralised data governance body. For example, the enabling legislation for the NSW Data Analytics Centre (DAC) is intended to '*remove barriers that impede the sharing of government sector data with the DAC or between other government sector agencies*'.[26] This legislation also clarifies the relationship between existing NSW privacy law (and its underlying principles), and the use of data by the DAC.[27] I support many aspects of the NSW DAC model, and would be happy to work with the Commission to further refine Recommendation 9.11 and consider how this could be emulated at the federal level.

The Commission will also need to consider how the proposed new Data Act will interact with the Privacy Act (and other relevant laws, such as secrecy provisions). In particular, the Commission should consider what alternative privacy settings will apply under the new Data Act, if the Privacy Act is to be overridden to any extent. I recommend that the settings in the Privacy Act be referenced wherever possible. Where existing privacy protections are to be modified, however, I recommend that alternative accountability, transparency and use restrictions be developed to ensure the appropriate handling of data. In this regard, I support draft recommendation 9.8, which recommends the development of a list of 'pre-approved uses' for NIDs. I have commented on this further below.

[24] Draft report, p 28.

[25] Ibid.

[26] See s 3(b) of the *Data Sharing (Government Sector) Act 2015* (NSW).

[27] See s 5 of the *Data Sharing (Government Sector) Act 2015* (NSW).

I therefore recommend that:

- the Commission consider what aspects of the NSW DAC model could be emulated in relation to the implementation of draft recommendation 9.11, and
- the Commission consult carefully with affected stakeholders, including my Office, when considering the relationship between the new Data Act and existing legislation such as the Privacy Act.

The role of the National Data Custodian

Draft Recommendations 2.1, 9.4 and 9.5

2.1 – A central government agency with policy responsibility for data should maintain a system for nominating high-value datasets

9.4 – Australian Government should develop a process for designating 'National Interest Datasets' (NIDs) and categorising NIDs for public or limited release

9.5 – The Australian Government should establish the NDC which will have responsibility for the designation of NIDs, ARAs and trusted users

I think there is merit in having a centralised body with overall responsibility for implementation of the proposed data governance reforms. I am also broadly supportive of the proposed model for designating high-value datasets as NIDs, provided this is in the public interest. I understand that, at present, the intention is to create a framework which would incentivise participation in the new model, rather than make participation mandatory. I also recognise the potential benefits that may accrue from empowering the NDC to designate entities as 'trusted users' for accessing data, and being responsible for the governance of these users more generally.

However, I also consider that certain aspects of the NDC's role need to be clarified. For example, I believe that internal governance and capability, and which agency will ultimately have responsibility for oversight and enforcement, is an issue which must be addressed in greater detail in the final report. This is particularly pertinent because, as I have recently stated in other fora, I believe that the existing privacy capability of Australian Public Service (APS) agencies, among other types of entities, may need to be strengthened.[28]

One way to strengthen privacy capability could be through the development of a Privacy Code. As the Commissioner, I have the power under Part IIIB of the Privacy Act to approve or develop (in certain circumstances) a Privacy Code. A Privacy Code sets out how one or more of the APPs are to be applied, and/or can impose requirements additional to those contained in the APPs, in relation to specific activities, industries or professions. Once registered, a breach of a registered code will be an interference with the privacy of an individual under s 13 of the Privacy Act. A Code could be used to set

[28] See the OAIC's submission to the Senate Legal and Constitutional Affairs Committee Inquiry into Census 2016, page 4, and the OAIC submission on the Commission's *Draft Report on a National Education Evidence Base*, p 10. Available at www.oaic.gov.au.

out the requirements for trusted users and other relevant bodies when handling NIDs. For more information about APP codes, see the OAIC's *Guidelines for developing codes*.[29]

I note that a Code can generally only apply to entities that are subject to the Privacy Act. Therefore, whether or not the development of a Code is a viable option would depend on the extent to which the new Data Act modifies entities' existing obligations under the Privacy Act.

