Australian Government

Office of the Australian Information Commissioner

Data Availability and Use

Submission to Productivity Commission Issues Paper

August 2016

Mr Timothy Pilgrim PSM
Australian Privacy Commissioner
Acting Australian Information Commissioner

Contents

Introduction: Privacy is integral to a successful data-driven economy

As the Australian Privacy Commissioner and Acting Australian Information Commissioner (Commissioner), I welcome the opportunity to comment on the Productivity Commission's *Issues Paper for the Inquiry into Data Availability and Use* (Issues Paper).

Today's economy is underpinned by the flow of information, including personal information. In the digital age, more information is being collected than ever before, and advances in technology are allowing organisations to use and analyse these new sources of data in innovative ways, often to great social and economic benefit. However, if the full potential of data is to be realised in a sustainable way, privacy must be integral to the equation. Simply put, a successful data-driven economy needs a strong foundation in privacy. 'Getting privacy right' will help to engender public trust and build a social licence for organisations to engage in new data-related activities. It will also help to ensure that if personal information is mishandled, appropriate accountability mechanisms are in place and have been well-integrated by industry.

Building trust and confidence by getting privacy right

The experience of my Office and community research shows that people are displaying an increasing level of privacy awareness, particularly in light of the increased availability and use of online services. For example, in a 2013 survey conducted by my Office,[1] 82% of survey participants were aware of the existence of federal privacy laws - a significant increase from only 69% of people in the 2007 survey. Further, 60% of Australians had decided not to deal with an organisation due to concerns about how their personal information will be used. Almost universally, individuals consider transparency to be extremely important in the handling of their personal information, with 97% of participants unhappy about their personal information being used for a secondary purpose.[2] Secondary uses are, of course, critical to data innovation and maximising the value of research and data-analytic activities.

However, when there is transparency in the way personal information is handled, it gives individuals choice and confidence that their privacy rights will be respected. Most people expect Australian government agencies and private sector organisations to use their information where it is necessary to provide them with the services they want, or to improve on those services. However, people also want to know how their information is being used, who has access to it, and what impact this will have on their lives. When

[1] See the *Community Attitudes to Privacy* survey, a longitudinal survey into community attitudes to privacy run by the OAIC, with the most recent survey conducted in 2013. For more information about the OAIC Community Attitudes to Privacy survey 2013, see the *Launch of Community Attitudes to Privacy* report, available on the OAIC's website at: https://www.oaic.gov.au/engage-with-us/community-attitudes/launch-of-community-attitudes-to-privacy-report.

[2] A secondary purpose is any purpose other than the purpose for which the information was originally provided.

people have confidence about how their information is managed, and understand the purposes it will be used for, they are more likely to support those uses of information.

Accordingly, privacy law - often misunderstood to be about secrecy - is underpinned by transparency and accountability. This can pose challenges in the research and big data analytic contexts, as organisations can sometimes have a lack of clarity about the purposes for which information collected for one purpose, may be subsequently used - because the relevance or usefulness of a specific data set may not be known until after analysis has been performed. While this can pose challenges, for example in terms of formulating appropriate notifications and obtaining consent, these challenges can be overcome effectively when privacy is embedded into the design of a project from the very beginning.

Australia's existing privacy framework is flexible and appropriate for the new technology age

Privacy is often named as one of the primary barriers that prevents the sharing or accessing of personal information from and between government agencies – that is not correct. As identified in the Issues Paper, one of the main impediments to information sharing is rather a general reluctance to disclose personal information, due to a number of misunderstandings about obligations under privacy and other laws. Rather than preventing the sharing of personal information, privacy law places important limitations around the circumstances under which it can be collected, used and disclosed, consistent with the community's expectations.

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. It is my long-held view that the Privacy Act should remain the central framework for regulating the handing of personal information, including information within the financial sector. The Privacy Act is well-adapted to ensuring the protection of individual privacy in an environment of technology-driven innovation, for the following reasons:

- the Privacy Act includes thirteen legally binding Australian Privacy Principles (APPs). This principle-based approach provides entities with the flexibility to tailor their personal information handling practices to their needs and business models, and to the needs of individuals
- the APPs are technology neutral, thereby ensuring that they remain applicable in the face of continually changing and emerging technologies
- the Privacy Act allows regulated entities the opportunity to develop (and voluntarily opt-in to) a binding privacy code. These codes are approved and registered by the Commissioner, and can set out with greater specificity how the APPs should be implemented in relation to a particular sector (or in relation to the use of particular technology)
- the Privacy Act is the privacy oversight instrument with which the public is most familiar, and reflects community expectations of the appropriate level of protection that should be afforded to personal information in Australia

- the APPs promote national consistency of regulation by providing a minimum set of standards that are applicable to both government agencies and the private sector, facilitating information sharing across sectors
- entities regulated by the Privacy Act are familiar with the privacy framework set out in the APPs, and have generally integrated these standards well into their business practices. For this reason, the Privacy Act represents the most efficient and cost-effective approach to the continuing regulation of privacy in Australia.

Approach taken in this submission

In this submission, I will address the matters raised in the Terms of Reference and Issues Paper.

Part A outlines the role of the OAIC, and explains how Australia's approach to privacy regulation fits into the broader international privacy landscape. It goes on to sketch the framework for privacy protection provided in the Privacy Act, as well as the broader Australian context for privacy regulation.

Part B outlines the current availability and use of data under the Privacy Act, the challenges posed by new data activities and technologies, and how these can be overcome. It goes on to consider whether the Privacy Act framework could be enhanced to allow for greater access to information (while still respecting privacy), as well as the importance of incorporating privacy into the new data agenda.

Part C outlines the current framework for the regulation of the credit reporting system, as set out in Part IIIA of the Privacy Act. It goes on to consider the current availability of credit and financial data for broader purposes, the general efficacy of the current arrangements, and whether further reform is needed.

Key messages

1. Australians are increasingly aware of privacy and expect organisations to comply with the standards enshrined in the Privacy Act when handling their personal information. Data-related activities involving personal information should not be governed by different standards without justification and in the absence of a robust public debate.
2. The greater use and availability of data must incorporate good privacy practices if new data activities are to enjoy public support, and therefore be sustainable.
3. The OAIC has responsibility for the regulation of privacy, freedom of information and information policy, and is therefore well placed to assist organisations in balancing access to information with the protection of individual privacy. Having a single regulator with the OAIC's unique perspective for the handling of all types of personal information (including financial information) has allowed for the development of better privacy and information policy, and promotes consistency and efficiencies by avoiding regulatory overlap.

4. Australia's privacy laws are underpinned by Australia's international human rights law obligations, and are based on a set of principles developed by the Organisation for Economic Cooperation and Development (OECD). These principles are considered to be the universal benchmark for information privacy law across OECD nations and increasingly, the Asia Pacific and other regions.
5. Generally speaking, the Privacy Act provides a workable and robust framework to safeguard individuals' information privacy, although I note some personal information is handled by entities that are not covered by the APPs. The Privacy Act framework is flexible and facilitates the use of data for secondary purposes in a number of circumstances, for example where the affected person consents to the use of their data.
6. Existing mechanisms in the Privacy Act, such as the Commissioner's powers to approve and register binding privacy codes and issue public interest determinations, provide additional flexibility and can, where this is in the public interest, accommodate specific information-handling practices which may not otherwise comply with the general requirements in the APPs.
7. If entities can successfully de-identify data sets which contain personal information, the Privacy Act will not apply to activities using that information.
8. There may be scope to broaden the research exceptions in the Privacy Act to allow for greater access to data for non-health related research, where this is in the public interest. Specifically, it may be useful for a legislative review to be undertaken, to:
    - consider whether it is still reasonable to limit the existing research exceptions in the Privacy Act to health and medical research, and
    - to explore other mechanisms to facilitate the availability of data for research whilst maintaining adequate protection for personal information.
9. The FOI Act facilitates a public sector culture in which information is valued, properly managed and shared widely, by providing a right of access to documents held by Commonwealth Australian Government ministers and most agencies.
10. Australian Government agencies involved in the collection, use or disclosure of personal information may wish to review any applicable secrecy or confidentiality provisions, to determine whether these provisions are still relevant to their circumstances.
11. The OAIC is working with the Department of Health to look the operation of s 135AA of the *National Health Act 1953*, including considering whether s 135AA, and the corresponding Guidelines, strike an appropriate balance between the need to protect sensitive health data, and the research and policy benefits which could be yielded by greater access to this data.
12. Data breaches are a significant risk associated with greater access to and use of data. The introduction of a mandatory data breach notification scheme would give individuals confidence that, if affected by a serious data breach, they will be given a chance to protect their interests. It will also signal to entities that the protection of personal information is a priority in the digital age.

13. The Privacy Act is one of the primary existing mechanisms which facilitates individuals' access to their own data, including financial and credit data.
14. Australians consider their personal financial and credit data to be particularly sensitive and in need of protection in the digital age.
15. The Privacy Act provides an appropriate framework for the regulation of use and access to credit information. It allows for the free flow of information while building in appropriate consumer protections.
16. It would be premature to consider further changes to the credit reporting provisions in the Privacy Act, given the current provisions were introduced only in 2014 and work is currently underway to facilitate greater participation in comprehensive credit reporting.

Part A: The OAIC and the regulation of the right to privacy in Australia

About the Office of the Australian Information Commissioner (OAIC)

The Australian Parliament established the OAIC to bring together three functions: freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (FOI Act)), privacy functions (protecting the privacy of individuals under the Privacy Act, and other Acts) and information management functions. Together, in the exercise of these three functions the OAIC has acted in the various roles of regulator, decision maker, adviser, researcher and educator to individuals, businesses and agencies alike.

The integration of these three interrelated functions into one agency has meant the OAIC is well placed to strike the right balance between confidentiality and transparency — between the right to privacy, and the right to access government information, which should be recognised as a key national resource. It has also provided my Office with a unique insight into the key issues canvassed by the Issues Paper, on potential means of improving the availability and use of data.

The OAIC's promotion of greater access to public sector information

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. The OAIC's work in this area provides an opportunity not only to reiterate core FOI and privacy themes, but to connect and unify them in a broader policy setting focussed on responsible information management.

The OAIC's FOI functions include the merit review of FOI decisions, investigating complaints about FOI administration, publishing guidelines on the FOI Act, promoting awareness and understanding of the FOI Act, conducting training, providing advice and assistance, monitoring agency compliance with the FOI Act, and collecting and publishing information and statistics about FOI matters.

Over the last 6 years the OAIC has worked to encourage an 'open access by default' approach to government information and to define standards and principles to shape government information management practices. In particular, the Office has provided guidance and initiated the growing national debate about the importance of developing a national information policy which promotes openness and transparency in the management of public sector information, and the importance of access to information for business in stimulating innovation and economic prosperity.

This work included the development by the OAIC of *Principles on open public sector information*[3], which encourage default open access as the first principle, followed by the need to engage the community.[4] These principles also promoted the discoverability and useability of public sector information, and the development of clear reuse rights, with a view to enhancing the economic and social value of public sector information.[5] With the future funding of the OAIC's privacy and FOI functions now confirmed, my Office will continue to engage with the Department of Prime Minister and Cabinet and other Australian Government agencies and interested stakeholders in this area, and provide advice and guidance based on our experience with balancing these three key functions.

The OAIC's work promoting a balance between access to data and privacy

The OAIC has a wealth of experience in providing advice and guidance to enable agencies and organisations to facilitate access to and innovate with data, while minimising the risks to privacy. For example, in 2016 alone, with data analytics set to expand as a key policy and service development tool, my Office is developing and continuing to update resources in this area. This includes:

- a consultation underway on a draft *Guide to big data in the context of the Australian Privacy Principles*.[6] 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.
- a consultation on a draft *Privacy business resource: Privacy and start-up businesses*.[7] This resource provides the operators of start-up businesses with guidance on managing privacy risks while taking advantage of developments in technology and analytics to use information in new and innovative ways.
- revisiting OAIC guidance on de-identification in coming months.[8] De-identification has the potential to be a privacy enhancing tool that facilitates access to data and data sharing, unlocks the potential of big data, and supports the Internet of Things. To that end, the OAIC will be conducting a series of conversations, through the OAIC's Privacy Professionals Network and other networks, to work with

[3] Available on the OAIC's website at https://www.oaic.gov.au/information-policy/information-policy-resources/principles-on-open-public-sector-information.
[4] Further resources on information policy are available on the OAIC's website at https://www.oaic.gov.au/information-policy/.
[5] The principles were first published in Issues Papers 1 and 2, available on the OAIC's website at: https://www.oaic.gov.au/information-policy/information-policy-issues-papers/.
[6] Available on the OAIC's website at: https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/.
[7] Available at www.oaic.gov.au/engage-with-us/consultations/privacy-and-start-up-businesses/.
[8] The current OAIC guidance *Information policy agency resource 1: De-identification of data and information* is available on the OAIC's website at: https://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resource-1-de-identification-of-data-and-information. The OAIC's *Privacy business resource 4: De-identification of data and information* is available at: https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information.

