Australian Government

Office of the Australian Information Commissioner

October 2016

National Education Evidence Base

Submission to Productivity Commission Draft Report

www.oaic.gov.au

Introduction

I welcome the opportunity to comment on the Productivity Commission's *National Education Evidence Base – Draft Report* (Draft Report). This submission complements and builds on my previous submission to the Productivity Commission's *National Education Evidence Base – Issues Paper* in June 2016 (Issues Paper Submission).

In my dual roles of Australian Information Commissioner and Australian Privacy Commissioner (the Commissioner), I am supportive of data-related activities which seek to maximise and enhance the use of public data. I recognise that these activities can yield significant public benefits. However, I also note that where data is entrusted to government agencies, and derived from personal information collected on a mandatory basis, it should be respected, protected and handled in a way that is commensurate with broader community expectations.

These considerations are heightened when data is derived from the youngest members of our community. Early childhood education and care providers (ECEC providers) and schools are among the most significant institutions shaping the future of our children and young people. A vast amount of personal information is collected by these institutions, over a number of years, for wide ranging purposes. This information enables a highly detailed picture to be built of children and young people from a very early age, which can include health information, academic aptitude and behavioural issues.

I appreciate the great potential that this information has to improve the development of education policy and programs. However, to ensure that the national education evidence base is effective in achieving its objective of helping to improve educational outcomes for Australia's children, it is imperative that privacy considerations are adequately addressed at the outset. Steps must be taken to acknowledge and mitigate against any risks associated with the long term collection and retention of a large volume of granulated information. Good privacy practice and community engagement strategies, underpinned by effective and consistent privacy regulation, will help to engender public trust and build a social licence to engage in data-related activities with children's personal information. Maintaining trust is vital to this type of ongoing data innovation and research. Not only is it a means of building community support for projects involving children and young people, but increased trust can lead to higher quality data by supporting a greater willingness to divulge accurate information.

I welcome the consideration that the Draft Report gives to the privacy risks and privacy protections that should apply in the framework for improving the national education evidence base. The Draft Report recognises that within the framework, there is scope to maximise the utility of data while still respecting the standards enshrined in privacy legislation. Greater uniformity of privacy laws is promoted as a means of reducing the regulatory complexity that contributes to the risk adverse behaviour of some data custodians. As Commissioner, my interest lies in promoting a consistent approach to privacy regulation throughout Australian jurisdictions, and I support moves towards greater uniformity of privacy laws and approaches to information sharing.

This submission addresses the information requests and recommendations set out in the Draft Report that have particular implications for privacy, including those relating to:

- the value of a unique (or universal) student identifier
- the obtaining of prior consent to facilitate greater access to data, and collection procedures more generally
- the streamlining of privacy provisions, specifically those dealing with
    - public interest research

- general privacy laws across jurisdictions, and

- the creation of enduring linked datasets.

In summary, my view is that when formulating recommendations in these areas the Inquiry should aim to strike an appropriate balance between any privacy risks and the potential benefits to the community. The success of any proposed initiatives will ultimately depend on whether or not the scheme engenders the community's trust and support. To this end, I support moves that will lead to greater transparency, and improve the ability of individuals to have control over their personal information.

I also support efforts to harmonise privacy regulation across Australia. Provided that care is taken to ensure that existing safeguards are not unduly weakened, I believe that harmonisation will reduce complexity and uncertainty about the operation of privacy regulation, and thus remove an impediment to information sharing. I am also in favour of a review of the framework for research under the *Privacy Act 1988* (Privacy Act), which could explore mechanisms for improving the availability of data for research.

Comments on the Draft Report

Information Request 4.1

The Commission seeks further information on:

- ***the costs and benefits of moving towards a national student identifier (compared to jurisdictional systems)***

As part of any assessment of the costs and benefits of moving towards a national unique student identifier (USI), I would encourage the Productivity Commission to consider the costs associated with the potential intrusion on individuals' privacy. It is important to ensure that the privacy risks of a national USI scheme do not outweigh its benefits to the community.