When further refining draft recommendations 2.1, 9.4 and 9.5, I would encourage the Commission to consider the following questions:

- **How will accountability for data governance be shared?** My Office is responsible for oversight of the internal privacy governance of APP entities at present.[30] The new data governance model would involve a number of key bodies, all of whom may handle large quantities of sensitive data (including the original data custodians, the NDC, trusted users, other receiving entities, and ARAs). The Commission should determine where the ultimate responsibility for any mishandling of data should lie. In addition, the final report should address who will ultimately have responsibility for oversight of compliance with the new Data Sharing and Release Act and other relevant legislation or standards.
- **How will the NDC (or other regulatory body) ensure appropriate internal governance mechanisms are in place?** There are a range of internal governance mechanisms that could be used to ensure data is handled appropriately by relevant bodies in implementation of the reforms. One potentially effective mechanism could be the development of a Privacy Code. I have commented further on accreditation requirements below.

[29] These are available on the OAIC website at www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.

[30] For example, I oversee entities' compliance with APP 1, which says an APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.

The 'trusted user' model

Draft Recommendations 9.4, 9.7, 9.8 and 9.10

9.4 – Australian Government should develop a process for designating 'National Interest Datasets' (NIDs) and categorising NIDs for public or limited release

9.7 - The NDC should accredit 'trusted users' for access to NIDs that are not to be publicly released

9.8 – The NDC should develop pre-approved uses of NIDs and grant trusted users access to data for specific projects subject to conditions

9.10 – All non-sensitive public sector data should be released, including some identifiable data which is already publicly available in a less accessible form

I support the establishment of a tiered-access model, which will enable the NDC to designate entities as 'trusted users' if they wish to access identifiable or more sensitive datasets. Likewise, in principle, I support a framework that recognises the spectrum of risk associated with different types and uses of data, and applies corresponding risk controls. However, in my view, these draft recommendations are in need of further refinement.

It appears the intention is to allow a wide of range of bodies to be accredited as trusted users, including all Australian Government agencies, all State and Territory agencies, and all Australian universities (draft recommendation 9.8). It is also envisaged that corporations and not-for-profit organisations may meet the requirements for trusted user status. In my view, this aspirational list of users may be too broad, particularly at a stage where the permitted uses of NIDs are yet to be determined or restricted in any way. Indeed, the intention is that there be as few restrictions as possible on what trusted users will be able to do with NIDs.

The draft report does state that trusted users should be '*accredited as capable of responsibly accessing and using* [NIDs]'. It also states that, in particular, these bodies should be covered under the Privacy Act, have appropriate governance structures, and have access to appropriate and secure facilities to enable safe data use.[31] I agree, however the specifics of this should be set out in further detail in the final report. Some factors which I believe should be addressed include:

- whether an entity is subject to legal obligations which will ensure the appropriate level of accountability, transparency and security required for 'trusted user' status. While the draft report suggests that coverage under the Privacy Act will suffice, the Commission may wish to consider whether additional conditions should be imposed, for example either under the new Data Act or via appropriate contractual mechanisms
- the entity's security capability (both in terms of its IT/other technological infrastructure, and physical work environments)

[31] Draft report, p 355.

- personnel vetting procedures/performance management of staff
- overall internal data governance capability (as discussed in the previous section),[32] and
- whether the community would, on the whole, consider that there would be a public benefit in enabling that particular user to access and use the most sensitive, identifiable NIDs. This will tie into the 'use' question as outlined in relation to social licence above.

As the new Data Act will allow trusted users to collect, share and use identifiable data in ways that individuals may not be aware of, and may not have consented to, use of this data should not be treated as 'business as usual'. I have already commented on the importance of social licence above, and the importance of establishing publicly acceptable uses for data. Ensuring adequate accreditation and oversight for trusted users will also be key to the success of the data reforms as a whole.

Further, I wish to caution that the vast majority of unit-level record datasets containing (or derived from) personal information may not be suitable for general, open publication, as envisaged in draft recommendation 9.4. This is because data of this kind requires additional mechanisms to be in place to ensure the risk of re-identification remains acceptably low (for example, the presence of physical and other control mechanisms which I have outlined earlier in this section, in relation to accreditation). Further, even where data may appear to be adequately de-identified, the risk profile of a dataset will change over time. Greater quantities of (ever richer) data will be produced and released (which could be matched with the dataset), and more sophisticated analysis techniques will become available. Therefore, once data has been released publicly, any increased risk of re-identification cannot be effectively contained. Control is effectively lost at the point of publication. For this reason, NIDs containing personal information (even where de-identified) should generally not be published openly, but shared only with trusted users.

