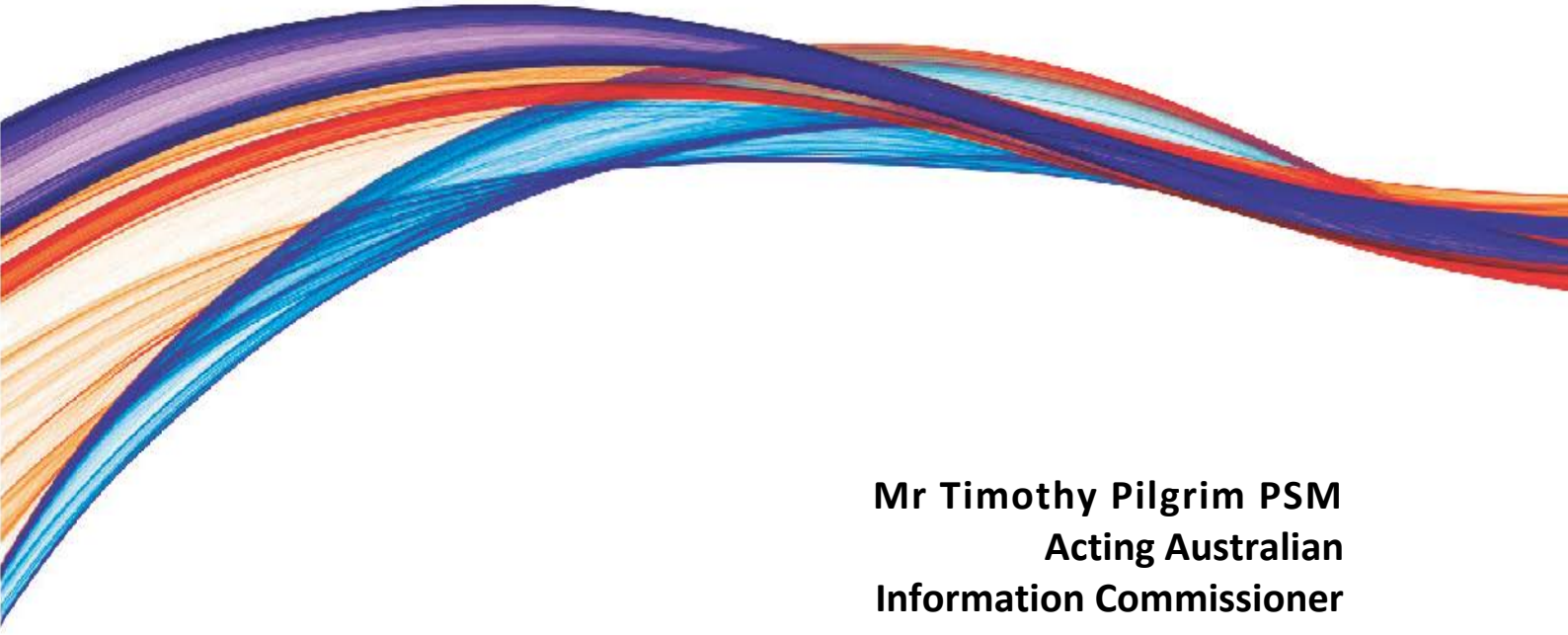
Australian Government
Office of the Australian Information Commissioner

National Education Evidence Base

Submission to Productivity Commission

June 2016



Mr Timothy Pilgrim PSM
Acting Australian
Information Commissioner

Contents

Introduction: Good privacy management facilitates data innovation

I welcome the opportunity to comment on the Productivity Commission's *Issues Paper for the Inquiry into the National Evidence Base for School and Early Childhood Education* (Issues Paper).

The creation of a more comprehensive and consistent national education evidence base can provide a valuable resource to improve Australia's educational outcomes. The Issues Paper suggests that while Australia already has significant data assets the potential of this data is not being capitalised on and fully realised.[1] Lost opportunities will continue to grow as technology opens up new ways to use and analyse data. However, realising the potential of these national assets can only occur sustainably, if privacy is integral to the equation. Simply put, a successful data-driven economy needs a strong foundation in privacy.