The introduction of a national USI creates an increased risk that the identifier, and information associated with it, will be able to be used beyond the original purposes. Such linkages may combine personal information that has been collected for very different purposes and create rich datasets about individuals' interactions in society. This creates the risk that the data may be put to unforeseen purposes beyond the research purposes contemplated in the creation of the data set. The degree of this risk will be highly dependent on the type of information that is associated with a USI. For instance, a heightened risk might be associated with some types of information, including sensitive information such as health information[1] or information that the community might consider to be more sensitive, such as information about behavioural issues with a child or their progress against development milestones. To guard against 'function creep' any national USI should be introduced with a robust legislative framework setting out clearly defined uses of the USI and information associated with it.

The successful implementation of a national USI will also depend on whether or not the scheme carries the public's trust and support. Given the privacy risks associated with unique identifiers, if a USI were to be introduced, it should be done in a transparent manner with sufficient consultation and scrutiny. The purposes for which the USI is to be used, and the public benefit of the scheme should be clearly articulated in a manner which can be understood by the community. Consideration should be given to the risks and benefits of linking different types of personal information to the USI, and to mechanism's for dealing with issues around individual's access to their personal information after the completion of education.

A Privacy Impact Assessment (PIA) is one mechanism that may assist in assessing and mitigating against privacy risks associated with a national USI.[2] A failure to adequately identify and manage contemporary privacy concerns carries the risk that it will not maintain the confidence of the public, potentially impacting the utility of any scheme introduced.

- ***the feasibility of using the unique student identifier system used in the vocational education and training sector to deliver more comprehensive student coverage***

The existing vocational education sector USI scheme in its current form is intended to:

[1] Sensitive information is a subset of personal information that is generally afforded a higher level of privacy protection under the APPs. For example, sensitive information includes information about a person's political opinions, religious beliefs, sexual orientation and health information (see s 6 of the Privacy Act).

[2] Available at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

- enable the student to create a current and certified record of any vocational training or education activities undertaken or completed, which can then be provided to potential employers
- prevent unnecessary retraining and the costs associated with investigating the qualifications of potential employees
- enable data held by the USI Registrar to be used for education research and development.[3]

Under the *Student Identifiers Act 2014* the Office of the Australian Information Commissioner (OAIC) has a role in overseeing the handling of the student identifier by the Student Identifier (SI) agency and other related entities.[4] The OAIC has a current memorandum of understanding with the SI Registrar and so has a particular interest in any potential expansion of the USI scheme. Furthermore, the OAIC has privacy oversight of a number of identifier schemes, including Healthcare Identifiers and Tax File Numbers, and has considerable experience in this area.

Drawing on this experience, it is not clear to me that the existing scheme is suitable for expansion to deliver more comprehensive student coverage. The USI scheme was primarily designed to provide vocational education and training students with the ability to obtain a record of their training, and was not designed to be used in other educational settings. The legislative framework for this scheme would need to undergo substantial amendment to ensure that it was fit for purpose across all education sectors, and able to safeguard the considerably increased amounts of personal information.

- ***the costs and benefits of children in the early childhood and care sector being covered by the same identifier as school students.***

The privacy implications of the use of a unique identifier for children in the early childhood education and care (ECEC) sector are similar to those I have set out above in respect of a national USI. However, the privacy risks are arguably compounded in the ECEC sector, given the longer timeframe over which information will be collected and held.

Careful consideration should be given to whether there might be any potential unforeseen long term consequences if information is to be collected from the very youngest members of our community, and retained throughout their schooling to the end of tertiary education. The length of time for which the information associated with the USI will continue to be relevant and provide a benefit to the individual (as opposed to the community as a whole) should also be taken into account in considering the benefits of introducing a USI in this sector.

Draft Recommendation 5.1

Agencies responsible for education data collections should amend their processes for collecting personal information from parents/guardians to incorporate formal consent and notification procedures regarding the use and disclosure of personal information at the initial point of collection.

I welcome steps to incorporate formal consent and notification procedures at the initial point of collection. Well thought out consent and notification procedures can provide parents and guardians

[3] Explanatory Memorandum, *Student Identifiers Bill 2014* (Cth), p. 2.