However, restricting these datasets to trusted users need not hinder the goals of the proposed reforms. The entities which will be able to derive value from such datasets (i.e., researchers at universities) are likely to meet appropriate trusted user requirements.

Lastly, I note that draft recommendation 9.4 suggests that NIDs that contain 'non-sensitive' data should be immediately released. I note that the Privacy Act already contains a definition of 'sensitive information'.[33] However, it is not clear what non-sensitive data means in this context.

I therefore recommend that:

- the Commission develop an appropriate and robust framework for determining whether an entity should be given trusted user status, in a way that ensures appropriate accountability and oversight
- the Commission be mindful that very few NIDs involving personal information are likely to be suitable for open publication, and
- for clarity, a definition of 'non-sensitive data' be included in the final report (noting that generally, 'sensitive data' should be defined as any data containing or derived from personal information).

[32] As noted in the draft report, an example of a trusted user model that has been implemented in Australia is the Trusted Access Model based on the 'five safes' principle, which has been adopted by the Australian Bureau of Statistics (ABS).

[33] See s 6(1) of the *Privacy Act*.

Accredited Release Authorities (ARAs)

Draft Recommendations 9.6 and 5.1

9.6 - The NDC should accredit selected Australian and State/Territory Government agencies as ARAs; ARAs to determine what data can be made available to whom

5.1 – State-based linkage units should be able to apply for accreditation as Accredited Release Authorities (ARAs)

I am broadly supportive of draft recommendation 9.6. Under the proposed model, the NDC would have responsibility for oversight of Accredited Release Authorities. These are intended to be selected Australian and State/Territory government agencies, who would be responsible for managing NIDs, and deciding whether a dataset should be made available for public release or limited sharing with trusted users. The process for accreditation may be similar to that for the accreditation of integrating authorities, as currently overseen by the National Statistical Service (NSS).

As ARAs will be responsible for deciding whether datasets are available for public or limited release, they will play an important technical advisory role to government and the broader community.

I therefore recommend that:

- The number of bodies to be accredited as ARAs be kept to a minimum. Currently, there are only a handful of bodies in Australia who have been assessed as having the requisite expertise and safeguards in place, for example the Australian Bureau of Statistics, the Australian Institute of Health and Welfare, and the Australian Institute of Family Studies.[34]
- ARAs be subject to rigorous internal governance requirements and external oversight, given they will handle very large quantities of identifiable information.
- The new Data Act include governance requirements for ARAs. This will be particularly important for ARAs which are state-based bodies and are not subject to privacy legislation (for example, SA and WA-based bodies). The broader interaction between the Privacy Act and the new Data Act will determine the extent to which governance arrangements need to be built into the new Data Act. Either way, ARAs should be subject to standards which are, at the very least, as rigorous as the APPs/other relevant requirements in the Privacy Act.[35]

[34] These are all accredited integrating authorities. See the National Statistical Service's website for more information: http://www.nss.gov.au/nss/home.NSF/pages/Data+Integration+Landing%20Page?OpenDocument.

[35] The legislative framework which applies to the Australian Bureau of Statistics (ABS) may give an indication of the appropriate level of regulation required.

Other specific recommendations

Draft Recommendations 4.1, 5.1, 5.2 and 5.3

4.1 – Mandate comprehensive credit reporting if 40% participation is not achieved before 30 June 2017

I do not support the recommendation to mandate comprehensive credit reporting, if 40% participation is not achieved before 30 June 2017. As I said in my previous submission, I believe that this would be premature, particularly given that the Principles of Reciprocity and Data Exchange (PRDE) are currently in the process of being implemented.[36] These principles should help to improve participation rates, and were successfully negotiated between key affected stakeholders.

Further, the Australian Government accepted (in principle) the Australian Law Reform Commission's recommendation to review the changes to the credit reporting provisions in the Privacy Act five years after commencement (in 2019). This was intended to enable a more meaningful evaluation of the reforms, once they had been fully implemented by industry.[37]

5.1 - OAIC to produce de-identification guidance and certify entities that are using 'best practice' techniques

I support the Commission's recommendation that my Office should produce de-identification guidance. My Office is currently in the process of developing this guidance, and will conduct a public consultation on this resource during 2017.