Privacy, however, is often named as the primary barrier to sharing or accessing personal information from and across government agencies – that is not correct. Privacy rather than preventing the sharing of personal information places important limitations around the circumstances under which it can be collected, used and disclosed. Instead, and as identified in the Issues Paper, impediments to appropriate information sharing often include a general reluctance to disclose personal information due to misunderstandings of privacy law, secrecy issues and a risk averse culture within agencies.[2]

This submission addresses issues relevant to terms of reference three and four of the Inquiry into the National Evidence Base for School and Early Childhood Education (Inquiry). It explains how the right to privacy is regulated in Australia and considers the role privacy legislation plays in the sharing of education relevant data to support Australia's educational outcomes.

Generally speaking, I believe that the *Privacy Act 1988* (Privacy Act) provides an appropriate and effective framework for the sharing of personal information in a manner that safeguards individuals' privacy. Technological changes and shifts in community expectations may make a case for, the way in which the Privacy Act deals with sharing and accessing information for research purposes to be reviewed and further enhanced. Review may assist in identifying other mechanisms for making information available for research, whilst maintaining robust and appropriate privacy protections. I would welcome the opportunity to engage in further debate on the possible means of achieving this.

Key Recommendations

The Office of the Australian Information Commissioner recommends that:

[1] Productivity Commission, *Issues Paper for the Inquiry into the National Evidence base for School and Early Childhood Education* (May 2016), page 21.
[2] Issues Paper, page 21.

1. Australian Government agencies involved in the collection, use or disclosure of personal information in the national education evidence base, could review any applicable secrecy or confidentiality provisions, to determine whether these provisions are still relevant to their circumstances.
2. Australian Government agencies involved in the collection, use or disclosure of personal information in the national education evidence base ensure they have developed and implemented policies to clarify the application of their enabling legislation to their information holdings, clearly setting out the circumstances in which the agency will and will not share the information.
3. A legislative review be undertaken to:
    a. consider whether it is still reasonable to limit the existing research exceptions in the Privacy Act to health and medical research and
    b. to explore other mechanisms to facilitate the availability of data for research whilst maintaining adequate protection for personal information.
4. Should a unique identifier be proposed for the education sector, that a privacy impact assessment be undertaken for the purpose of privacy risk identification and mitigation.

About the Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth statutory agency within the Attorney-General's portfolio. The OAIC integrates three key functions:

- protecting the public's right of access to documents under the *Freedom of Information Act 1982* (FOI Act)
- ensuring proper handling of personal information in accordance with the standards of the Privacy Act
- providing advice to government on information policy and practice in accordance with the *Australian Information Commissioner Act 2010* (AIC Act).

In the exercise of these three functions, the OAIC is cast in the various roles of regulator, decision maker, adviser, researcher and educator.

Of particular relevance to this inquiry, the integration of the functions of information policy, independent oversight of privacy protection and freedom of information in one agency, places the OAIC in a unique position to contribute to the discussion on optimising the use of education relevant data while protecting privacy rights.

The FOI Act, which the OAIC has responsibility for regulating, is underpinned by the principle that government held information is a national resource. The OAIC has long

supported the view that the value of this information is often best realised when it can be shared, used and built upon.

A key objective in government information management is to make public sector information available to the community as openly as possible, in a form that is both discoverable and reusable. Over the last 6 years the OAIC has done a great deal of work to encourage an 'open access by default' approach to government information. This includes the earlier development by the OAIC of *Principles on open public sector information*, which encourage default open access as the first principle, followed by the need to engage the community. The OAIC has encouraged agencies to embed these principles into their internal policies and procedures on information management to help build a culture of proactive information disclosure and community engagement.[3]

In 2016, with open government an ongoing priority and with data analytics set to expand as a key policy and service development tool, the OAIC is developing and updating resources in this area. This includes:

- a consultation underway on a draft *Guide to big data in the context of the Australian Privacy Principles*. This has been developed in recognition of the use of data, and its potential to bring about social and economic benefits. The draft guide is aimed at facilitating big data activities while protecting personal information.
- de-identification has the potential to be a privacy enhancing tool that facilitates data sharing, unlocks big data, and supports the Internet of Things. The OAIC will be revisiting its guidance on de-identification in coming months.[4] To that end we will be conducting a series of conversations, through the OAIC's Privacy Professional's Network and other networks, to work with business, government, consumer and technical groups on the possibilities of big data and de-identification.
- guidance for Australian Government agencies is also being developed to address factors that prevent effective information sharing and provide a framework for considering whether information should be shared under the Privacy Act.