[4] More detailed information about the OAIC's role under the *Student Identifiers Act 2014* is set out in the *Issues Paper Submission*, page 15.

with greater transparency and choice about the management of their children's personal information. To maximise the privacy enhancing potential of these collection procedures, consideration should be given to the manner in which notification is provided, and to the steps required to ensure that consent is meaningful.

Consent

As outlined in the Draft Report,[5] consent is not the only basis for permitting personal information to be handled in a particular way under the Privacy Act. There are a range of other exceptions to APP 6, under which an entity may use and disclose personal information that was collected for a particular purpose for another purpose (a secondary purpose). However, requiring entities to obtain an individual's consent at the time of collection for the use of their personal information for research purposes is privacy enhancing, as it gives individuals greater control over their personal information. Seeking consent at the time of collection may also provide time and cost efficiencies for researchers, as it can help to avoid the subsequent need to pursue cumbersome, expensive and inefficient consent procedures for additional secondary uses or disclosures.[6]

A key element of consent is that the consent is current and specific. Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. To this end I suggest that when seeking consent, an individual should be informed of the likely period for which the consent will be relied on. Consideration might also be given as to whether innovative use of technology might be used to sustain the validity of a previously provided consent.

For any consent to be meaningful, it is also essential that the individual must give the consent voluntarily. To this end great care should be taken if 'bundled consents' are contemplated. Bundled consent refers to the practice of 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information. This practice has the potential to undermine the voluntary nature of the consent, as individuals are not provided with the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

A challenge is to ensure that any consent obtained is meaningful, and gives the individual the choice and control the Privacy Act is intended to provide. For this reason, the *APP guidelines* published by the OAIC explain the key elements of consent.[7] The APP guidelines also address some of the key challenges and issues in ensuring an individual's consent is meaningful. For example, the APP guidelines discuss:

- the limited circumstances in which use of an opt-out mechanism to infer consent may be appropriate (paragraph B.34)
- the potential for the practice of bundled consent to undermine the voluntary nature of consent (paragraphs B.39 – B.40)
- the assessment of whether an individual under the age of 18 has capacity to consent (as the Privacy Act does not specify an age after which individuals can make their own privacy decisions) (paragraph B.50 – B.52).

[5] *National Education Evidence Base – Draft Report,* Productivity Commission, (September 2016), p 125.

[6] Ibid, p 126.

[7] The OAIC's APP guidelines have been published to assist in interpreting the APPs and key concepts in the Privacy Act. They are available on the OAIC's website, at: www.oaic.gov.au/agencies-and-organisations/app-guidelines/.

Transparency and notice

In addition to supporting the exercise of meaningful consent, notification procedures underpin the exercise of individual choice and control and enhance the accountability of entities covered by the Privacy Act. Relevantly, APP 5 requires an APP entity to take reasonable steps to notify an individual of certain matters relating to the collection of their personal information before collecting the information, or as soon as practicable after (APP 5).

To be effective notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. Advances in technology present opportunities for more dynamic, multi-layered and user centric privacy policies and notices. Innovative approaches to privacy notices include 'just-in-time' notices, video notices and privacy dashboards and multi-layered privacy policies to assist with readability and navigability.

To assist entities in preparing effective notices, approaches aimed at ensuring privacy policies and notices contain clear, accessible and meaningful information have been suggested in a range of OAIC guidance, including the *APP guidelines*, the *Guide to developing an APP Privacy Policy* and *Mobile Privacy: a Better Practice Guide for Mobile App Developers.*[8]

Depending on the circumstances, a well drafted notification can help to establish that a secondary use was within the reasonable expectations of an individual. However, if the intent of a notification is to enable an entity to rely on the 'reasonable expectations' exception in APP 6.2(a), care should be taken to ensure that overly permissive privacy notices are not used to attempt to authorise secondary purposes. This is because under the APP 6.2(a) exception, even if a proposed use or disclosure is within the reasonable expectations of an individual, it must also be related (or directly related for sensitive information) to the primary purpose of collection. If the relationship between the primary and secondary purposes is not sufficiently close, this exception does not apply.