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 common misconceptions that prevent effective information sharing and provide a framework for considering whether information should be shared under the Privacy Act.

The OAIC has also been monitoring, and engaging with industry on, privacy issues related to the Internet of Things (IoT). For example, my Office is participating in the IoT Alliance, including in work streams on 'open data and privacy' and 'security'. Given that IoT increases the interconnections between systems and raises a number of new privacy issues, my Office has emphasised the need for good privacy management and a privacy-by-design approach to IoT systems and technology.

Freedom of information - Government information is a national resource

Government information has social and economic value and should be recognised as an asset to be used for public purposes. This principle is enshrined in the objects clause of the FOI Act.[9] The FOI Act offers direction and legislative weight to information policy endeavours centred on promoting a public sector culture in which information is valued, properly managed and shared widely.

The FOI Act provides a right of access to documents held by Australian Government ministers and most agencies through a written request procedure. This is a necessary legislative right and is appropriate for certain types of document requests, and to resolve disputes about information access.

Changes to the FOI Act in 2010 placed greater emphasis on proactive disclosure, through the Information Publication Scheme, FOI disclosure logs and discretionary release by agencies. Proactive release can be effective in making information publicly accessible through the web to a wider audience. Information released at the right time can facilitate public participation in policy development and implementation at a formative stage.

As outlined in the previous section, my Office has strongly advocated proactive release through its open government messages, guidance material on web publication and accessibility, seminars that bring government and the community together, and liaison with other government agencies that promote the same philosophy.

Despite the range of exemptions available in the FOI Act, these are not intended to restrict the circumstances in which government information can be released. Section 3A(2) states that it is not the intention of the Parliament in enacting the FOI Act to limit the power of agencies to publish information or give access to documents, or to prevent or discourage agencies from doing so. This means that an agency may disclose a

[9] See s 3(3) FOI Act.

document to which an exemption applies where there are no other restrictions outside the FOI Act that would apply to that release.

Overview of the OAIC's regulation of privacy

As Commissioner, I have a wide range of regulatory responsibilities in the privacy space. As outlined below, these extend well beyond the Privacy Act. Having a single regulator, which is responsible for regulating privacy matters across a broad range of sectors, has allowed the OAIC to consider the numerous policy spaces and contexts in which privacy matters are relevant. It has also allowed my Office to develop clear, consistent and useful guidance, which helps regulated entities to understand their obligations and reduce their regulatory burden.

The international basis for regulating the right to privacy in Australia

Privacy is a fundamental human right recognised in the UN *Declaration of Human Rights*, and in many other international and regional treaties. In Australia, the right to privacy is protected by a number of different regulatory schemes. The Commonwealth scheme applies to the handling of information by both the Commonwealth government and the private sector, while the various State and Territory schemes generally apply to the handling of information by agencies of those governments only.

In the Commonwealth jurisdiction, the key piece of legislation regulating the right to privacy is the Privacy Act. The Privacy Act is intended to give effect to Australia's obligations under international agreements[10], specifically:

- its obligations under Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)[11], and
- its agreement to implement the Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) (OECD Guidelines). [12]

The Privacy Act is consistent with these key international privacy agreements, and helps to ensure that Australia is able to meet the international community's expectations of privacy protection so that Australian organisations are not disadvantaged in the international market.

[10] See s 2A(h) of the Privacy Act, which states that the objects of the Privacy Act include 'to implement Australia's international obligation in relation to privacy'.
[11] Opened for signature 16 December 1966 (entered into force 23 March 1976), [1980] ATS 23. The full text of the ICCPR is available on the United Nations High Commissioner for Human Rights website, at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[12] The OECD Guidelines are available on the OECD's website, at: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

Article 17 of the ICCPR – Privacy is a human right

In 1972, Australia became a signatory to the ICCPR, one of the world's most-widely ratified human rights treaties. The ICCPR protects the right to privacy in Article 17:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[13]

While the right to privacy under the ICCPR is not absolute, any instance of interference must be 'necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.'[14]

Other international human rights instruments, as well as laws across many countries at the regional and national level, contain similar provisions. As recently noted by the Office of the High Commissioner for Human Rights, these laws reflect the 'universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.'[15]

OECD Guidelines - a universal information privacy law benchmark

The OECD[16] has played a major role in shaping and defining how privacy is protected around the globe. The OECD Guidelines were adopted by the OECD Council on 23 September 1980. They were designed to discourage the member countries of the OECD from introducing 'incompatible and conflicting laws for the defence of privacy in the newly established databases of the interlinked information technologies'.[17]

In 2013, a review found that the OECD Guidelines had been remarkably influential across the OECD member states, with almost all member states having adopted privacy or data protection legislation based upon its principles, and nearly all having established authorities responsible for the enforcement of these laws.[18] Further, the Guidelines have also influenced the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, thus expanding the reach of the Guidelines outside of the OECD member countries.[19] While there are jurisdiction-to-jurisdiction variations in the way that these

[13] See n 11.
[14] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (UN Doc A/HRC/27/37 (2014), paragraph 23).
[15] Ibid. paragraph 13.
[16] The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union also takes part in the work of the OECD.
[17] M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 25.
[18] See the OECD's *OECD Privacy Framework* (2013), available at*:* http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.
[19] Ibid.

have been implemented, they are considered the universal information privacy law benchmark.

The OECD Guidelines set out eight 'basic principles' for the handling of personal information.[20] Like the Australian Privacy Principles contained in the Privacy Act, the OECD principles are concise, technologically neutral, and written using commonly understood language, and were developed with the aim of 'reconciling fundamental but competing values such as privacy and the free flow of information'.[21]

The Privacy Act

Coverage of the Australian Privacy Act

The APPs in the Privacy Act 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').[1] APP entities can include individuals (including sole traders), body corporates, partnerships, unincorporated associations and trusts. I note that, except for a few explicit exceptions, the standards enshrined in the APPs apply equally to all APP entities, regardless of their entity 'type'.[22]

Part IIIA of the Privacy Act (which contains the 'credit reporting provisions', which are addressed in further detail in Part C) applies only to 'credit providers' and 'credit reporting bodies', whether or not they are also APP entities. Part IIIA applies to these entities only in relation to the exchange of 'credit information', which can be exchanged for the purposes of compiling consumer credit reports about individuals, and other related purposes.

The range of entities subject to the Privacy Act has also been expanded by other legislative schemes. This includes the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), which expands the application of the APPs to a business with an annual turnover of less than $3 million if the business is a reporting entity or an authorised agent of a reporting entity, in respect of specified personal information handling activities.[23] An obligation to comply with the Privacy Act is also imposed by the *Telecommunications (Interception and Access) Act 1979* (TIA Act)[24] which

[20] The eight *Basic Principles of National Application* (OECD Privacy Guidelines, Part 2) relate to Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability. See the *OECD Privacy Framework* (2013), above n 18.
[21] See the OECD's *Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data* (23 September 1980), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation.
[22] Some APPs impose slightly different obligations depending on whether the APP entity is a government 'agency' or a private sector 'organisation'. For example, APP 12 permits organisations (but not agencies) to charge a (non-excessive) fee for access to personal information.
[23] This includes information-handling activities under the *Anti-Money Laundering and Counter-Terrorism Financing Rules*.
[24] See s 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth).

requires providers of telecommunications services in Australia (service providers) [25] to comply with the Privacy Act in relation to telecommunications data collected and retained under the data retention scheme.

As set out below, I also have a number of additional regulatory responsibilities under a range of other laws with links to privacy.

Exemptions

Some Commonwealth agencies are completely exempt from the Privacy Act, including intelligence agencies, the Australian Crime Commission, the Integrity Commissioner and royal commissions. Other agencies are only partially exempt, including certain courts and tribunals (in respect of non-administrative matters) and Ministers. For some exempt agencies, other oversight mechanisms may apply to the handling of personal information.[26]

Most State or territory government agencies are exempt from the Privacy Act. Some private sector entities are also exempted from the obligations in the APPs. This includes most small businesses with an annual turnover of $3 million or less, registered political parties and media organisations (where the media organisation is publicly committed to observing published privacy standards). These organisations may, nevertheless, handle sensitive personal information.

Some categories of personal information are also exempt from the Privacy Act. For example, personal information will not be covered by the APPs if it directly relates to a current or former employment relationship between the organisation that employs the individual, and is held in an employee record.

As Commissioner, consistent with international standards, I support exemptions which are justified on sound policy grounds, and are reasonable, proportionate and necessary in order to meeting those grounds. However, I note that some exemptions to the Privacy Act were introduced a number of years ago, and the environment in which personal information is handled has since evolved. For instance, when the existing exemptions contained in the Privacy Act were enacted, small businesses were exempted on the basis that did not have significant holdings of personal information, and those that did have customer records did not sell or otherwise deal with customer information in a systematic way that posed a high risk to their customer's privacy.[27] In today's increasingly data driven economy, there are a number of economic sectors in which some small businesses have significant holdings of personal information and use this personal

[25] Sections 306 and 306A, which contain the record-keeping requirements in the *Telecommunications Act 1997* (Cth), apply to 'eligible persons'. An 'eligible person' includes a carrier, carriage service provider and their respective employees, and also applies to their associates, as defined by the *Telecommunications (Interception and Access) Act 1979* (Cth).

[26] See for example, the Attorney-General's Guidelines, which set out the Attorney-General's expectations of ASIO in its collection and handling of personal information. These are available on ASIO's website, at: https://www.asio.gov.au/.

[27] Revised *Explanatory Memorandum, Privacy Amendment (Private Sector) Bill* 2000 (Cth), 6, and Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General), 22370–22371.

information, which in some circumstances is often sensitive information, in their business activities, such as online dating, or mobile app developers. It may be timely to re-examine the application of the small business exemption in this context.

Background to current provisions of the Privacy Act – 2014 reforms

The Issues Paper flagged the significant amendments to the Privacy Act which came into force on 12 March 2014, including the implementation of the APPs. These reforms were introduced following the comprehensive review by the Australian Law Reform Commission (ALRC) into Australia's privacy laws which identified significant fragmentation and inconsistency in the regulatory framework, including inconsistency between privacy requirements applying to the public and private sectors.[28] The reforms also included amendments to the Part IIIA credit reporting provisions, and new regulatory powers for the OAIC.

As noted by the Issues Paper, the APPs maintained the Privacy Act's principle-based approach to privacy regulation, and did not introduce any technology-specific obligations. The reforms intended to keep this flexible approach, to allow them to remain applicable to a rapidly changing technological environment without the need for constant amendment.

The Australian Privacy Principles

A key objective of the Privacy Act - as for the OECD Guidelines - is to facilitate the free flow of information across national borders, whilst ensuring that the privacy of individuals is respected.[29] The objectives of the Privacy Act also include promoting the protection of the privacy of individuals and balancing this protection with the interests of entities in carrying out their activities. These objects reflect that the Privacy Act does not treat the protection of individuals' privacy as an absolute right. Rather, those interests must be balanced with other legitimate rights and interests.

The APPs in the Privacy Act are ultimately derived from the privacy principles in the OECD Guidelines. The APPs are the cornerstone of the privacy protection framework in the Privacy Act.[30] The APPs set out standards, rights and obligations in relation to the handling, holding, accessing and correcting of personal information. 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'.

The APPs are principles-based law. This provides regulated entities with the flexibility to tailor their personal information-handling practices to their diverse needs and business models, and to the diverse needs of individuals.[31] The APPs are also technology neutral, applying equally to paper-based and digital environments. This is intended to preserve

[28] ALRC, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) (For Your Information Report), available at: http://www.alrc.gov.au/publications/report-108.
[29] Sections 2A(a) and 2A(d) of the Privacy Act.
[30] See p 52 of the Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, available for download at: https://www.legislation.gov.au/Details/C2012B00077/Download.
[31] Ibid.

their relevance and applicability, in a context of continually changing and emerging technologies.

Personal information

The APPs apply to the handling of personal information (including sensitive information). Personal information, as defined in the Privacy Act, is 'information or an opinion about an identified individual, or an individual who is reasonably identifiable

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not.'[32]

Personal information in the FOI Act is defined as having the same meaning as in the Privacy Act, and consequently many stakeholders in both the public and private sector are familiar with this definition. The Issues Paper talks about both 'personal information' and 'personal data', and sets out a definition of 'personal data' very similar to 'personal information' in the Privacy Act. To avoid confusion, I would encourage the Productivity Commission to adopt the definition of personal information set out in the Privacy Act.