However, I do not support the recommendation to give the OAIC a discretionary certification role in relation to 'best practice de-identification techniques', for a range of reasons. First, the OAIC is an independent regulatory body, and therefore it would not be appropriate for the OAIC to also have a role in 'certifying' best practice de-identification techniques. As the OAIC has responsibility for overseeing compliance with the Privacy Act, this could create a conflict of interest where certification has taken place, and then an alleged breach of protocol occurs.

Further, my Office does not at this time have sufficient in-house technical expertise to perform this role. In fact, I believe that many organisations would have difficulty securing ongoing expertise for this purpose, given there is a relatively limited number of experts in this field within Australia.

I therefore recommend:

- that the Commission modify draft recommendation 5.1, to remove the proposal to give the OAIC a power to certify best-practice de-identification techniques.

[36] OAIC Submission to Commission's Issues Paper 'Data use and Availability', August 2016, p 50.

[37] See the Australian Government's First Stage Response to the Australian Law Reform Commission Report 108, *For Your Information: Australian Privacy Law and Practice* (October 2009). Available at: www.alrc.gov.au/sites/default/files/pdfs/government_1st_stage_response.pdf.

5.2 – The medical research exceptions in the Privacy Act should be broadened to all research in the public interest; OAIC to develop associated guidance

I supported this recommendation in my earlier submission to the Commission on its Issues Paper. However, it is not clear to me how this will operate in light of the overhaul of the data governance regime as proposed in the Commission's Draft Report. If a dataset has been designated as an NID, then it would appear that this recommendation may not be necessary.

I therefore recommend that:

- the Commission clarify why this recommendation is needed. If it is still considered a necessary reform, the final report should explain how it will fit into the broader proposed reforms.

5.3 – The requirement to destroy linked datasets should be abolished

The draft report recommends that the requirement to destroy linked datasets should be abolished. The Commission states that this requirement is found in s 135AA of the *National Health Act 1953* (in relation to MBS and PBS data specifically), and in other requirements, such as the NSS's *High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes*.[38]

I recognise that it could be valuable to bring datasets together, to build enduring national linked datasets for research purposes. However, in moving to a model of enduring linkage, the potential public benefits of the ongoing retention of identifiable data in a linked form must be balanced against the increased privacy risks. These include security risks that data may be inappropriately accessed, as well as the risk of future unanticipated uses of such data.

To ensure that the retention of identifiable data in a linked form is consistent with the community's expectations, this proposal should be subject to public scrutiny. My comments above in relation to social licence apply equally here. Consultation should provide individuals with a clear understanding of how their information will be used, and an understanding of the benefits for them as well as the potential risks.

I note that at present, there appears to be a low level of community awareness about the risks and benefits of data integration projects. By way of example, the Australian Bureau of Statistics decided to retain name and address information from the 2016 Census in order to better enable data linkage and integration projects such as the Multi-Agency Data Integration Project (MADIP). However, this decision ultimately generated significant community concern. As Alistair MacGibbon, Special Adviser to the Prime Minister on Cyber Security, noted in his recently published *Review of the Events Surrounding the 2016 eCensus*, there was a failure to conduct adequate community consultation, which may have undermined support for the ABS's proposal: '[*t]he impact of the privacy concerns illustrates how privacy issues can escalate rapidly and cause significant reputational damage for agencies, endangering the viability of key government projects*'.[39]

In my view, if new enduring linked datasets are created it is important that an integrated approach to privacy management is taken from the beginning. This includes, for example undertaking a Privacy Impact Assessment before the linkage occurs, to identify and implement appropriate safeguards.[40] This

[38] See the Commission's draft report, p 204.

[39] Office of the Cyber Security Special Adviser, *Review of the Events Surrounding the 2016 eCensus* (13 October 2016), p 41.

[40] A privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. Further information about privacy impact assessments can be found on the OAIC website at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.

requirement could be included in the new Data Act framework. See also my recommendations relating to internal governance and accountability more broadly, above.

I therefore recommend that:

- the Commission consider whether the retention of linked datasets strikes an appropriate balance between achieving the relevant policy goals, and any impact on privacy. As part of this, it will be necessary to assess whether enduring data linkage and the handling of personal information is consistent with the community's expectations. This could be done as part of the broader consultation on permitted uses which I have recommended above.