Draft Recommendation 5.2

The Australian Government should amend the Privacy Act 1998 (Cwlth) to extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover public interest research more generally.

Information Request 5.1

The Commission invites participants to comment on the operation of the section 95 guidelines in health research and lessons for other forms of research including education.

The Privacy Act recognises the strong public interest in the conduct of medical and health research, and provides a framework to facilitate data access arrangements for these research purposes. This framework consists of two sets of Guidelines:

- *Guidelines under Section 95 of the Privacy Act 1988* (s 95 Guidelines) which apply to agencies and provide an exception for acts that would otherwise breach the APPs where those acts are done in the course of medical research (and in accordance with the s 95 Guidelines).

[8] These are available on the OAIC's website, at: www.oaic.gov.au/agencies-and-organisations/guides/.

- *Guidelines approved under Section 95A of the Privacy Act 1988* (s 95A Guidelines) which apply to private sector organisations. The s 95A Guidelines deal with the collection of health information that is necessary for the secondary purpose of the management, funding or monitoring of a health service, and the collection use and disclosure of health information for research relevant to public health or public safety.

I agree in principle that there is value in looking to this model to guide considerations around data access arrangements for research in the education sector. However, certain aspects of the current framework of the Privacy Act in facilitating research were questioned by the ALRC in its 2008 Report,[9] with the ALRC making a number of recommendations in this regard. As noted in the Draft Report, these recommendations were not implemented as part of the 2014 reforms to the Privacy Act.[10]

The 2008 Report recommended that the Privacy Act should be amended to extend the existing arrangements relating to health and medical research to cover human research without consent more generally.[11] The ALRC also considered a move away from the current legislative provisions which require the two sets of Guidelines to be issued. It was found that having the two sets of Guidelines gives rise to inconsistency and confusion, leading to conservative and incorrect decision making. The ALRC recommended that the framework be amended so that "the Privacy Commissioner should issue one set of rules under the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle" to replace the current two sets of Guidelines.[12]

Given technological advancements and shifting community attitudes since the publication of the ALRC's *For Your Information Report* in 2008, I am of the view that it may be timely to re-evaluate the provisions, and consider whether it is still reasonable to limit the existing exceptions to health and medical research.

However, any enhancement of the framework for research under the Privacy Act would need to balance a range of factors, including the potential benefits to the community, the potential to adversely impact on individuals' privacy interests, and the potential impact that changes to the research framework might have upon community trust in the use of public data for research. Consistent with the existing exceptions set out in the Privacy Act, a revised framework should impose positive obligations upon an entity to asses:

- whether the personal information is reasonably necessary to achieve the purpose of the research
- whether de-identified information could achieve the purpose of the research
- whether it is reasonable and practicable to obtain consent.

Additional matters which could be considered could include a review of the measures which have been adopted by other jurisdictions, including s 27B in the *Privacy and Personal Information Protection Act 1998* NSW (PPIPA). Section 27B provides an exception to the application of several of the information protection principles, if the use or disclosure is reasonably necessary for research that is in the public interest, and if certain other conditions are met (including that s 27B will only apply if the public interest

[9] Australian Law Reform Commission report, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108 (2008) (ALRC Report 108).

[10] *National Education Evidence Base – Draft Report,* Productivity Commission, (September 2016), p 129.

[11] ALRC Report 108, Recommendation 65-2.

[12] ALRC Report 108, Recommendation 65-1.

purpose cannot be met if de identified information is used, and it is not practical to seek consent). It will also be important to consider accountability, oversight and assurance procedures.

An evaluation of the framework should be mindful of the importance of maintaining public trust in the framework, not just to build community support for data-related activities but also as an enabler of research interests, as increased trust can lead to a greater willingness to divulge accurate information, and to higher quality data.

Draft Recommendation 5.3

The ACT Government should enact in its privacy law an exception to cover public interest research. In Western Australia and South Australia where there is not a legislated privacy regime, their privacy arrangements should reflect a similar public interest research exception.