How is the right to privacy regulated in Australia?

In Australia, personal information in data sets may be subject to privacy specific legislation, including the Commonwealth Privacy Act, and State and Territory privacy

[3] The OAIC has developed *Principles on open public sector information*, to define standards and principles to shape government information management practices. Further resources on information policy are available on the OAIC website.

[4] The current OAIC guidance *Information policy agency resource 1: De-identification of data and information* and *Privacy business resource 4: De-identification of data and information* *are* available on the OAIC website.

legislation. Personal information may also be subject to additional legal obligations such as statutory secrecy provisions and contractual or common law duties.

The Australian *Privacy Act 1988*

The Privacy Act gives effect to, among other things, Australia's agreement to implement the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)[5], as well as to its obligations under Article 17 of the *International Covenant on Civil and Political Rights*.[6] The Privacy Act establishes a strong and effective mechanism for protecting individuals' personal information, that is, information or an opinion about an identified individual, or an individual who is reasonably identifiable.[7]

The objectives of the Privacy Act include promoting the protection of the privacy of individuals and promoting the responsible and transparent handling of personal information by entities.[8] The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, accessing and correction of personal information (including sensitive information).[9] The principles are structured to reflect the information lifecycle and each of the principles interact with and complement each other. A breach of an APP is an 'interference with the privacy of an individual'.

As principles-based law, the Privacy Act is able to apply to many different Australian Government agencies and industry sectors, and to the myriad of ways personal information is handled in Australia. Moreover, the Act provides an accessible mechanism for individuals to complain to the OAIC about acts or practices that may be an interference with their privacy and a range of powers that allow me as Commissioner to resolve those disputes.

Recent Reforms to the Privacy Act

Significant amendments to the Privacy Act came into force on 12 March 2014. These amendments included the replacement of the Information Privacy Principles (applying to public sector agencies) and the National Privacy Principles (applying to private sector

[5] In 1980 the Organisation for Economic Co-operation and Development (OECD) published its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines). The guidelines represent an international consensus on how best to balance effective privacy protection with the free flow of personal data. Although there are jurisdiction-to-jurisdiction variations in the way they are implemented, they are the universal information privacy law benchmark.

[6] The objects in s 2A of the Privacy Act include 'to implement Australia's international obligation in relation to privacy' (s 2A(h)).

[7] Section 6(1) of the Privacy Act.

[8] Sections 2A(a) and 2A(d) of the Privacy Act.

[9] 'Sensitive information' is a subset of personal information and is defined in s 6(1) of the Privacy Act. Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information (for example, see APPs 3 and 6).

organisations) with the APPs, the amendment of the Part IIIA credit reporting provisions, and new regulatory powers for the OAIC.[10]

The amendments aimed to modernise privacy law in response to developments in technology, data acquisition and management, domestic and global information flows, and heightened community privacy awareness and concern.

Coverage of the APPs

The APPs apply to most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities').[11] APP entities can include individuals (including sole traders), body corporates, partnerships, unincorporated associations and trusts.[12]

Many private sector educational organisations and institutions are covered by the Privacy Act either because they:

- are connected to a larger organisation (with a turnover of more than $3 million)
- provide a health service and hold health information (even if providing a health service is not their primary activity).

This includes most private childcare centres, private schools and private tertiary educational institutions.[13]

Is 'ownership' a relevant concept under the APPs or the Privacy Act?

When considering issues around access to data sets questions of ownership and custodianship may be asked. These are not concepts found in the Privacy Act and questions that are not applicable to determining the obligations which will apply under the Privacy Act. The APPs create obligations for APP entities when they 'hold' personal information. An APP entity 'holds' personal information if 'the entity has possession or control of a record that contains the personal information'.[14] The APPs will apply to personal information which has been collected or is held by an APP entity, regardless of whether or not that entity is the owner of the personal information.