The types of data that may constitute personal information can vary widely. Common examples are an individual's name, signature, address, telephone number and date of birth. Personal information of one individual may also be the personal information of another individual. For example, a marriage certificate that contains personal information about both parties to a marriage. Some types of information may also be brought under the coverage of the Privacy Act by other legislation. For example, telecommunications data held under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (sometimes called retained data or metadata) is deemed to be personal information for the purposes of the Privacy Act.[33]'Sensitive information' is a subset of personal information, and is afforded a higher level of protection under the APPs. This is because sensitive information poses greater concerns for privacy protection. Sensitive information includes information about a person's political opinions, religious beliefs, sexual orientation and health information.[34]

Recently, the United Kingdom, Information Commissioner Elizabeth Denham wrote '…it isn't always possible to draw the definitive personal/non-personal data distinction that legal certainty in the field of data protection depends on'.[35] I agree with this proposition.

Whether data is personal information or sensitive information depends on the context and circumstances in which the data appears. This flexibility allows entities to assess risks realistically and in relation to the particular facts and circumstances they are managing.

---

[32] Section 6(1) of the Privacy Act.
[33] See s 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth).
[34] See the APP guidelines for a full definition of 'sensitive information', available on the OAIC's website at: https://oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#sensitive-information.
[35] Foreword to *The Anonymisation Decision-Making Framework* (2016), M Elliot, E Mackey, K O'Hara and C Tudor (The UK Anonymisation Network), available at: http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf.

For example, some data may not be personal information when considered on its own. However, when combined with other data or information it may become personal information.

The definition of personal information will be a live issue in proceedings before the full bench of the Australian Federal Court on 23 August 2016. These proceedings follow the determination by the Privacy Commissioner in the matter of *Ben Grubb v Telstra Corporation Limited* [2015] AICmr 35, which was appealed to the Administrative Appeals Tribunal. The Privacy Commissioner filed a Notice of Appeal to the Federal Court in January 2016. The Federal Court is due to hear the appeal in August this year, and its decision may be crucial for determining what constitutes personal information under the Privacy Act.

'Ownership' of personal information is not relevant under the Privacy Act

As the Issues Paper notes, the concept of ownership of data in general and personal information in particular can be complex.[36]

The OECD has looked at this issue, questioning whether the concept of ownership maps well to people and organisations that have a relationship with that data, given that data typically involves complex assignments of different rights across different stakeholders, requiring of some stakeholders "the ability to access, create, modify, package, derive benefits from, sell or remove data, but also the right to assign these privileges to others".[37] The OECD notes that the situation is even more complex in the case of personal data, where certain (non-proprietary) rights of the data subject cannot be waived.

Similarly, data ownership is not a concept in the Privacy Act framework, and questions of data ownership are not applicable to determining the obligations which will apply under the Privacy Act. The APPs create obligations for APP entities that collect or hold personal information, regardless of whether that entity is the owner of the personal information. Each APP entity that "holds" the information is required to comply with the APPs, and each individual to whom the personal information relates has rights in respect of that information.[38]

Credit reporting provisions

As outlined above, the Privacy Act also contains credit reporting provisions, which regulate the handling and maintenance of certain kinds of personal information concerning consumer credit.[39] That is, credit that is intended to be used wholly (or primarily) for domestic, family or household purposes. For example, the provisions in Part IIIA of the Privacy Act outline:

[36] See the Productivity Commission's *Data Availability and Use – Issues paper* (Issues Paper), p 6.
[37] See p 195 of the OECD's *Data driven innovation: Big data for growth and well-being* (2015), OECD Publishing, Paris, available at: http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm.
[38] An APP entity 'holds' personal information if 'the entity has possession or control of a record that contains the personal information' (s 6(1) of the Privacy Act).
[39] See Part IIIA of the Privacy Act, and the *Privacy (Credit Reporting) Code 2014 Version 1.2*.

- the types of personal information that credit providers can disclose to a credit reporting body, for the purpose of that information being included in an individual's credit report
- what entities can handle that information, and
- the purposes for which that information may be handled.

The credit reporting system aims to balance an individual's interest in protecting their personal information, with the need to ensure that credit providers have access to enough information to assist them in determining whether an individual should be given credit (and for related purposes). Further consideration of the credit reporting provisions is contained in Part C of this submission.

The OAIC's regulatory approach

Essential to an effective regulatory regime is an independent regulator with powers to monitor and investigate non-compliance, and encourage best practice privacy practices. Independent oversight to protect individuals' interests is particularly important where individuals have limited control over their personal information.

Regulatory powers

The Privacy Act provides an accessible mechanism for individuals to complain to the OAIC and a range of regulatory powers that allow the Commissioner to resolve those disputes. This allows my Office to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred. These powers include:

- issuing guidelines for the avoidance of acts or practices that might interfere with privacy
- directing agencies to give the Commissioner a privacy impact assessment for proposed activities or functions that might have a significant impact on the privacy of individuals
- registering and, where necessary developing, APP and credit reporting codes of practice
- making determinations, by way of legislative instrument (a 'public interest determination'), that a particular act or practice of an APP entity which may otherwise constitute a breach of an APP or registered Code shall not be regarded as a breach
- conducting an assessment (audit) of privacy compliance for both an agency and a private sector entity
- accepting an enforceable undertaking and bringing proceedings to enforce an undertaking
- making a determination in both a complaint investigation and a 'Commissioner initiated investigation' (CII)

- seeking a civil penalty from the courts in the case of a serious or repeated interference with privacy, or in the case of a breach of certain credit reporting provisions.

While I have a range of regulatory action powers to draw on, my preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches. When resolving matters and complaints brought to the OAIC's attention, my Office will take into account the steps taken by an entity to comply with its privacy obligations.

In addition to the regulatory action powers and the collaborative approach to regulation outlined above, the OAIC has extensive experience in complaint conciliation, meaning it provides a method for fast, informal and low-cost resolution of disputes.

In addition to the OAIC's own complaint-conciliation work, from 2014, the Privacy Act has also required all credit providers that participate in the credit reporting system to be a member of an external dispute resolution (EDR) scheme recognised by the Information Commissioner. The inclusion of recognised EDR schemes in the OAIC's regulatory model is a relatively new development that offers the potential to further contribute to a dispute resolution model, and the OAIC is committed to working collaboratively with EDR schemes to ensure consistency in the application of the Privacy Act. The OAIC is observing the existing EDR framework to evaluate its effectiveness as part of the privacy regulatory framework.

The *Privacy regulatory action policy* [40] explains the OAIC's approach to using its privacy regulatory powers and communicating information publicly. A more detailed explanation of each privacy regulatory power is given in the *Guide to privacy regulatory action*.[41]

Regulatory responsibilities under other legislation

As Commissioner, I also have regulatory responsibilities under a range of other laws with links to privacy. These include:

- *Telecommunications Act 1997*. This has a number of provisions that deal with personal information held by carriers, carriage service providers and others.
- *Telecommunications (Interception and Access) Act 1979*. This prohibits the interception of communications passing over a telecommunications system.
- The *National Health Act 1953* and legally binding privacy guidelines issued under this Act. These regulate the handling of Medicare and pharmaceutical benefits information.
- The *Data-matching Program (Assistance and Tax) Act 1990* and legally binding guidelines issued under that Act. These regulate the use of tax file numbers in matching personal information held by the Australian Taxation Office and

[40] Available on the OAIC's website at: www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.
[41] Available at: www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/.

assistance agencies such as the Department of Human Services and the Department of Veterans' Affairs.

- Part VIIC of the *Crimes Act 1914*. This relates to criminal records covered by the Commonwealth Spent Convictions Scheme, which provides protection for individuals with old minor convictions in certain circumstances.
- The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. This imposes a number of obligations on the financial sector, gambling sector, bullion dealers and other professionals or businesses that provide particular 'designated services'.
- The *Healthcare Identifiers Act 2010*. This establishes the Healthcare Identifiers Service and prescribes how healthcare identifiers will be assigned and how they can be used and disclosed.
- The *My Health Records Act 2012* and the rules and regulations issued under that Act. These create the legislative framework for the Australian Government's My Health Record system.
- The *Personal Property Securities Act 2009*. This established a single, national, online Personal Property Securities Register. This Register allows lenders and businesses to register their security interests over personal property. Registrations on the Register may include personal information about individuals.
- The *Student Identifiers Act 2014*. This establishes a national online record of student's vocational education and training attainments and qualifications, as part of the Unique Student Identifier scheme which commenced on 1 January 2015.

Data matching responsibilities

Another area of my regulatory responsibility relates to data matching activities. Agencies that carry out data matching must comply with the Privacy Act when doing so. In addition, data matching between certain agencies to detect incorrect payments using Tax File Numbers (TFNs) is also subject to the requirements of the *Data-matching Program (Assistance and Tax) Act 1990* (the Data Matching Act).

The Data Matching Act regulates the use of TFNs to compare personal information held by the Australian Taxation Office and by certain 'assistance agencies' including the Department of Human Services (which administers the Centrelink, Child Support Agency and Medicare programs) and the Department of Veterans' Affairs. I have issued separate mandatory guidelines in respect of the data matching programs authorised by the Data Matching Act.

I have also issued *Guidelines on Data Matching in Australian Government Administration*. These voluntary guidelines apply to data matching activities where TFNs are not used.

I recognise the benefits of government data matching, which include protecting the public revenue by identifying instances of welfare or tax fraud and deterring non-compliance through ongoing monitoring and education activities. However, data matching does impact personal privacy because it can involve analysing information

about large numbers of people without prior cause for suspicion, and may result in the generation of new personal information.

Enhanced welfare payment integrity initiative

The OAIC has received additional funding to provide oversight of the 'enhanced welfare payment integrity' data matching program. The program applies a simplified and more dynamic data matching process to detect and action discrepancies in welfare payments and income. The OAIC has been working with Department of Human Services (DHS) to design an effective privacy oversight regime that will provide assurance to DHS and the public that privacy risks are being addressed.

Engagement with relevant agencies as part of our regulatory activities

We also actively develop and nurture our partnerships with government agencies domestically. These partnerships allow us to educate and improve our stakeholders' understanding of Australian privacy and information access laws, which helps these agencies achieve efficiencies. It also provides us with opportunities to gather best practice and receive advice and guidance from other agencies.

International Partnerships

The Privacy Act operates in an environment where organisations and governments carry on their businesses globally, and where personal information is regularly transferred, handled and stored overseas. My Office therefore works towards a co-ordinated approach, internationally, to privacy regulation.[42]

The OAIC participates actively in international privacy and data protection forums. This enables my Office to build collaborative relationships with other privacy regulators, and to aim for consistency and interoperability in regulatory guidance and approach (where appropriate). It also helps us to keep abreast of emerging international privacy protection issues.[43] For example, with the majority of European nations soon to be governed by the European Union's (EU's) *General Data Protection Regulation,* the OAIC will be working with EU privacy authorities to encourage simultaneous compliance with EU and Australian privacy laws wherever possible. The OAIC also works with other jurisdictions which have implemented the OECD Guidelines, considered to be the universal information privacy law benchmark.

[42] For example, my Office worked together with the Canadian Office of the Privacy Commissioner to investigate the 2015 Ashley Madison data breach incident. See the OAIC's website for further information.

[43] For example, the OAIC has previously provided secretariat services to the Asia Pacific Privacy Authorities (APPA) Forum, that includes members from the United States, Mexico, Hong Kong, South Korea, Canada, New Zealand and Singapore. The OAIC's responsibilities included hosting and administering two websites (both of which include privacy education materials), secretariat functions and the facilitation of a range of working groups. The OAIC has also led the APPA Communications Working Group for the last four years, developing education products for use across 17 jurisdictions in the Asia Pacific Region. These products include an identity theft tool, a survey on social media and video and privacy tips for using mobile apps.

The OAIC also participates in a number of other formal and informal global forums and arrangements, as outlined briefly below, that aim to build a coordinated approach to regulating cross border data flows and challenges, including the Global Privacy Enforcement Network, under the auspices of the OECD, the Asia-Pacific Economic Cooperation Cross Border Privacy Enforcement Arrangement, and the International Conference of Information Commissioners. These networks allow us to work closely with and learn from our freedom of information, data protection and privacy counter parts.

Asia Pacific Privacy Authorities

The Asia Pacific Privacy Authorities (APPA) brings together privacy and data protection authorities from across our region. APPA currently includes 19 members, including the privacy regulator for the United States, New Zealand, Hong Kong and other countries from the Asia Pacific region. Members meet bi-annually and work cooperatively throughout the year. The OAIC will be hosting the next APPA Forum in Sydney in 2017.