While ultimately a matter for each jurisdiction, I support efforts to harmonise privacy regulation across the various Australian jurisdictions. In my view, a nationally consistent or uniform approach to public interest research exceptions would help to avoid further fragmentation of privacy rights and obligations between Australian privacy jurisdictions, and improve cross jurisdictional data flows.

In particular, as a privacy regulator in both the Commonwealth and ACT jurisdictions, I welcome steps to ensure that a consistent approach is followed between the Commonwealth Privacy Act and the ACT's *Information Privacy Act 2014* (Information Privacy Act). I currently exercise some of the regulatory functions of the ACT Information Privacy Commissioner under an arrangement between the ACT Government and the Australian Government.

The Information Privacy Act includes a set of Territory Privacy Principles (TPPs). The TPPs set were modelled on the APPs, and apart from some minor textual differences are generally similar. It follows that maintaining a consistent approach between Commonwealth and ACT regulation of public interest research will help reduce the regulatory burden as well as allaying uncertainty about the privacy obligations which may apply to cross jurisdictional information sharing between these two jurisdictions.

I consider it particularly important for my Office to work together with other privacy authorities towards a co-ordinated, national approach to privacy regulation. Where possible, my Office seeks to maximise the opportunities that exist to work together with State and Territory privacy regulators, and, when appropriate, to align and harmonise our approach and policy advice.

Draft Recommendation 5.4

The Australian, state and territory governments should pursue legislative consistency in education and related Acts regulating the use and disclosure of education information, and amend legislation so that it is aligned with the intent of general privacy laws.

When personal information is subject to more than one regulatory scheme, compliance can become more complex. Regulatory overlap can potentially inhibit the sharing of data even where the applicable regulatory schemes do not prevent the sharing of personal information. Some agencies and organisations may adopt a more risk averse approach when sharing information due to a failure to understand their obligations.

Regulation should apply to all education sectors equally, establishing uniform standards and avoiding gaps or overlap in coverage. A consistent and nationally harmonised approach to education sector laws that authorise or limit the sharing of information would help to promote the clarity and confidence in information sharing necessary to develop the education evidence base. However, care should be taken

to ensure that existing safeguards for the protection of personal information are not unduly weakened and I welcome the consideration that has been given to alignment with the intent of privacy laws in the recommendation.

Draft Recommendation 5.5

The Australian, state and territory governments should introduce policy guidelines which place the onus on data custodians to share data unless a privacy (or other) exception can be justified.

The Draft Report recommends the introduction of guidelines that set out an expectation of information sharing as the default position, unless specific exceptions apply. This recommendation is in line with the Australian Government's broader data innovation agenda, which aims to enhance access to (and use of) data, in order to achieve innovation in the digital age. Australian government are agencies expected to share data by default "unless there are ongoing insurmountable legislative barriers or risks to privacy, security or confidentiality".[13]

My view is that within an appropriate framework, well drafted guidelines setting out expectations on data custodians when sharing information could create additional clarity, certainty and help to build public confidence. Guidelines could address the privacy risks associated with data projects involving personal information, including by helping to ensure appropriate ICT security measures are in place. The success of this framework, however, would be dependent on entities having the capability, and in particular the capacity to assess and manage privacy and security risks associated with sharing data.

Particularly if information sharing is the default position, for the guidelines to be effective in ensuring good privacy outcomes, privacy capabilities within an entity must be mature. If data custodians do not have adequate internal privacy capability they may not be able to identify and manage privacy and security risks in a way that maintains and builds public trust. Staff must be adequately equipped to assess not only general legislative and privacy compliance issues (such as compliance with the Privacy Act or other relevant legislation), but broader external risk factors (such as broader reputational risks if data is mishandled, and whether they have the requisite 'social licence' for any new or innovative uses of personal information). Privacy capability must encompass the ability to communicate well with the public about any new or innovated uses of data.