[10] The amendments stemmed from recommendations made by the Australian Law Reform Commission report, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108 (2008)
[11] The terms 'APP entity' and 'agency' are defined in s 6(1) of the Privacy Act. The term 'organisation' is defined in s 6C of the Privacy Act, and the term 'small business operator' is defined in s 6D of the Privacy Act.
[12] Section 6C(1) of the Privacy Act.
[13] This does not generally include State or Territory government bodies.
[14] Section 6(1) of the Privacy Act.

State and Territory privacy laws

The Privacy Act generally does not apply to State and territory government agencies.[15]

Instead, as noted in the Issues Paper[16], where they exist, state and territory laws create information privacy requirements similar to those under the Privacy Act (the exceptions are Western Australia and South Australia). These generally apply to state and territory government agencies as well as local councils, state and territory government-owned corporations and universities.[17] These laws provide various mechanisms for individuals to make complaints and seek redress. With the exception of the Australian Capital Territory (ACT) *Information Privacy Act* 2014, the OAIC does not have regulatory responsibilities in relation to these laws.[18]

In many cross jurisdictional information sharing arrangements, personal information would be subject to more than one regulatory scheme. Regulatory overlap potentially can restrict access to data even where the applicable regulatory schemes do not prevent the sharing of personal information, as some agencies and organisations may adopt a more risk adverse approach when sharing information across jurisdictions.

The OAIC, along with other Australian privacy authorities has formed Privacy Authorities Australia, a group which meets regularly to promote best practice and consistency of privacy policies and laws. I consider it particularly important for the OAIC and other authorities to work towards a co-ordinated approach, nationally, to privacy regulation.

Additional legal obligations

While the Privacy Act provides an overarching framework for how personal information should be handled, additional legal obligations apply to some types of data and may have implications for information sharing and access. This includes enabling legislation for government agencies which may expressly or impliedly authorise or limit the sharing of information. Data sets may also be subject to confidentiality provisions, contractual obligations or to equitable obligations based in the common law (such as an obligation to maintain confidence). Statutory secrecy provisions[19] can complement the framework provided by the Privacy Act. Secrecy provisions serve an important role in circumstances

[15] However, section 6F of the Privacy Act provides for a State or Territory authority or an instrumentality of a State or Territory to be prescribed in the Privacy Regulations in certain circumstances, with the effect it will be treated as an organisation under the Privacy Act.
[16] Issues Paper, page 21.
[17] *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Premier and Cabinet Circular No 12* (SA); *Personal Information Protection Act 2004* (Tas); *Privacy and Data Protection Act 2014* (Vic); *Information Privacy Act 2014* (ACT); *Information Act* (NT). For more information about State and Territory privacy laws, please see Other privacy jurisdictions on the OAIC website.
[18] Under an arrangement between the ACT Government and the Australian Government, the OAIC is exercising some of the functions of the ACT Information Privacy Commissioner. For more information on the OAIC's role, please see Australian Capital Territory Privacy on the OAIC website.
[19] These can apply to a specific type of information (such as tax file numbers), or can be agency specific in that they address where the agency needs to protect the confidentiality of personal information as they carry out their particular activities. The ALRC identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences in the its report *Secrecy Laws and Open Government in Australia (ALRC Report 112)* (2010).

where a need has been identified for that information to be subject to additional protections or specific handling requirements over and above those afforded by the Privacy Act.

However, I note the recommendation of the ALRC in their 2010 report, *Secrecy Laws and Open Government in Australia*, that for effective information handling, agencies need to develop and implement policies to clarify the application of relevant secrecy laws to their information holdings.[20] I encourage agencies involved in the national education evidence base to ensure they have implemented this recommendation. I believe that by providing clarity about the situations in which an agency can and cannot share information, an information handling policy can alleviate some of the barriers to information sharing identified in the Issues Paper.[21] Implementing good information handling practices and governance arrangements not only helps to ensure compliance with the APPs but also can help to develop more efficient business processes.[22] Agencies may consider also reviewing the relevant secrecy and confidentiality provisions to determine whether they are still needed.