International Conference of Data Protection & Privacy Commissioners

The International Conference of Data Protection & Privacy Commissioners (ICDPPC) is the largest and oldest network for data protection and privacy administrators. The network brings together 113 organisations from around the world. Members meet annually to discuss the latest trends and the current privacy and data protection environment. My Office attends this meeting regularly and contributes to papers and discussions.

Global Privacy Enforcement Network

The OAIC is a member of the Global Privacy Enforcement Network (GPEN) which is open to all data protection and privacy authorities with currently 63 authorities, including economic unions, state and federal authorities.

GPEN does not hold any official in-person meetings. However, members regularly share news and information through GPEN's website and forum. GPEN also hosts monthly teleconference meetings, where members, stakeholders, academics and others share information on a variety of matters including best practice investigative techniques, communication and awareness raising approaches, the latest privacy research and findings and more.

The GPEN network provides a secure means of exchanging information between privacy regulators on issues of common concern.

Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation (APEC) administers a number of working groups on privacy, data transfers and digital interactions. We do not currently participate in APEC's working groups. However, we make contributions to issues and monitor them regularly and assess the impacts on our operating landscape. We also regularly review opportunities to co-sponsor APEC projects and research.

Common Thread Network

The Common Thread Network (CTN) is a relatively new network focused on bringing together and linking data protection and privacy authorities from across the Commonwealth. The CTN aims to promote cross-border co-operation between members and to build strong capabilities for effective data protection across Commonwealth countries.

The CTN currently includes 11 members. Members meet regularly via teleconference and in person annually on the fringe of the International Conference. My Office is currently working closely with members to develop and establish the CTN website.

International Conference of Information Commissioners

The International Conference of Information Commissioners brings together a number of Commissioners or organisations from around the world. Members meet every few years to discuss the latest trends and the current environment in relation to transparency and freedom of information, including the role of the media, open data and open government. My Office has previously attended this meeting and contributed to papers and discussions.

Privacy in a federal system - State and Territory privacy laws

In Australia's federal system, the laws of one government (including the Commonwealth government) generally do not bind other governments. The Privacy Act therefore does not generally apply to State and territory government agencies.[44]

Instead, where they exist, State and Territory laws create information privacy requirements which are similar to those under the Privacy Act (the exceptions are Western Australia and South Australia). As noted in the Issues Paper, State and Territory laws generally apply to State and Territory government agencies. They also can apply to local councils, State and Territory government-owned corporations and public universities.[45] 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, I do not have regulatory responsibilities in relation to these laws.[46]

[44] However, s 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 that it will be treated as an organisation under the Privacy Act. There are also some other exceptions – for example, State and Territory entities may be bound in relation to their handling of Tax File Numbers under the *Privacy (Tax File Number) Rule 2015.*

[45] *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). More information about State and Territory privacy laws is available on the OAIC website, at: https://oaic.gov.au/privacy-law/other-privacy-jurisdictions.

[46] 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. More information on the

As the Issues Paper identifies, some specific types of information are also subject to Commonwealth or State and Territory legislation, including for instance health information in NSW, which is subject to the *Health Records and Information Privacy Act* 2002 (NSW) the *National Health Act* 1953 (Cth) as well as the Commonwealth Privacy Act.

As well as Commonwealth and State and Territory privacy specific obligations, personal information may also be subject to additional regulation including agency specific legislation, such as statutory secrecy provisions.

Regulatory overlap of personal information in Australia

When personal information is subject to more than one regulatory scheme, compliance can become more complex. For example, some private health service providers may have obligations under both the Commonwealth Privacy Act and the relevant State and Territory privacy legislation. Regulatory overlap can potentially inhibit to 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.

I consider it particularly important for my Office to work together with other 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 to align and harmonise our approach and policy advice, where appropriate.

The importance of a nationally consistent privacy law

In my view, an important aspect of a strong and effective privacy framework is national consistency, and I therefore support efforts to harmonise privacy laws across the various Australian jurisdictions. Regulation should apply to all sectors equally, establishing uniform standards and avoiding gaps or overlap in coverage. Inconsistency and fragmentation in privacy regulation may cause a number of problems, including unjustified compliance burden and cost, impediments to information sharing and national initiatives, and confusion about who to approach to make a privacy complaint. National consistency, therefore, should be one of the goals of privacy regulation.[47]

The OAIC's broad coverage of privacy regulation is helpful in this respect. Consistency of regulation is facilitated by the principle-based nature of the APPs. As the APPs are technologically neutral and generally non- prescriptive, they provide entities with the flexibility to tailor their personal information handling practices to their diverse needs and business models.

OAIC's role is available on the OAIC website at: https://www.oaic.gov.au/privacy/privacy-act/australian-capital-territory-privacy.

[47] See 3.13 of the ALRC's For Your Information Report, above n 28.

Domestic Partnerships

In order to facilitate greater harmonisation of privacy laws in Australia's federal system, we actively develop and nurture our partnerships with government agencies domestically. These partnerships provide us with opportunities to gather best practice and receive advice and guidance from other agencies.

Privacy Authorities Australia

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. Members meet once a year and also cooperate regularly on a variety of matters. At a recent meeting, the groups discussed topics including national consistency in health privacy regulation, interoperability, the development of health privacy guidance, and privacy issues relating to new technologies that are relevant to State, Territory and Commonwealth privacy regulators.

Association of Access Commissioners'

This is a national network for organisations who administer freedom of information legislation. Members meet in person annually to examine a range of matters including the legislative and operating environment, new and merging areas of interest and research and best practice approaches.

Part B: The availability and use of personal information under the Privacy Act

Personal information can be an extremely valuable resource, and seeking to improve the access to (and effective use of) personal information can bring significant gains to individuals, businesses and government agencies.

Generally speaking, the APPs provide a framework for the sharing of personal information in a manner that safeguards individuals' privacy, although I note that some personal information is handled by entities that are not covered by the APPs.

To help explain the mandatory requirements in the APPs, and set out the OAIC's interpretation of the APPs, the OAIC has issued non-binding APP Guidelines.[48] These include information on the factors that may be taken into account when exercising functions and powers relating to the APPs, and explain that the Privacy Act - rather than preventing access/use of personal information - places important limitations around the circumstances under which it can be collected, used and disclosed.

Under the APPs, purpose limitation, transparency, notice and consent offer key privacy protections that facilitate individual choice and control, supplemented by a range of other complementary measures that protect individuals' privacy. However, as outlined earlier in this submission, the Privacy Act and the APPs recognise 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 other legitimate rights and interests. 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 – for example, a number of law enforcement related exceptions - operate to allow APP entities to use or disclose information in a way which would otherwise breach the APPs, where this is deemed to be in the public interest.

This Part of the submission will address some of the specific questions raised by the Terms of Reference and Issues Paper, including the extent to which individuals can access their personal information (from the perspective of the OAIC's areas of regulatory responsibility), the right to deletion, the current restrictions which may be seen to exist regarding the use of personal information, and areas of privacy regulation which could be enhanced or improved for the purposes of data use (in a privacy-friendly way). At the beginning of this section, however, I would like to examine how personal information must be handled under the APPs, and consent, transparency and notice key means by which the APPs protect privacy. I would also like to draw the Commission's attention to some complementary privacy-enhancing tools which can help to facilitate greater access to and use of data.

[48] Available on the OAIC website, at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/preface.

Notice, transparency and consent – the keystones of information-handling under the APPs

The APPs are structured around the central principle that personal information collected for one purpose should generally not be used or disclosed for a secondary purpose, unless an exception applies.

APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. APP 3 contains additional requirements 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.

APP 6 applies to the use or disclosure of personal information. Under APP 6, an APP entity can only use or disclose personal information for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure (APP 6.1(a)) or 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)).

The Issues Paper explores the challenges associated with the consent model in light of significant technological developments, including the increasing proportion of data that is observed.[49] In my view, consent, notice and transparency remain an appropriate foundation for protecting privacy under Australian law, complemented with other measures that protect individuals' privacy.

A requirement to obtain consent is not an APP in itself. It is relevant, however, to the operation of some APPs, including the collection of sensitive information (APP 3) and use and disclosure (APP 6), as set out above, and also direct marketing (APP 7) and cross-border disclosure of personal information (APP 8). In certain instances, consent can provide legal authority for an APP entity to deal with an individual's personal information in a particular way. A challenge is to ensure that any consent obtained is meaningful, and gives the individual the choice and control these provisions are intended to provide.

In each case 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, under which an entity may collect sensitive information and use and disclose personal information. In this way the Privacy Act recognises that consent and the individual autonomy it protects do not override all other interests, and reflects the balance between privacy and other public interest objectives inherent in the Privacy Act.

Obtaining an individual's consent before collecting sensitive information and handling personal information is a key privacy protection in the Privacy Act. It is adapted to the

[49] See p 24 of the Productivity Commission's Issues Paper.

contextual nature of privacy, balancing individual privacy self-management with organisational accountability.

In addition to supporting the exercise of meaningful consent, the discrete transparency and notice requirements in APPs 1 and 5 underpin the exercise of individual choice and control and enhance the accountability of APP entities. APPs 1.3 – 1.6 require an APP entity to have a clearly expressed, up-to-date and freely available APP Privacy Policy about how the entity manages personal information. 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).

Supplementing consent and notice

While purpose limitation, transparency, notice and consent offer key privacy protections that facilitate individual choice and control, the Privacy Act includes a range of other complementary measures that protect individuals' privacy while facilitating greater use of and access to data. Some of the measures my Office is currently focused on include fostering a culture of good privacy governance and facilitating an agreed understanding about the role of de-identification. These measures are outlined below.

Good privacy governance - privacy by design

Whether personal information can be used for a secondary purpose has often proved to be a significant question for APP entities. As outlined in the introduction to this submission, secondary uses of data are often critical to innovative success in the data space. In some cases, it is not always possible to identify the additional purposes for which information will be useful, prior to the data being analysed.

However, these challenges can be addressed. In order to optimise the value of data which includes personal information, an entity can take steps to minimise risks to an individual's privacy while still maximising the range of permissible uses of the data. This approach is called 'privacy by design', and is intended to build privacy into systems and projects from the design stage onwards.[50] The OAIC's *Privacy Management Framework*, which is annexed to this submission, can assist agencies to implement a 'privacy by design' approach to information handling arrangements.[51]

[50] '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.

[51] The Privacy Management Framework is also available at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework. I also note that once the European Union's *General Data Protection Regulation* (GDPR) enters into force in May 2018, all entities (including Australian entities) which provide certain services to the EU will need to implement the use of (EU-specific) data protection policies such as a 'data protection by design and by default' program in place (see Articles 24 and 25 of the GDPR), with respect to the provision of those services.

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. For instance, entities should consider whether the secondary use is permitted under one of the exceptions set out in APP 6.

- *what personal information can be collected*

  Entities collecting personal information are required to consider the purpose of the collection (APP 3).

- *how it should be collected, including whether any consents should be sought at the time of collection*

  As set out above, an entity can use or disclose personal information for a secondary purpose if the individual has consented to the use or disclosure (APP 6.1(a)). Seeking consent at the time of collection is particularly important as seeking consent at a later time 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 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 under the exception set out in APP 6 .2(a).

I appreciate that prior to the collection of personal information, an entity may not be able to predict with certainty the full range of purposes that it might be desirable to use that information for in the future. However, by considering the matters raised above at the outset of a project, the APP entity will place itself in the best possible position to maximise the use of the data it holds, while still respecting the privacy of the affected individuals.

De-identification

Another mechanism which can improve the ability of APP entities to maximise the use of data in a privacy-friendly way is through de-identification. De-identification is a key mechanism to facilitate data sharing and use. It involves removing or altering information that identifies an individual, or is reasonably likely to do so. Data that has been successfully de-identified is not personal information and the Privacy Act will not apply to its handling.[52] This means entities can maximise the utility and value of the data while safeguarding privacy.

[52] Note: Credit reporting bodies must also comply with s 20M of the Privacy Act, which prevents the use and disclosure of de-identified credit reporting information except when that use or disclosure is for the purpose of conducting research in accordance with the *Privacy (Credit Related Research) Rule 2014*, available at: https://www.comlaw.gov.au/Details/F2014L00503.