The capability of data custodians to address contemporary privacy issues needs to be strengthened and supported on an ongoing basis. The OAIC already has a range of resources which are intended to help entities understand their current capability levels, and identify what they need to do to achieve better practice.[14] The OAIC is also currently in the process of building on these resources with a focus on developing guidance on the application of the Australian Privacy Principles in the context of big data activities,[15] and is also revising its guidance on de-identification.[16]

---

[13] Department of Prime Minister and Cabinet, *Guidance on Date Sharing for Australian Government Entities*, March 2016 available at www.dpmc.gov.au/resource-centre/public-data/guidance-data-sharing-australian-government-entities

[14] This includes the Privacy Management plan template and Privacy Management Framework: enabling compliance and encouraging good practice, the Guide to securing personal information, the Guide to undertaking privacy impact assessments and the Data breach notification – A guide to handling personal information security breaches. These are available on the OAIC's website, at: www.oaic.gov.au/agencies-and-organisations/guides/.

[15] See the OAIC's website at: www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/.

[16] The OAIC intends to release an updated version of this resource in the near future. See the existing version on the OAIC's website, at: www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information.

To ensure that privacy issues are given appropriate regard, as part of the implementation of the guidelines, senior staff within the data custodian should be made directly responsible for broader strategic privacy policy issues, including issues relating to information sharing. This role could be similar to the role of Data Champions recommended by the Public Sector Data Management Project Report (PSDM Report).[17] Data Champions are senior officials within government agencies appointed to promote greater use and sharing of data within their agency. I suggest that appointing Privacy Champions would similarly help to provide cultural leadership and promote the value of personal information.

A failure to take adequate privacy and security measures could result in loss of confidence in projects which seek to harness the value of data. For this reason, I suggest that if guidelines were to be developed, they should also require that, where relevant, data custodians must undertake a written PIA prior to developing new information sharing arrangements or undertaking high risk data integration projects. I would encourage the use of a PIA to assess the potential privacy impacts of such projects to ensure that the personal information handling activities are accompanied by an appropriate level of privacy safeguards and accountability. The PIA should assess the overall proportionality of the project, and consider broader external perception risks. A mere 'tick-the-box' compliance approach should not be taken. A PIA can also be an important too in helping to build the community's trust that privacy risks have been identified, and necessary protections are embedded.

Draft Finding 6.1

The system of data linkage could be improved if linked data were retained by the linking authority.

The Draft Report also recognises the value that could be achieved by bringing datasets together to build enduring national linked datasets for research purposes. I appreciate that the move away from a link and destroy model to a create, reuse and keep model presents a number of efficiencies and opportunities to improve the education evidence base.[18]

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 the data may be inappropriately accessed as well as the risk of future unanticipated uses of the data. Consideration must be given to whether the retention of linked data sets strikes an appropriate balance between achieving 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.

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 rigorous public scrutiny. Consultation should provide individuals with a clear understanding of how their information will be used, and an understanding of the benefits for them.

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 PIA that considers:

- whether any restriction on an individual's right to privacy that arises from the creation of the dataset is reasonable, necessary and proportionate to the expected benefits

[17] Department of the Prime Minister and Cabinet, Public Sector Data Management Report (July 2015).

[18] *National Education Evidence Base – Draft Report,* Productivity Commission, (September 2016), p 145.

- whether personal information is in fact required, or whether de-identified or anonymised information will suffice
- the governance arrangements of the entity performing the linkage and maintaining the dataset, including whether it has the requisite skills, processes, infrastructure and culture to undertake such a role
- what safeguards can be implemented to make clear the uses the dataset can be put to and limit the possibility of function creep as well as the controls that could be put in place around the criteria for granting access to the data set and its security.

One way which these privacy safeguards could be built in is 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 out the requirements for establishing and maintaining enduring linked datasets. Creation of a code would not only provide greater certainty as to how APP obligations should be met but can also provide individuals with additional transparency about how their information will be handled as part of the dataset. For more information about APP codes, see the OAIC's *Guidelines for developing codes*.[19]

[19] Available at www.oaic.gov.au/agencies-and-organisations/advisory-guidelines/guidelines-for-developing-codes.