Privacy regulation and education relevant data sharing provisions

The Privacy Act is built on the central principle that personal information collected for one purpose should generally not be used or disclosed for a secondary purpose. Questions around the secondary use and disclosure of personal information have often proven to be a point of uncertainty and may contribute to the reluctance to make information available, even where this is permissible. There is no doubt that emerging data innovation practices require fresh consideration about how key existing privacy principles — including notice and consent, data collection, use limitation, and retention minimisation — work in practice. However, as principles-based law, the Privacy Act is flexible enough to support all manner of data initiatives and sharing, provided that an integrated approach to privacy management is taken up front.

Information sharing under the Privacy Act

The sharing of personal information is governed by the collection, use and disclosure provisions of the Privacy Act. I recognise that the usefulness of data can be greatly increased when information is shared, reused and built upon. The wide variety of personal information that is held by educational institutions and government agencies can be an immensely valuable data resource for policy, planning, research and innovation – ultimately providing better services to Australian communities.

If this personal information is to be shared for social research purposes, then it must be done respectfully and sensitively. Improving access and sharing of information both from

[20] See Recommendation 14-1, ALRC Report 112.
[21] Issues Paper, page 21.
[22] APP 1.2 requires APP entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. See the OAIC's Privacy Management Framework available through the OAIC website for more information.

and across Australian Government agencies offers immense potential to improve policy and service delivery, provided it is done in a way that supports and protects the existing rights of those from whom the information was derived.

The Australian Privacy Principles

The APPs provide a framework for agencies to share personal information in a manner that safeguards individuals' privacy. The OAIC has issued non-binding APP Guidelines[23] to explain the mandatory requirements in the APPs and set out the OAIC's interpretation of the APPs, including the matters that may be taken into account when exercising functions and powers relating to the APPs.

The Privacy Act recognises that the protection of individuals' privacy, through the protection of their personal information, is not an absolute right. Rather, those interests must be balanced with the broader interest of the community in ensuring that APP entities are able to carry out their legitimate functions and activities. This balancing is reflected in the objects of the Privacy Act, as well as in some of the exceptions to a number of the APPs. These exceptions operate to exclude certain information handling practices from breaching one or more APPs where the practice is considered to be in the public interest when balanced with the interest in protecting an individual's privacy.

The collection of personal information for research purposes

The Privacy Act sets out a number of obligations for entities collecting personal information, including collection for research purposes.

APP 3 outlines when an APP entity may collect solicited personal information. An entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information.

APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. For personal information (other than sensitive information), an APP entity that is:

- an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities
- an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities.

APP 3 contains a different requirement for the collection of sensitive information compared to other types of personal information. Unless an exception applies, such as where the collection is required or authorised by law, an APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.

Personal information must only be collected by lawful and fair means. Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to agencies).

[23] *Australian Privacy Principles guidelines* available on the OAIC website.

APP 5 provides that an APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. The matters include (but are not limited to) the purposes of collection and the entity's usual disclosures of personal information of the kind collected by the entity. This requirement applies where either the personal information has been collected from a third party or the individual may not be aware that the entity has collected their personal information. These provisions have implications for entities:

- collecting personal information for the primary purpose of research; and
- those entities collecting personal information for a different purpose but are aware the information is likely to be used or disclosed for research purposes at a later date.

The practical consequence is that, if the APP entity plans to routinely use or disclose personal information for research purposes, in addition to the primary purpose, this secondary purpose should also be included in the APP 5 notice. A privacy notice that sets out a range of likely secondary uses or disclosures may assist an APP entity in establishing an individual's consent to, or reasonable expectation of, those uses or disclosures (see discussion below).

The use of disclosure of personal information for research purposes

Under APP 6, an APP entity can only use or disclose personal information for a secondary purpose if an exception applies. The most relevant exceptions to information sharing for a research purpose include:

- *where the individual has consented to the use or disclosure (APP 6.1(a))*

  While it will not always be possible to obtain consent, advantages of doing so include:

  - an individual is provided with greater transparency and choice about the management of their personal information
  - the entity is able to use the information for a wider range of applications than may have been within the reasonable expectations of the individual (see below).

- *where the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP 6.2(a))*

  This exception creates a two-limb test which focuses both on the reasonable expectations of the individual, and the relationship between the primary and secondary purposes. Notices (APP 5) and privacy policies (APP 1) may serve to support the 'reasonable expectations' test and expand the range of uses that personal information can be put to. However, to rely on the exception the relationship between the purposes must be sufficiently close. This may mitigate against the use of overly permissive privacy notices to 'authorise' secondary purposes.