De-identification may not altogether remove the risk that an individual may be re-identified – nor does the Privacy Act require this. Rather, the Privacy Act defines 'de-identified information' as 'information [that] is no longer about an identifiable individual or an individual who is *reasonably* identifiable'.[53]

It is important to remember that de-identification is not an exact science - it is heavily context dependent and requires a flexible, risk-based approach. As the UK Information Commissioner Elizabeth Denham wrote recently:

> 'It is easy to say that anonymization is impossible and that re-identification can always take place… It is more difficult to evaluate risk realistically… and to strike a publicly acceptable balance between access to information and personal privacy'.[54]

To successfully de-identify data, the environment in which data will be handled must be considered in full, to determine what de-identification techniques are necessary and/or appropriate. Where de-identification is done properly and with proper consideration of the specific context the activities will take place in, the risk of re-identification should be low. Its potential as a tool for enhancing the ability of entities to engage in a range of valuable big data activities is therefore very significant.

The OAIC's guidance on de-identification

the Privacy Act defines 'de-identified' as 'information [that] is no longer about an identifiable individual or an individual who is *reasonably* identifiable'.[55] The Privacy Act also refers to de-identification in the context of APP 11, which states that information must be de-identified (or destroyed) if is no longer needed for any purpose for which it may be used or disclosed (APP 11.2).

The OAIC published guidance about de-identification in 2014.[56] The guidance notes that de-identifying data:

- is required in specified circumstances
- facilitates the use of data for research purposes
- lessens the risk that personal information will be compromised should a data breach occur.

The OAIC's de-identification guidance provides principle-based policy information about when de-identification may be appropriate, how to choose appropriate de-identification techniques and how to assess the risk that data may be re-identified. The guidance also

[53] Section 6(1) of the Privacy Act.
[54] See page vi (the Preface by Elizabeth Denham, UK Information Commissioner) of the *Anonymisation Decision-Making Framework*, above n 35.
[55] Section 6(1) of the Privacy Act.
[56] Available at: https://oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information.

refers readers to technical guidance, the National Statistical Services' Confidentiality Information Series.

My Office is revisiting its de-identification guidance in 2016 to provide further policy guidance:

- about using a risk management approach
- to reflect developments in de-identification techniques
- to expand the discussion of re-identification, including how to deal with data that is re-identified, and
- to clarify the terminology used.

We see a need to clarify the terminology used in its guidance because different terminology is used at the international and domestic level. At the international level, privacy and data protection laws use the terms de-identification, confidentialisation and anonymisation in similar ways, but with legislative and technical differences. At the domestic level, there is a difference in the terminology used by privacy professionals and data analysts, and between specific agencies.

Revisiting the de-identification guidance will provide the OAIC with the opportunity to consider how best to advise on this tool.

Optimising information sharing for research: the research exceptions in the Privacy Act

I appreciate that emerging data innovation practices may require fresh consideration about how key existing privacy principles - including notice and consent, data collection, use limitation, and retention minimisation - work in practice. As I have expressed above, in my view, as principles-based law, the Privacy Act is, in most cases, flexible enough to support programs to improve the availability and use of data, provided that an integrated approach to privacy management is taken up front. However, I consider that 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.

The framework for information sharing for research under the Privacy Act

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. The framework includes the *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).

The *Guidelines approved under Section 95A of the Privacy Act 1988* (s 95A Guidelines) apply to private sector organisations, and deal with the disclosure of health information

that is necessary for the secondary purpose of research relevant to public health or public safety.

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. However, these bodies may have obligations under State legislation.

ALRC recommendations regarding the research exceptions

Certain aspects of the current framework of the Privacy Act in facilitating research were questioned by the Australian Law Reform Commission (ALRC) in the *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)* (For Your Information Report),[57] 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.

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.[58]

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 Commissioner issues one set of rules under the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle to replace the current Guidelines.[59]

Potential review of the research exceptions in the Privacy Act

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.

Questions around the secondary use and disclosure of personal information have often proven to be problematic, particularly where an entity is unclear about whether or not a collection, use or disclosure for a secondary purpose would fall within an exception to the APPs. This uncertainty may contribute to a reluctance to make information available,

[57] See above n 28.
[58] Ibid, Recommendation 65-2.
[59] Ibid, Recommendation 65-1.

even where this would be permissible under the framework. A review of the framework for research under the Privacy Act would therefore enable other mechanisms to be explored, alleviating this uncertainty, and could thus improve the availability of data for research.

However, any enhancement of the framework for research under the Privacy Act would need to balance the potential benefits to the community against the potential to adversely impact on individuals' privacy interests. 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 evaluated as part of a review 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. It will also be important to consider accountability, oversight and assurance procedures.

Individuals' access to their personal information

The Inquiry seeks to understand to what extent individuals are currently able to access and maximise the potential of their personal data.

In Australia, individuals have rights to access and amend their personal information under the Privacy Act, for both private and government sectors and also the FOI Act for accessing personal information held by government. In many respects, the FOI Act provides a similar access mechanism to the Privacy Act for individuals. However, some key differences are that there are wider grounds for refusal to grant access under the FOI Act.

As Commissioner I have found that both mechanisms are well-used.[60]

While the existence of two schemes may sometimes result in some complexity for individuals seeking to access their personal information - for example, where a government agency may require an individual to apply for access under the FOI framework (instead of the Privacy Act framework) - the OAIC continues to work with

[60] An entity's failure to provide access to personal information is one of the more frequently complained about APPs. By way of illustration, last financial year the OAIC received approximately 300 privacy complaints relating to access to personal information, with most of these relating to personal information held by the private sector.

agencies to promote consistency in responding to requests for access and amendment of personal information.

Data access and portability is increasingly important in the information economy. The issue of data access is receiving attention internationally, with the EU taking steps to provide individuals with an express right of data portability. Article 20 of the EU's *General Data Protection Regulation* (GDPR) is due to come into effect in 2018, and is intended to provide individuals with easier access to their data as and to give them the right to have their data transferred from one automated processing system to, and into, another system.[61]

The framework for accessing information under the Privacy Act

Individuals have rights under the Privacy Act to request access to their personal information. Under APP 12, an APP entity that holds personal information about an individual must, on request, give that individual access to the information (subject to limited exceptions). APP 12 sets out the minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

APP 12 operates alongside, and does not replace, other informal or legal procedures by which an individual can be given access to information. As noted in the Issues Paper, in addition to rights to access personal information under APP 12 the FOI Act also provides a right of access to information (including personal information) in documents held by Australian Government ministers and most agencies.

Access to credit information

The Privacy Act also sets out specific access requirements for credit information. The provisions around access are a key consumer safeguard in the credit reporting provisions. Individuals can access their credit report from a credit reporting body for free, once per year, as well as in the following circumstances:

- if they have been refused credit within the past 90 days, or
- If a credit reporting body or credit provider has made a decision on a correction request from the person.

The credit reporting body must grant access within 10 days. Individuals are also entitled to access their personal and other information (including credit information) held by a credit provider. Credit providers may charge a fee for giving access to this information, but this cannot be excessive. Credit providers must respond to access requests within a reasonable time (usually within 30 days).

[61] See *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

I note that I have addressed issues related to credit and financial information more broadly in Part C below.

Access to information under the Freedom of Information Act

The FOI Act provides a right of access to documents held by Australian Government ministers and most agencies. Most freedom of information (FOI) requests involve people seeking access to documents containing their personal information. Individuals can also request access to documents containing other information, such as information about government policies, programs and decision-making processes.

The FOI Act also allows individuals to ask a minister or government agency to amend or annotate a personal record they hold about them, on grounds that the personal record is out of date, misleading, incorrect or inaccurate. Individuals can request amendment or annotation of any record of information about them that an agency or minister has used, is using or could use for an administrative purpose.

Enhancing individuals' access to personal information

Streamlining the regulatory framework for accessing personal information from government agencies

The Privacy Act and FOI Act provide some points of difference in relation to procedures, criteria and review mechanisms. While the OAIC continues to work with agencies to promote consistency in responding to requests for access and amendment of personal information, at times, the current regulatory framework can create complexity for individuals seeking to access their personal information from government agencies. To simplify the current regulatory scheme, consideration could be given to whether the Privacy Act should be the primary avenue for individuals to access and amend their own personal information. I would recommend that if that suggestion was to be adopted, some right of access to personal information should be retained under the FOI Act.

Optimising the manner in which information is provided to consumers

The Issues Paper expresses a concern that the Privacy Act does not specify the format the information is to be provided to consumers, other than it "must be in a manner requested by the individual", and notes that this was identified by the Murray Report[62] as an impediment to consumers being able to access their data.[63]

Chapter 12 of the *APP Guidelines* provides guidance about how access is to be given under APP 12.[64] However, as the APPs apply across all Australian industries, that guidance is by necessity general in nature.

[62] See p 184 of The Financial System Inquiry Committee's *Financial System Inquiry Final Report* ('Murray Inquiry Report') (7 December 2014), available at: http://fsi.gov.au/.
[63] See p 19 of the Productivity Commission's Issues Paper.
[64] Available at https://oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-12-app-12-access-to-personal-information#_Toc380671641.

Importantly, APP 12 only sets out the *minimum* access requirements. It is open to entities to adopt processes and procedures that go beyond the minimum requirements of APP 12, to make it easier for individuals to access their personal information in their preferred format. This would be something that the OAIC both encourages and supports. The OAIC encourages entities to endeavour to provide access in a manner that is as prompt, uncomplicated and inexpensive as possible.

There are mechanisms in the Privacy Act that allow for entities to develop binding obligations that apply in addition to those in the APPs. Under the Privacy Act, an APP entity (or a body or association representing them) can develop a written code of practice for the handling of personal information, called an APP code. An APP code sets out how one or more of the APPs are to be applied or complied with, and the APP entities that are bound by the code. 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 can provide individuals with additional transparency about how their information will be handled and greater certainty to entities about how to meet their obligations. Accordingly, APP entities operating within a given industry or sector may wish to consider developing an APP code setting out further details of how individuals are to be provided with access to their personal information under APP 12. For more information about APP codes, see the OAIC's *Guidelines for developing codes*.[65]

Addressing gaps in community knowledge

Community education may have an important role to play in enhancing individuals' awareness of their rights to access their personal information. For example, in relation to credit information more specifically, it was found that only 17% of respondents to the OAIC's Community Attitudes Survey had accessed their credit report from a credit reporting body in the past (as they are entitled to do, see above). While nearly half (48%) of participants were aware that they *could* access their credit report if they wanted to, most (74%) were not aware that this information could be accessed for free.[66] This is also reflected in the figures published by Veda, Australia's largest credit reporting body, in its *Credit Reporting Annual Report*. This Report suggested that while there were around 258,000 requests for free access to credit reports in the 2014/15 financial year, there were also around 252,000 requests for paid access (although I note that individuals may elect to pay for access, because this may provide them with a faster service, or additional information or benefits).[67]

I am also aware that a number of private organisations may offer individuals a paid service to access their credit report, credit information and/or other financial information. While individuals may choose to use these services where they see a benefit in doing so, again, my Office has been working actively to ensure that individuals are aware of their ability to access their reports for free. In particular, the OAIC encourages

[65] Available at https://oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/guidelines-for-developing-codes.
[66] See the OAIC's 2013 *Launch of Community Attitudes to Privacy* report, above n 1.
[67] See Veda's *Credit Reporting Annual Report 2014/2015*, available on the Veda website at: https://www.veda.com.au/credit-reporting-privacy-code-annual-report.

individuals to access and check their credit report regularly, and to ensure that they request correction of any information they consider to be inaccurate.[68]

I am therefore aware that there remains a gap in community knowledge in this regard, and my Office continues to work proactively to ensure that individuals are aware of their ability to access their credit report for free.

The use of third party intermediaries to optimise the utility of data

I note the concern expressed by the Murray Report and set out in the Issues Paper that in many cases consumers are unable to authorise trusted third parties to access their personal information directly from their service provider. I wish to address the misconception that the Privacy Act restricts consumers from entering into this type of arrangement.

The Privacy Act does not prevent an individual from authorising a third party to access their personal information on their behalf, other than the limited situation where certain entities are excluded from accessing credit reporting information on behalf of an individual.[69] Instead, the requirements imposed by the Privacy Act include that where a request for access to personal information under APP 12 is not made by the individual to whom the personal information relates, an APP entity must satisfy itself that the request is made by a person who is authorised to make the request on their behalf, such as a legal guardian or authorised agent.[70]

Similarly, the FOI Act does not prevent an individual from authorising a third party to access their personal information from a government agency on their behalf.

Facilitating new markets for personal information services

The Issues Paper canvasses the potential benefits of improving access to information by facilitating new markets for personal information services. Where sufficient privacy and security safeguards are in place, there may be value in enabling consumers to access data about themselves, and enabling consumers to use third party intermediaries to optimise the utility of that data. The Midata program in the UK, referenced in the Issues Paper, shows the potential opportunities presented by these types of arrangements.[71]

Broadly speaking, I am supportive of initiatives that empower individuals to use the information that entities hold about them for their own benefit. However, I am mindful that such services may involve the handling of large amounts of personal information and therefore carry significant privacy risks. For example, the sharing of energy consumption

[68] See, for example, the OAIC's *Privacy fact sheet 31: How you can access your credit report*, available at: https://www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/privacy-fact-sheet-31-how-you-can-access-your-credit-report.
[69] See s 20R(2) and 21T(2) of the Privacy Act, and the definition of access seeker in s 6L of the Privacy Act.
[70] Further information about appropriate steps that may be taken to verify an individual's identity is set out in available in Chapter 12 of the APP Guidelines, available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-12-app-12-access-to-personal-information#verifying-an-individuals-identity.
[71] See p 20 of the Productivity Commission's Issues Paper.

data that includes personal information, like the sharing of any data set, may carry privacy risks. However, those privacy risks may increase significantly if this personal information is ultimately combined with data from other sources, such as banking transaction data.

The merging of such data will create a much more detailed, richer picture of the consumer, inherently increasing the risk of harm to the affected person should the information be accessed or handled improperly (as the data will reveal more information about the person – as it is intended to). While this may beneficial for the individual (as well as a number of organisations, and potentially governments), caution should therefore be exercised when opening up access to personal information, particularly where there are few or inadequate safeguards in place to ensure that consumers retain control over the use of their personal information. Safeguards should also be in place to ensure that the data will be used fairly, and that the data will not be used in a way that erodes consumer trust and confidence.

The framework for providing access should also ensure that consumers are adequately protected from the risk of fraud, unauthorised access or theft. With that in mind, I welcome the emphasis that the Issues Paper places on the need to consider privacy risks and appropriate privacy protections. I suggest that entities seeking to establish these types of schemes consider whether it may be appropriate to develop an APP Code (see above), or to look at other regulation in this area, which could apply to any potential access scheme.

Deletion of personal information under the Privacy Act

As the Issues Paper identifies, the issue of whether individuals should be able to request deletion of data about themselves is gaining prominence as personal information is increasingly able to be shared with a wider audience and is more readily searchable.[72]

Generally speaking, APP entities must take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs (APP 11.2). However, if personal information is contained in a Commonwealth record, the agency is not required to destroy or de-identify the personal information, even if it is no longer needed. The agency will instead be required to comply with the provisions of the Archives Act in relation to those Commonwealth records. Likewise, an APP entity that is required to retain personal information by an Australian law or a court/tribunal order is not required to destroy or de-identify the personal information (APP 11.2(d)).

A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the *Archives Act 1983*. The grounds on which this may be done

[72] Issues Paper, p 24.

include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with a 'normal administrative practice'.[73]

However, under the Australian Privacy Act individuals have no general right to deletion of information held about them. This problem has been acknowledged by privacy regulators globally, including the European Union (EU) Council and Parliament, which has introduced a right to erasure in Article 17 of the GDPR. Article 17(1) will enable an individual to require data controllers to delete their data on a number of grounds, including if the information is no longer necessary for the purpose for which it was collected, or if an individual withdraws their consent and there is no other legal ground for processing their data. There will be exceptions to this right such as:

- where processing of the data is necessary for exercising the right of freedom of expression and information
- for compliance with a legal obligation
- for reasons of public interest in the area of public health
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- for the establishment, exercise or defence of legal claims.

Article 17(2) of the GDPR deals with content that has been made public, and will oblige data controllers to take measure to inform third parties who process the relevant data about the request.

In principle, I support the right of an individual to request the deletion of information about themselves. The existing measures in the APPs balance the need to give an individual control over the handling of their personal information with the obligation on entities to consider the ongoing retention of personal information. An APP entity should have practices, procedures and systems in place to identify personal information that needs to be destroyed or de-identified (APP 1.2). Where there is no lawful purpose or requirement for an entity to retain an individual's personal information, the individual could lodge a complaint with the OAIC where the organisation fails to destroy or de-identify the information.

Whether Australia should introduce legislation to address serious invasions of privacy

In its consideration of a right to deletion, the Issues Paper noted that an Australian Senate Committee has proposed laws criminalising the non-consensual sharing of intimate information about an individual.[74] I am generally supportive of laws aimed at achieving resolution of serious invasions of privacy. However, my view is that this issue

[73] See Chapter B (Key concepts) of the APP Guidelines for more information about Commonwealth records, available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information#key-points.
[74] See p 26 of the Productivity Commission's Issues paper.

would require greater consideration of issues that relate more closely to the rights and responsibilities of individuals than the current inquiry, which seeks to address some of the broader questions surrounding the greater use of and access to data.

I note that in addition to the ALRC's *Serious invasions of privacy in the digital era* report (ALRC Report 123), the New South Wales Government has also considered further regulation in this area.[75] The OAIC made submissions to each of these enquires.[76]

Restrictions around the release of particular data

While the Privacy Act provides an overarching framework for how personal information should be handled, as the Issues Paper has noted, additional legal obligations apply to some types of data that 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[77] can complement the framework provided by the Privacy Act. Secrecy provisions serve an important role in circumstances 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.

The Issues Paper has asked for suggestions for further measures which might facilitate the disclosure and use of data about individuals while protecting privacy interests.

Potential review of s 135AA of the National Health Act

To facilitate disclosure, the OAIC and the Department of Health are working together to look at the operation of s 135AA of the *National Health Act 1953* (National Health Act). Section 135AA of the National Health Act regulates the handling of government-held Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data by Australian government agencies. Under s 135AA, the Australian Information Commissioner is required to issue the legally-binding *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* (the Guidelines).

[75] See the (NSW) Standing Committee on Law Justice, 'Remedies for the serious invasion of privacy in New South Wales' (3 March 2016, available on the NSW Parliament's website). See also the South Australian Law Reform Institute, 'Invasion of personal privacy' report (March 2016), available on the University of Adelaide Law School's website at: https://law.adelaide.edu.au/research/law-reform-institute/.

[76] Submission to the Attorney-General's Department on Issues Paper, 'A Commonwealth statutory cause of action for serious invasion of privacy', November 2011; Submission to the ALRC on Issues Paper 43, 'Serious Invasions of Privacy in the Digital Era', December 2013; Submission to the ALRC on Discussion Paper 80 'Serious invasions of privacy in the digital era' May 2014. These submissions are available on the OAIC website at: https://oaic.gov.au/engage-with-us/submissions/.

[77] 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 *Secrecy Laws and Open Government in Australia (ALRC Report 112)* (2010), available at: http://www.alrc.gov.au/publications/report-112.

I am aware that some consider s 135AA, and by extension the Guidelines, to be too restrictive and to not allow the disclosure and linkage of MBS and PBS data in ways that are needed for research and policy analysis activities. A recent report of the Senate Select Committee on Health - *Big health data: Australia's big potential*, noted the difficulties associated with accessing MBS and PBS data, and particularly when trying to link it with other data sets.[78] Legislative constraints on the use of MBS and PBS data were also specifically identified as an issue for consideration in the Department of Prime Minister and Cabinet's *Public Sector Data Management Report*.[79] Given these matters, together with the evolution of policy and research needs since these legislative provisions were originally enacted, further consideration of the operation of s 135AA and the Guidelines may be warranted.

My Office and the Department of Health are committed to working together to consider this further with the aim of improving access to de-identified MBS and PBS data, for the purpose of health policy evaluation and development (as well as research undertaken in the public interest).

Potential review of secrecy and confidentiality provisions found in other legislation

More generally, I note the recommendation of the ALRC in their 2010 report, *Secrecy Laws and Open Government in Australia* - that to enable effective information handling, agencies need to develop and implement policies to clarify the application of relevant secrecy laws to their information holdings.[80]

I encourage agencies 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 according to secrecy laws, an information-handling policy can alleviate some of the barriers to information sharing identified in the Issues Paper.[81] Implementing good information handling practices and governance arrangements not only helps to ensure compliance with the APPs but can also help to develop more efficient business processes.[82]

Agencies may also wish to consider reviewing their relevant secrecy and confidentiality provisions, to determine whether they are still needed.

[78] Senate Select Committee on Health, *Big health data: Australia's big potential* (May 2016), Recommendation 4, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Health/Health/Sixth_Interim_Report.
[79] Department of the Prime Minister and Cabinet, *Public Sector Data Management Report* (July 2015), available at: https://www.dpmc.gov.au/resource-centre/public-data/public-sector-data-management-report.
[80] See Recommendation 14-1 of the *Secrecy Laws and Open Government in Australia Report,* above n 77.
[81] See p 27 of the Productivity Commission's Issues Paper.
[82] APP 1.2 requires APP entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs. For more information, see the OAIC's Privacy Management Framework, which is annexed to this submission, also available at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework.

Data security obligations

The Issues Paper asks a number of questions about the obligations of Australian entities with respect to data security.

This Inquiry seeks to raise awareness about the inherent value of data, and will make recommendations that seek to enable Australian entities to maximise the value of data, and the economic opportunities that it presents in the digital age. With this in mind, I note that data security measures must be recognised as being central to the building of a successful, data-driven economy. Where valuable and/or sensitive data is not protected from unauthorised access, use or disclosure, its value and community trust may be severely undermined.

A number of data security obligations apply in the Australian context, including the requirement in APP 11, the operation of which is outlined below.

Security obligations under the APPs

APP 11 requires APP entities to take reasonable steps to ensure they manage personal information securely. It also requires APP entities to take reasonable steps to destroy or de-identify any personal information that they no longer need, unless an exception applies. The approach taken under APP 11, as for the other APPs, is a flexible and principles-based approach which can be adapted to the circumstances of a particular business or industry.

My Office has produced a *Guide to securing personal information* (the Guide), which was developed to help entities understand and implement their APP 11 obligations. The Guide explains how entities can decide what 'reasonable steps' they should take to protect personal information. The Guide explains that this will depend on the entity's circumstances, such as:

- the nature of the entity
- the amount and sensitivity of the personal information held
- the possible adverse consequences for an individual in the case of a breach
- the practical implications of implementing the security measure, including the time and cost involved, and
- whether a security measure is itself privacy invasive.

What is reasonable in the circumstances may also vary between entities, and may change over time, for example as a result of technological change, or if the entity becomes aware that existing security measures are no longer adequate to protect the personal information they hold.

Interaction of APP 11 with other data security measures

As APP 11 is principles-based and not prescriptive, regulated entities are able to integrate these obligations in the context of their obligations under any other relevant Australian

or international standards, policies, frameworks or other information security guidance. APP 11 does not replace or override any existing government or industry policies regarding information security. Indeed, compliance with them can be part of taking reasonable steps under APP 11.

By way of illustration, certain Australian Government Agencies must comply with the Attorney-General's Department's *Protective Security Policy Framework* (PSPF) and the Australian Signals Directorate's Australian Government *Information Security Manual* (ISM) in addition to APP 11. While APP 11 applies to all APP entities whether they are part of the private or public sectors, the PSPF and ISM are only binding in respect of government agencies (though they may also be influential in the private sector).

There are a number of differences between APP 11 and the PSPF and ISM. APP 11 is concerned with the security of personal information only, whereas the PSPF and ISM apply to any type of information (including personal, security classified and/or commercially confidential information) that is not intended to be made publicly available. However, given the flexibility of APP 11, agencies are able to design their information handling-policies to comply with a number of different sets of obligations. The OAIC's Guide recognises that both public and private sector entities need to be aware of any relevant government, industry or technology specific standards, guidance, frameworks or obligations, and to incorporate these into their information security practices as part of taking reasonable steps under APP 11 to protect personal information.

Data breach notification

Data breaches are a significant risk associated with doing business in the information age. The preparation and implementation of a data breach policy and response plan (that includes notifying affected individuals, and the OAIC) helps entities deal with this risk, and respond to a breach, as well as mitigating the potential privacy impacts of a breach for individuals.

While Australia does not yet have a system of mandatory data breach reporting, other than in relation to specific digital health laws,[83] my Office has developed some voluntary guides to assist agencies and businesses to respond effectively to data breaches: the *Data breach notification – A Guide to handling personal information security breaches*,[84] And the *Guide to developing a data breach response plan*.[85] The guides are aimed, in part, at encouraging entities to voluntarily put in place reasonable measures to deal with data breaches (including notification of affected individuals and the OAIC). However, despite a recent increase in the level of data breaches reported to my Office, there have been a number of high profile data breaches that were not reported to me, and which were

[83] Section 75 of the *My Health Records Act 2012* requires certain participants in the My Health Records system to notify the OAIC of a data breach, and includes a civil penalty for failing to do so.
[84] Available on the OAIC's website at: https://oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.
[85] See the OAIC's Guide to developing a data breach response plan, available on the OAIC's website at: https://www.oaic.gov.au/engage-with-us/consultations/guide-to-developing-a-data-breach-response-plan/.

instead brought to the OAIC's attention through complaints made directly to my Office or through media reports.