- *if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).*

  If an entity is considering seeking legislative change to enable a use or disclosure for a secondary purpose, I suggest that any proposed law or practice is appropriately balanced with the overall public policy objectives. That is, the law or practice is reasonable, proportionate and necessary and the least privacy invasive option.

Taking a 'privacy by design' approach to information sharing

The object of APP 1 is 'to ensure that entities manage personal information in an open and transparent way'. This enhances the accountability of entities' personal information handling practices, which in turn can build community trust and confidence.

APP 1 lays down the first step in the information lifecycle – planning, and explaining how personal information will be handled before it is collected. In practice, APP entities may comply with APP 1 by implementing the OAIC's *Privacy Management Framework* and adopting a 'privacy by design' approach to information sharing arrangements.[24]

The 'privacy by design' approach is about finding ways to build privacy into systems and projects from the design stage onwards.[25] To optimise the value of data which includes person information, at the outset of any project there are certain steps that an entity can take to minimising risks to an individual's privacy while maximising the range of permissible uses of the data.

Entities should consider:

- *the likely purposes for which the information will be used, including any uses or disclosures for secondary purposes*

  Entities should consider how necessary secondary uses or disclosures might be achieved and how the privacy impacts will be addressed.

- *what personal information can be collected*

  Entities collecting personal information are required to consider what personal information is reasonably necessary and for what purpose (APP3).

- *how it should be collected, including whether any consents should be sought*

  Seeking consent at the time of collection is particularly important if the information is to be used for multiple research projects, as seeking consent at a later time for a secondary use of personal information can be costly and difficult.

- *the type of notice of collection that should be provided to the individual*

  A privacy notice, provided at the time of collection, that clearly describes the range of likely secondary uses of personal information, can help to establish

[24] The OAIC's *Privacy Management Framework* is available on the OAIC website.

[25] Privacy by Design was first developed in the 1990s by the former Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian. Since then it has been adopted by both private and public sector bodies internationally. For further information, see http://privacybydesign.ca.

consent to a secondary use or disclosure, or may assist an entity to establish that an individual would have reasonably expected the use or disclosure.

Privacy impact assessments (PIA) are one practical tool that can assist in facilitating 'privacy by design' and addressing the above considerations. A PIA identifies how a project can impact an individual's privacy and makes recommendations for managing, minimising or eliminating privacy impacts. Undertaking a PIA can assist APP entities to build privacy considerations into the design of a project and achieve their objectives while minimising the negative and enhancing the positive privacy impacts. A PIA can also help to build the community's trust that privacy risks have been identified, and necessary protections are embedded.

The OAIC strongly recommends that entities conduct PIAs as part of their regular risk management and planning processes. In addition, the Commissioner may formally direct an agency (though not an organisation) to conduct a PIA for new projects involving personal information, where the OAIC considers that the activity or function might have a significant impact on the privacy of individuals.[26] The scope of this provision is to be reviewed within 5 years of its commencement, to assess whether this section should also apply in relation to organisations.[27]

There is no formula to completing a PIA. Each PIA will vary depending on the nature and extent of personal information that is involved in a project. The OAIC's *Guide to undertaking privacy impact assessments* sets out a suggested ten step process for undertaking a PIA.[28]

Public Interest Determinations

In some circumstances, the public interest in conducting research projects by using personal information without the consent of the individuals involved may substantially outweigh the public interest in maintaining privacy. Where such circumstances arise, and is not possible to either to use de-identified data and the activity cannot otherwise be accommodated within the relevant privacy principles, the Public Interest Determination (PID) mechanism provided in the Privacy Act could be drawn upon to facilitate the research.

Part VI of the Privacy Act gives the Information Commissioner the power to make a determination, by legislative instrument, that an act or practice of an Australian Government agency, or a private sector organisation, which may constitute a breach of an APP or a registered APP code that binds the entity, shall be regarded as not breaching that principle or registered code for the purposes of the Privacy Act. In doing so, the Information Commissioner must be satisfied that the public interest in doing the act or practice substantially outweighs the public interest in adhering to the APP or registered APP code.