My Office continues to see evidence of a high number of serious data breaches. McAfee Labs Threat Report for August 2015, which reviewed changes in cyber threats and cybersecurity from 2010 to 2015, states that there has been a 'monumental increase in the number of major data breaches and in the volume of records stolen'.

My own Office has seen a significant increase in the number of entities voluntarily reporting breaches over the past two years, with 107 voluntary reports received in the 2015-16 financial year and 116 in 2014-15, compared with only 69 in 2013-14 (and 61 in 2012-13). The number of mandatory reports (relating to certain digital health information) has also increased, with 16 received last financial year (compared with 7 in 2014-15, and only 2 in 2013-14).

Benefits of notifying affected individuals about a data breach

Without mandatory reporting of serious data breaches, some entities may not notify individuals that could be affected, or my Office. I therefore believe that a mandatory notification scheme is necessary to:

- give confidence to all Australians that if they are affected by serious data breach, they will be given a chance to protect their interests, and
- signal to entities that protection of individuals' personal information should be a priority in the digital age.

When individuals are told about a serious data breach in relation to their personal information, they are able to take steps to minimise the impact of the breach, such as:

- cancelling credit cards
- changing online passwords, and
- monitoring their credit reports.

Where an entity notifies the OAIC about a serious data breach, my Office can in turn:

- give the entity guidance on responding to the data breach
- assist the entity to determine whether the breach has been contained
- meaningfully respond to community enquiries about the breach, and
- explain to individuals steps they may take to protect their personal information.

In the experience of my Office, when an entity notifies affected individuals about a breach, and signals that they are taking appropriate action, this can have a positive effect in terms of maintaining consumer trust, and can greatly assist with preventing or mitigating reputational damage. In this regard, notification of a data breach can be a very prudent business decision.

Mandatory data breach notification scheme

In late 2015 the Australian Government released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* for public consultation. In my submission to the Attorney-General's Department I expressed my continuing support for the introduction of a mandatory data breach reporting scheme for serious data breaches.[86]

The Bill provided for amendments to the Privacy Act, which would require entities which are covered by the Privacy Act (whether as APP entities, credit providers/credit reporting bodies, or otherwise) to notify my Office and affected individuals in the case of a serious data breach involving personal, credit, or tax file number information.[87] Entities not covered by the Privacy Act will not have notification obligations under the Bill.

The consultation version of the Bill would allow entities that have experienced a breach a period of up to 30 days in which to undertake a reasonable assessment of whether the data breach is serious or not, and therefore whether they must notify the OAIC and affected individuals. As Commissioner, I would also have the power to require an entity to notify individuals of a serious breach in certain situations.

Under the Bill, a data breach is defined as being serious and notifiable only when affected individuals face a 'real risk of serious harm' (see s 26WB (2) of the Bill). I support this limitation on the obligation to notify (only in situations where a breach is considered to be *serious*), as this will prevent notification fatigue and minimise the burden on regulated entities, while still ensuring that individuals are informed of breaches when this is appropriate.

I remain committed to providing support to government, business and the community if the Bill is enacted. If the Bill (or a similar Bill) is enacted, my Office will likely play an important role in the implementation of the Bill such as through the provision of guidance and other activities.

[86] See the OAIC's *Mandatory data breach notification discussion paper — submission to Attorney-General's Department* (March 2016), available at: https://www.oaic.gov.au/engage-with-us/submissions/mandatory-data-breach-notification-discussion-paper-submission-to-attorney-general-s-department. See also the OAIC's submission to the Senate Legal and Constitutional Affairs Committee, on the *Privacy Amendment (Privacy Alerts) Bill 2013* (June 2013), available at: https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-privacy-amendment-privacy-alerts-bill-2013.

[87] See the exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* released by the Attorney-General's Department (AGD) in late 2015, available at: https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx.

Part C: Credit reporting and financial information

Introduction and overview

Australian banks, financial institutions and other credit providers can collect a wide range of personal information in the course of their business. The APPs apply to the collection of all general categories of personal (including financial and credit-related) information by these entities, as outlined in the other parts of this submission.

By contrast, the credit reporting provisions in the Privacy Act apply only to a subset of the information collected by two types of entities - the information that is collected and exchanged between 'credit providers' and 'credit reporting bodies' for the purposes of compiling and exchanging consumer credit reports. The flow of information between these two types of entities is known as the Australian credit reporting system. This collection of credit data occurs on a vast scale, and is therefore an issue which affects almost all adult Australians. Veda, for example, is Australia's largest credit reporting body and claims to hold credit information on around 20 million individuals (as well as 5.7 million commercial entities) in Australia and New Zealand.[88]

I recognise that increased access to and use of data, including financial data and credit reporting data, may have potential benefits for both the financial sector and consumers. However, where data is also personal information, any increased access and use has the potential to adversely impact on individuals' privacy interests if not accompanied by an appropriate level of privacy safeguards.

Further, there are strong indications that the community considers credit and other financial data to be some of the most sensitive of all data sets, and therefore in need of strong and appropriate privacy protections. In the credit reporting context in particular, an individual's ability to access credit can have a significant impact on many aspects of their life, and it is therefore crucial that the information in the credit reporting system is both as accurate as possible, and used appropriately. I therefore welcome the emphasis that the Issues Paper has placed on the need for the Inquiry to consider the importance of engendering consumer trust, any likely privacy risks associated with proposals for reform, and the appropriate privacy protections that should apply in this space.

In this section, I present my observations on the application of the credit reporting provisions (and more broadly the application of the APPs to financial data) having regard to the matters raised in the Issues Paper and Terms of Reference. In summary, I do not consider that the credit reporting provisions represent a 'barrier' to the sharing of information in this context. Rather, the credit reporting provisions have created an information-sharing framework which allows for the free flow of information between credit providers and credit reporting bodies for specific, defined purposes, and with

[88] See p 58 of Veda Advantage's *2015 Annual Report*, available at: http://investors.veda.com.au/Investor-Relations/?page=Annual-Reports.

appropriate consumer privacy protections. The Privacy Act also permits research to be conducted on de-identified credit information provided that appropriate protections are in place.

I am of the strong view that the Privacy Act should remain the central framework for regulating the handing of personal information – both 'ordinary' personal information and credit reporting information - within the financial sector.[89] The OAIC remains uniquely placed to regulate the consumer credit reporting framework, given its broader privacy functions. The single-regulator model has proven to be an efficient and effective means of ensuring that privacy standards are applied consistently across industries, and in relation to the various categories of personal information in the financial system.

I am also of the view that it would be premature to consider further changes to the credit reporting provisions, given that the amended provisions have been in force for less than three years. Instead, I would suggest that the five-year review of the credit reporting system, due to be conducted in 2019 in consultation with all relevant industry and consumer stakeholders, would be a more appropriate forum in which to consider whether any further changes to the credit reporting system are desirable.

Community perceptions of the credit reporting system

The OAIC, as the national privacy regulator with responsibility for handling privacy complaints, is uniquely placed to gauge and in turn articulate any community concerns about the handling of credit information. On average, credit reporting complaints represent almost a quarter of all complaints received by the OAIC.[90] As outlined in the introduction to this submission, Australians are increasingly aware of privacy issues, including their financial and credit information.

The OAIC's community attitudes surveys confirm this.[91] The most recent survey conducted in 2013 found that a relatively high proportion of those surveyed (17%) had at some point sought access to their credit information. The results indicated that individuals consider their financial data to be the type of data that they are most reluctant to provide to an organisation. Participants also named the risk of ID fraud and theft as one of the biggest privacy risks facing people today, along with threats to data security and financial data in general. A majority (69%) of participants were concerned that they may become a victim of ID fraud or theft in future.

[89] The OAIC also expressed this view in its submissions in response to the Financial System (Murray) Inquiry's Interim and Final Reports. See the OAIC's *Financial System Inquiry: submission responding to the Inquiry's interim report* (August 2014), available at: https://www.oaic.gov.au/engage-with-us/submissions/financial-system-inquiry-submission-responding-to-the-inquiry-s-interim-report; and the OAIC's *Submission on the Financial System Inquiry Final Report* (April 2015), available at: https://www.oaic.gov.au/engage-with-us/submissions/submission-on-the-financial-system-inquiry-final-report.

[90] For example, 429 of the 2123 complaints received by the OAIC during the 2015-16 financial year (and 690 of the 2841 complaints received in the 2014-15 financial year) related to credit reporting.

[91] See the OAIC's 2013 *Launch of Community Attitudes to Privacy* report, above n 1.

The high level of interest in a number of recent media stories relating to ID fraud, alleged data breaches, and suspected unauthorised uses or disclosures of personal and credit information also strongly reinforce my observations in this regard.[92]

The handling of 'ordinary' personal information in the financial system

Australian credit and other financial service providers may collect, use and disclose a wide range of personal information about their clients. For example, banks, financial institutions and other credit providers will often hold information about their clients' employment status, tax file numbers,[93] income, spending habits and even information about their social media activities. This information can be used in a range of ways, including to manage the person's accounts or the provision of services to them, assess their applications for credit, to market goods and services to them, and for a range of other purposes.

The Privacy Act applies to all these general activities, and permits the collection and handling of this information, provided that the entity complies with the APPs. In particular, this includes the requirement that any information handled must be necessary for (or related to) an entity's business functions or activities (APP 3). The requirements of the APPs, and their application to the private sector more generally, is outlined in other parts of this submission.

As outlined above in relation to the broader categories of personal information, I consider that the Privacy Act continues to provide a suitably flexible yet robust framework for the handling of all personal information in the financial system. The Privacy Act is the privacy oversight instrument with which the public is most familiar, and in the view of my Office continues to reflect the Australian community's expectations about the appropriate level of protection that should be afforded to personal information in Australia today, including sensitive financial data which is considered to be in need of particular protection.

Credit reporting provisions

The 'credit reporting provisions' are contained in Part IIIA of the Privacy Act and are complemented by the binding *Privacy (Credit Reporting) Code 2014* (CR Code) and *Privacy Regulation 2013*. In contrast to the APPs, which are of general application, these provisions apply only to credit providers and credit reporting bodies in relation to the exchange of specific types of data, called credit information. This data can be exchanged for the purposes of compiling consumer credit reports about individuals, and other

[92] One often cited example is the data breach which affected the Ashley Madison website. See, e.g., Alex Hern, '*Infidelity site Ashley Madison hacked as attackers demand total shutdown*' (20 July 2015), published on the Guardian newspaper website, available at: https://www.theguardian.com/technology/2015/jul/20/ashley-madison-hacked-cheating-site-total-shutdown.

[93] Note: the handling of TFNs is covered specifically by the *Privacy (Tax File Number) Rule 2015*.

related purposes such as internal management, securitisation, or debt collection purposes.

While the credit reporting provisions are prescriptive (and not principles-based like the APPs), in essence they set out how these same principles are to apply in the credit context.

Credit reporting bodies

Credit reporting bodies are businesses which handle personal information for the purposes of providing information to other entities about individuals' creditworthiness. There are three major credit reporting bodies in Australia – Veda, Dun & Bradstreet, and Experian.

Credit providers

The term 'credit provider' captures a wide range of entities that provide credit, issue credit cards, or otherwise provide goods or services on credit. Goods or services are considered to have been provided on credit where payment is deferred for 7 days or more. The definition therefore encompasses banks, building societies, credit unions, payday lenders and other types of financial institutions/financial service providers, as well as utilities, telecommunication service providers, and toll road and public transport operators.

The credit reporting provisions set out when a credit provider can access a person's credit report. Most commonly, credit providers will seek access to a person's credit report when they have received a credit application, and are considering whether to grant credit to that person. For example, when a person applies for a personal or home loan, credit card, or new home or mobile telephone service account.

Credit information

Only limited, defined and relevant kinds of personal information are permitted to be exchanged between credit providers and credit reporting bodies in the credit reporting system. Once a credit provider gives this information to a credit reporting body, it will stay on the person's credit report for the relevant retention period (six years for most types of information).

The basic type of information that can be exchanged is 'credit information', defined in s 6N of the Privacy Act, which includes the following information:

- the person's name, date of birth, sex, address, employer name and driver's licence number[94]
- the names of the providers who have given credit to the person, and details about that credit (including the type of credit, relevant dates, and the credit limit)[95]

[94] See ss 6N(a) and 6(1) of the Privacy Act.

[95] See ss 6N(b) and 6(1).