[26] Section 33D of the Privacy Act

[27] Section 33D(7) of the Privacy Act provides that 'before the fifth anniversary of the commencement of this section, the Minister must cause a review to be undertaken of whether this section should apply in relation to organisations.'

[28] *Guide to undertaking privacy impact assessments* is available on the OAIC website.

The OAIC maintains a register of PIDs on its website[29] and notes that this mechanism has been utilised previously to facilitate research projects.[30]

De-identification

A key mechanism to be able to share and access data sets without revealing personal information is to de-identify it. Data that has been successfully de-identified is not personal information and the Privacy Act will not apply to its handling. I encourage any entity which is considering sharing educational relevant data to first consider whether de-identified personal information could be utilised.

De-identification, if done properly, can be a highly effective privacy solution when sharing personal information for research purposes. De-identifying personal information for the purposes of information sharing means the information may be used, shared and published without jeopardising personal privacy. In many cases this enables organisations to harness the utility and value of the information while safeguarding privacy. De-identifying information also lessens the risk that personal information will be compromised should a data breach occur.

Many organisations and agencies are unsure about how to de-identify data appropriately, and in some cases end up releasing personally identifiable information. I consider that this is an area of regulation where agreed industry terms and standards are important — not only to the actual efficacy of de-identification, but also to provide public confidence in it as a solution. To this end, I will be commencing a national conversation about de-identification and opening up consultation on renewed guidance later this year.

Data access arrangements for research under the Privacy Act

Research exceptions for health and medical research

The Issues Paper invites consideration of data access arrangements in the non-education sector and references the use of personal information without consent in the health sector for research.[31] 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. 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.

The framework includes *Guidelines under Section 95 of the Privacy Act 1988* (s 95 guidelines) and *Guidelines approved under Section 95A of the Privacy Act 1988* (s 95A

[29] See www.oaic.gov.au/privacy-law/privacy-registers/public-interest-determinations/
[30] See by way of example, Public Interest Determination No. 5 (www.legislation.gov.au/Details/F2014C00255), Public Interest Determination No. 8 (https://www.legislation.gov.au/Details/F2008B00572) and Temporary Public Interest Determination No. 2010-1 (https://www.legislation.gov.au/Details/F2010L01206)
[31] Issues Paper, pages 21 and 23.

guidelines). Both sets of guidelines are issued by the CEO of the NHMRC, with the approval of the Australian Information Commissioner.

The Section 95 and 95A guidelines do not apply to the collection, use and disclosure of health or medical information by agencies or organisations that are not covered by the *Privacy Act*. For example, they do not apply to the handling of personal information for research purposes by public hospitals and associated research bodies. These bodies may however have obligations under State legislation.

Dealing with personal information under s 95A

The s 95A guidelines only apply to organisations. Where an organisation wishes to use or disclose health information for the secondary purpose of research, it should consider whether the permitted health situation exception applies (APP 6.2(d)). Under this exception an organisation may use or disclose health information that is necessary for the secondary purpose of research relevant to public health or public safety if:

- it is impracticable to get the individual's consent
- the use or disclosure is conducted in accordance with the s 95A guidelines approved by the Information Commissioner
- for disclosure, the organisation reasonably believes the recipient will not disclose the information, or personal information derived from the information.[32]

Whether it is impracticable to seek consent will depend on the particular circumstances of the case. An organisation relying on this permitted health situation will need to justify why it is impracticable to obtain an individual's consent. Incurring some expense or doing extra work to obtain consent would not itself make it impracticable to obtain consent.

The organisation must be satisfied that the research for which health information is to be used or disclosed has been approved by a Human Research Ethics Committee (HREC) in accordance with the guidelines. The HREC may approve a proposed research activity where it is determined that the public interest in the research activity substantially outweighs the public interest in the protection of privacy.

Dealing with personal information under s 95

Section 95 applies to agencies and provides 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 s 95 guidelines.

An agency seeking to rely on the s 95 guidelines must be satisfied that the research for which the personal information is to be handled has been approved by an HREC for the particular purpose in accordance with the guidelines. In making a decision under these guidelines, a HREC must consider whether it is reasonable for the research to proceed without the consent of the individuals to whom the information relates. Under the s 95 guidelines the public interest in the research must outweigh, to a substantial degree, the

[32] See section 16B(3) of the Privacy Act.

public interest in protecting privacy. In addition, the proposed handling of personal information must be done in the course of medical research.