- whether the person has made any monthly payments on time[96]
- the providers that have requested access to the person's credit report[97]
- any past credit applications the person has made[98]
- any defaults the person has incurred (any payments of $150 or more that are overdue by 60 days or more)[99]
- whether a person has repaid any of their defaults[100]
- any new financial arrangements the person has entered into as a result of a default (such as a contract variation or new loan)[101]
- any credit-related court judgments made against the person[102]
- whether the person has been found insolvent or bankrupt[103]
- publicly available information about a person's credit-related activities,[104] and
- whether the person has, in the opinion of a credit provider, committed a serious credit infringement. [105]

Importantly, any personal information which relates to an individual's activities in relation to credit (but which is not included in the definition of 'credit information' in the Privacy Act, as defined above) cannot be exchanged between credit providers and credit reporting bodies under Part IIIA and the CR Code. As explained above, however, credit providers can still hold and use this wider range of financial and other information about their customers, provided that this is in compliance with their obligations under the APPs.

Purpose of the 2014 reforms – allowing the free flow of more comprehensive information while protecting sensitive financial data

The current credit reporting provisions were introduced as part of the 2014 reforms to the Privacy Act, with the aim of striking an appropriate balance between the sometimes competing interests of financial sector organisations and individuals. As outlined above, these reforms were heavily informed by the ALRC's For Your Information Report.[106]

[96] See ss 6N(c) and 6V.
[97] See ss 6N(d) and 6R.
[98] See s 6N(e).
[99] See ss 6N(f) and 6Q.
[100] See ss 6N(g) and 6T.
[101] See ss 6N(h) and 6S.
[102] See ss 6N(i) and 6(1).
[103] See ss 6N(k) and 6(1).
[104] See ss 6N(k) and CR Code, para 11.1).
[105] See ss 6N(l) and 6(1).
[106] Above n 28. See from s 52 onwards.

Prior to 2014, only a more limited data set of 'negative' information (primarily default information) was able to be exchanged in the credit reporting system. A major goal of the reforms was therefore to permit the exchange of additional types of 'positive' credit information, such as details about an individual's current credit accounts, and repayment history performance information. Allowing additional types of information to be exchanged in the system was intended to:

- allow credit providers to make a more robust assessment of credit risk, and better meet their responsible lending (ASIC) obligations[107]
- decrease levels of over-indebtedness
- lower credit default rates, and
- improve competition and efficiency in the credit market, resulting in reductions to the cost of credit for individuals.

As the new credit reporting provisions expanded the categories of information to be shared, they also included some additional consumer protections.

Consumer safeguards

One key safeguard of the new system is that credit providers and credit reporting bodies are prohibited from sharing any information that is not specifically prescribed in the credit reporting provisions. Further, credit information obtained through the system cannot be used for any secondary, non-prescribed purposes. For example, a person's credit report cannot be used for the purposes of direct marketing.

Other important consumer safeguards which apply under Part IIIA and the CR Code are the following obligations of credit reporting bodies and credit providers. These entities must 'take reasonable steps' to:

- ensure that the credit information they handle is accurate and up-to-date[108]
- store information securely and protect it from misuse, interference or loss[109]
- provide individuals with access to their credit report on request (see further on this in the access sections in Part B of this submission),[110] and
- correct credit information, on request or otherwise, if it is inaccurate, out-of-date, incomplete, misleading or irrelevant.[111] This will often require the body that receives the correction request to investigate the relevant listing.

These safeguards are crucial in maintaining public confidence that privacy rights will be protected in the context of consumer credit reporting and, moreover, public confidence in the integrity and reliability of the credit reporting system more broadly.

[107] For example, under the *National Consumer Credit Protection Act 2009*, administered by ASIC.
[108] See ss 20N and 21Q of the Privacy Act.
[109] See ss 20Q and 21S.
[110] See ss 20R and 21T.
[111] See ss 20S, 20T, 21U and 21V.

Participation in more comprehensive credit reporting and the Principles of Reciprocity and Data Exchange

While the 2014 reforms to the Privacy Act allowed for the sharing of new types of information in the credit reporting system, it appears industry has not yet responded to the opportunity to contribute these additional types of credit information. Rather, it appears that industry has continued to share only the types of information that were able to be shared prior to the amendments.

I understand that the *Principles of Reciprocity and Data Exchange* (PRDE), developed by the Australian Retail Credit Association (ARCA) and recently granted authorisation for five years by the Australian Competition and Consumer Commission (ACCC),[112] is intended to address the apparently low level of participation in more comprehensive consumer credit reporting. The PRDE is a set of standard-form principles, which will bind signatory credit providers and credit reporting bodies in relation to their handling of credit reporting information, and introduce the principle of reciprocity. The PRDE is intended to give credit providers an incentive to contribute more comprehensive credit reporting information, and will likely lead to signatories sharing more credit information (and with more credit reporting bodies) than they currently do.

Initiatives which incentivise participation in the credit reporting system are likely to have privacy impacts, because of the increased access to and use of personal information. In light of this, I have previously urged participants in the credit reporting system to continue to be mindful of their privacy obligations, and particularly their quality, security, access and correction obligations (as outlined above), should they become signatories to the PRDE. However, some features of the PRDE appear to be privacy-enhancing when compared with a mandatory system (see below). This is because under a tiered-access system, credit providers will only be able to collect and disclose the credit reporting information that they need for their business purposes, rather than access to all the information available about an individual.[113]

Whether participation in the credit reporting system should be mandatory

There has long been discussion about whether participation in the comprehensive credit reporting scheme should be mandatory. It is not for me to comment on the general advantages or disadvantages to the credit reporting market of comprehensive credit reporting generally, or of the PRDE scheme.

However, in my view a mandatory reporting system would increase the privacy risks associated with the system, due to the increased access, use and storage of information,

[112] Granted on 3 December 2015 (Authorisation A91482). See the ACCC's website at: http://registers.accc.gov.au/content/index.phtml/itemId/1184971/fromItemId/278039.

[113] This reflects the view expressed earlier by the OAIC in its submissions in response to the Financial System (Murray) Inquiry's Interim and Final Reports, see above n 89. In those submissions, the OAIC also noted that, at the time, the reforms to the Privacy Act had only recently entered into force and that, therefore, it would have been premature to mandate participation in comprehensive credit reporting.

and as explained above would likely be less privacy-friendly than a tiered-access system such as the PRDE. The introduction of mandatory reporting would also represent a significant policy shift compared with the current arrangements, which have been developed following extensive consultations with all relevant stakeholders.[114] The ALRC found in the *For Your Information* report that while compulsory reporting may be beneficial for some providers, it would also impose a significant burden on smaller credit providers. The ALRC therefore concluded that this was a matter that should be resolved in a consultative manner between credit providers, their industry associations, and other affected stakeholders such as consumer groups and regulators. [115]

In addition, the reforms to the credit reporting provisions, which were considered in depth by the ALRC and the parliament, entered into force less than three years ago. Further, as outlined above, the PRDE - developed by ARCA following extensive consultations with industry – has recently been approved by the ACCC and is in the process of being implemented, which may help to encourage greater participation in more comprehensive credit reporting.

For all of these reasons, in my view it would be premature to contemplate further changes to the credit reporting system at this stage. Instead, the new credit reporting provisions and the PRDE should be given a chance to be fully implemented by industry. The Australian Government has already signalled that these matters will be considered further when the five-year review of the credit reporting laws occurs in 2019.

Allowing individual access to credit information

Access to credit information is dealt with above in Part B, which addresses individuals' access to personal information more broadly.

Current availability and use of credit data for broader purposes

As outlined above, the credit reporting provisions represent a carefully negotiated balance between sometimes competing interests, with the aim of allowing credit data to flow freely in the Australian credit reporting system. While parliament did not consider research to be a primary purpose of the credit reporting system,[116] provision is made to allow the use of credit data for research purposes, where this is in the public interest.

Privacy (Credit Related Research) Rule 2014

The Privacy Act does not generally regulate the use or disclosure of de-identified information, as explained in Part B, once information has been successfully de-identified,

[114] See the OAIC's *Submission on Draft Determination to grant authorisation to the Australian Retail Credit Association's Principles of Reciprocity and Data Exchange (Authorisation A91482)* (August 2015), available at: https://www.oaic.gov.au/engage-with-us/submissions/submission-draft-determination-to-grant-authorisation-to-arca-s-principles-of-reciprocity-and-data-exchange-authorisation-a91482.
[115] See Part 55 of the ALRC's For your Information Report, above n 28.
[116] See p 145 of the Explanatory Memorandum, above n 30.

it no longer meets the definition of personal information. Credit providers, like most other APP entities, are therefore able to use de-identified information for a range of purposes, including research.

However, given the highly sensitive nature of credit-related data, specific arrangements were developed for the use of de-identified credit information by credit reporting bodies. Credit reporting bodies must therefore comply with the *Privacy (Credit Related Research) Rule 2014* (the Research Rule) when conducting research using de-identified credit data. The Research Rule sets out the specific purposes for which research can be conducted:

- the assessment or management of current, and development of new, credit services
- developing methodologies to combat fraud, anti-money laundering, counter terrorism financing and other unlawful activity involving credit
- assisting responsible lending obligations and other consumer protections, or
- any other purpose for the general benefit of the public.[117]

Further, the Rule requires credit reporting bodies to take steps to ensure that credit data is adequately de-identified prior to disclosure for research purposes, and to take steps to ensure that information is not re-identified.

In my view, the Privacy Act therefore makes adequate provision for the sharing of credit information for research and analytics purposes, while building in appropriate safeguards.

The de-identification requirements are an important privacy protection measure, rather than a 'barrier' to use or disclosure - and represent a standard that the community would expect when dealing with sensitive financial data.

Accuracy of data sets

There is a large volume of information held in the credit reporting system, and this is accessed and updated frequently by multiple sources. As mentioned above, Veda, for example, holds credit reports on around 20 million adult Australian and New Zealanders. Inevitably, some of this information is not accurate. This is reflected in complaints received by the OAIC, as well as the corrections requests received and processed by credit providers and credit reporting bodies themselves. Based on statistics provided in its *Credit Reporting Annual Report*, Veda, by way of example, received approximately 40,000[118] correction requests from individuals in Australia and New Zealand in the 2014/15 financial year, with nearly 31% of these corrections requests being 'successful'.[119] Further, the OAIC's community attitudes survey found that of the 17% of

[117] See s 6 of the *Privacy (Credit Related Research) Rule 2014*.
[118] Based on Veda holding a database of records on 20,000,000 individuals, with 0.2% of those individuals making correction requests that financial year. See p 5 of Veda's *Credit Reporting Privacy Code Annual Report 2014/15*, above n 67.
[119] Ibid.

survey participants who had accessed their credit report in the past, around 10% of those had found errors in their credit report which they were able to have corrected.[120]

While there are likely to be quality and accuracy issues with all comparably large data sets, my Office seeks to ensure, through its oversight role and enforcement powers, that credit reporting bodies and credit providers have appropriate systems in place to ensure the compliance with the credit reporting provisions, and through that the quality of their data sets. I consider the Privacy Act and CR Code set out appropriate requirements for regulated entities to comply with, and provides appropriate enforcement mechanisms that help to ensure credit providers and credit reporting bodies are taking the necessary steps to ensure credit information is accurate, up-to-date and complete.

For example, s 20N of the Privacy Act requires credit reporting bodies to take reasonable steps to ensure that the credit information they collect, use and disclose is accurate, up-to-date, complete and relevant. Taking reasonable steps will include (but is not limited to) (1) entering into agreements with credit providers to require those providers to ensure that the information they disclose to the credit reporting body is accurate, and (2) ensuring that regular audits are conducted by an independent person to ensure credit providers are complying with those agreements (and dealing appropriately with any suspected breaches). As a breach of these requirements may constitute a breach of privacy under s 13(2) of the Privacy Act, I can also use my general enforcement powers (see above) to ensure that these statutory requirements are complied with.

I recommend that the Commission takes into account the quality of the data held in the credit reporting system when considering what, if any, recommendations it should make regarding the use of (and access to) credit data. The Commission should also ensure that any envisaged uses are appropriate, having regard to the purposes of the credit reporting system.

Other financial data sets that may be useful

I am not in a position to comment on any other data sources which may potentially be of value in the credit reporting space. However, I would emphasise that under the current arrangements, the information which can be exchanged between credit providers and credit reporting bodies, and the uses to which this information can be put, are limited and exhaustively prescribed. Legislative change would be required to permit other types of information to be exchanged, or used for additional purposes.

I also reiterate that while other, more general types information may be collected by credit providers in the general course of their business, providers still must comply with the APPs when doing so, including in relation to publicly available information.

[120] See the OAIC's 2013 *Launch of Community Attitudes to Privacy* report, above n 1.