Review of the research exceptions in the Privacy Act

Certain aspects of the current framework of the Privacy Act in facilitating research were questioned by the ALRC in its 2008 Report,[33] with the ALRC making a number of recommendations in this regard. These recommendations were not implemented as part of the 2014 reforms to the Privacy Act.

As part of its review, the ALRC questioned the limited scope of the research exceptions in the Privacy Act and considered options for their expansion. The ALRC found that there was no in-principle reason to limit the arrangements for research under the Privacy Act to health and medical research. Further, other areas of research, such as sociology and criminology, have a strong public interest basis because of their potential to lead to evidence-based policy development and significant positive outcomes for the community. 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.[34]

The ALRC also considered that having the two sets of guidelines gives rise to inconsistency and confusion, leading to conservative and incorrect decision making, and recommended 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 Guidelines.[35]

Given technological advancements and shifting community attitudes since the publication of the 2008 report, I am of the view that, if the case could be made as to the need, it would be timely to re-evaluate the provisions, and consider whether it is still reasonable to limit the existing exceptions to health and medical research. A review of the framework for research under the Privacy Act would enable other mechanisms to be explored, to facilitate the availability of data for research whilst maintaining adequate protection for personal information.

A unique identifier for the education sector

The Issues Paper invites consideration of the costs and benefits of a unique identifier, or expanding the current Unique Student Identifier (USI) to students in schools and early childhood education and care, to better balance confidentiality with utility of data. The USI scheme currently applies to individuals undertaking nationally recognised vocational education and training.

[33] Australian Law Reform Commission report, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108 (2008) (ALRC Report 108).
[34] Recommendation 65-2 ALRC Report 108.
[35] Recommendation 65-1 ALRC Report 108.

The USI scheme

This USI scheme in its current form is intended to deliver a number of direct benefits to students and to the community at large. It:

- enables 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
- prevents unnecessary retraining and the costs associated with investigating the qualifications of potential employees
- enables data held by the USI Registrar to be used for education research and development.[36]

The *Student Identifiers Act 2014* establishes a privacy oversight function for the Australian Information Commissioner in relation to the handling of the student identifier by the Student Identifier (SI) agency and other related entities. 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.

Given the USI scheme has been primarily designed to provide vocational education and training students with the ability to obtain a record of their training, it is not clear to the OAIC whether the existing scheme is suitable for expansion across the education sector or to be used for the primary objective of enhancing data linkage.

Framework for a unique identifier

If a new unique identifier for the education sector is proposed, it is important that the intrusion on individuals' privacy is appropriately balanced with the overall public policy objectives of the identifier. That is, whether the introduction of a unique identifier is reasonable, proportionate and necessary and the least privacy invasive option to achieve the policy objective.

In this regard, I note that the use of an identifier is expected to provide balance between confidentiality and utility of data for linkage purposes. There are a number of benefits from using an identifier to enhance data accuracy and increase administrative efficiency. The use of an identifier can be an effective means to facilitate the linkage between disparate datasets. However, when calculating the potential costs and benefits of such a scheme, the Productivity Commission will need to take into account that it will not address the problem of linking education data to data collections outside of the education sector.

Any unique personal identifier raises a significant privacy risk of inappropriate data linking or use of the identifier without justification beyond the original purposes. Such linkages may combine personal information that has been collected for very different

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

purposes and create rich datasets about individuals' interactions in society. Given the privacy risks associated with unique identifiers, it is important that identifiers are not permitted to be used beyond their original intention without sufficient consultation and scrutiny. The introduction of an identifier to the education sector therefore needs to be accompanied by strong legislative safeguards to limit the possibility of 'function creep'.

For the full value of a new identifier to be realised, it should be introduced in a transparent manner and with a robust legislative framework. As part of this process, the OAIC considers that a privacy impact assessment must be undertaken for the purpose of privacy risk identification and mitigation. A failure to so carries the risk that it will not maintain the confidence of the public, potentially circumscribing the utility of the identifier.