Australian Government
Office of the Australian Information Commissioner

Privacy Act Review – Issues Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
11 December 2020

Contents

Abbreviations

Term	Description
AAT	Administrative Appeals Tribunal
ACAPS	Australian Community Attitudes to Privacy Survey
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ADHA	Australian Digital Health Agency
AHRC	Australian Human Rights Commission
AIC Act	*Australian Information Commissioner Act 2010* (Cth)
ALRC	Australian Law Reform Commission
APEC	Asia Pacific Economic Cooperation
APP	Australian Privacy Principles
ASIC	Australian Securities and Investments Commission
CAG	Council of Attorneys-General
CBPR	Cross Border Privacy Rules
CDR	Consumer Data Right
CR	Credit Reporting
DPI	Digital Platforms Inquiry
DVA	Department of Veterans' Affairs
EDPB	European Data Protection Board
EDR	External Dispute Resolution
EM	Explanatory Memorandum
FCA	Federal Circuit Court
FOI	Freedom of Information
FOI Act	*Freedom of Information Act 1982* (Cth)
GDPR	General Data Protection Regulation, European Union
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IoT	Internet of Things
IP	Internet Protocol

ISO	International Standards Organisation
MAC	Media Access Control
MOU	Memorandum of Understanding
NDB	Notifiable Data Breach
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Cooperation and Development
PIA	Privacy Impact Assessment
PIPEDA	*Personal Information Protection and Electronic Documents Act 2000* (Canada)
TFN	Tax File Number
UKAS	United Kingdom Accreditation Service
UK ICO	United Kingdom Information Commissioner's Office

Executive summary

The privacy landscape has changed significantly since the introduction of the *Privacy Act 1988* (Cth) (the Privacy Act) 32 years ago. In the intervening decades, most aspects of the daily lives of Australians have been transformed by innovations in technology and service delivery. This has resulted in a dramatic increase in the amount of data and personal information collected, used, and shared, both in Australia and globally. Alongside this significant shift in data handling practices has come an increase in community expectations that their personal information will be protected.

The Privacy Act is a well-established framework for the protection of fundamental privacy rights and an enabler of innovation that supports economic growth. Being principles-based, it is technologically neutral and flexible. However, given the scale and scope of environmental change, the current review of the Privacy Act is necessary to ensure that this framework is proportionate, sustainable and responsive to emerging privacy risks into the future.

A greater emphasis on the rights of individuals and the obligations of entities to protect those rights is required to ensure the public interest is served by privacy law into the next decade. Australia's privacy framework can also be strengthened by a more central focus on protecting individuals from the harms associated with current and emerging practices around the collection, use and disclosure of their personal information.

The OAIC considers that there are four key elements needed to support effective privacy regulation over the next decade:

- Global interoperability — making sure our laws continue to connect around the world, so our data is protected wherever it flows
- Enabling privacy self-management —so individuals can exercise meaningful choice and control
- Organisational accountability — ensuring there are sufficient obligations built into the system
- A contemporary approach to regulation — having the right tools to regulate in line with community expectations.

Strong data protection and privacy rights are both necessary to uphold our human right to dignity in the digital age, and a precondition for consumer confidence and economic growth. They are also critical to achieving other societal objectives such as the protection of health, safety and security. As well as implementing Australia's international human rights obligations, the Privacy Act was designed to support economic growth.[1] It supports

[1] The Explanatory Memorandum to the 2000 Bill that expanded the scope of the Privacy Act to private organisations noted: 'The Australian public has expressed concern about doing business online, and this concern could frustrate the growth of electronic commerce. The Government acknowledges that user confidence in the way personal information is handled in the online environment will significantly influence consumer choices about whether to use electronic commerce. Any business demonstrating that it will protect the privacy of its customers will therefore gain a competitive advantage. Similarly, a country that can demonstrate it protects its citizens' privacy will have an advantage over those countries that do not.'

Government to deliver better outcomes for Australians that are technology-enabled and citizen-focused, and supports organisations to deliver products and services that can provide both profit and public benefits.

Effective and proportionate privacy regulation is essential to achieving these benefits. When regulated entities have a clear framework that sets out their personal information handling responsibilities, they will be able to operate and innovate with confidence. Equally, when Australians have clear privacy rights and trust that their personal information is protected, they will feel confident to engage in the data-driven economy and to access services.

Government and organisations are increasingly aware of the benefits that good privacy practice brings. The response to the COVID-19 pandemic has demonstrated that privacy is crucial to achieving large-scale public policy initiatives. In developing the COVIDSafe application, the government recognised that strong privacy protections are essential to public confidence in engaging with the technology. For organisations, privacy is becoming a market differentiator.

Australians have consistently indicated that they care deeply about their privacy, but are challenged in a digital age where individuals are increasingly asked to consent to information handling practices that are not clearly explained, and are buried in long, complex terms and conditions.

The OAIC's Australian Community Attitudes to Privacy Survey (ACAPS) 2020 found that 69% of individuals do not read privacy policies attached to any internet site. The key reasons Australians don't read privacy policies attached to internet sites is because of the length (77%) followed by their complexity (52%) .[2]

The Consumer Policy Research Centre's 2020 Data and Technology Consumer Survey found that 69% of consumers who read privacy policies reported accepting terms even though they weren't comfortable with them. The main reason for doing so was it was the only way to access the product or service (75%).[3]

The alternative is to not engage with the product or service at all, which, as Daniel Susser points out, is often not a realistic option:

> … the cost of opting out is often too high. If, for instance, the choice is between accepting a social network's privacy policy and getting to see pictures of one's grandchildren, or rejecting the policy's terms and not getting to see them, many grandparents will not view the latter as an acceptable option.'

[2] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 70

[3] Consumer Policy Research Centre, CPRC 2020 Data and Technology Consumer Survey, Consumer research conducted in partnership with Roy Morgan Research over March and April 2020, https://cprc.org.au/app/uploads/2020/11/CPRC-2020-Data-and-Technology-Consumer-Survey.pdf (accessed 8 December 2020).

These issues are diminishing the Australian community's trust in personal information handling. The OAIC's research shows a steady decline in trust since 2007: trust in companies in general is down by 13% and trust in Federal Government departments is down 14%.

The OAIC's ACAPS 2020 results found that privacy is a major concern for 70% of Australians:

- Australians consider the social media industry the most untrustworthy in how they protect or use their personal information (70% consider this industry untrustworthy), followed by search engines (55% untrustworthy) and apps (54% untrustworthy)
- 40% feel the privacy of their personal information is poorly protected, while 24% feel it is well protected
- 83% of Australians would like the government to do more to protect the privacy of their data
- 84% of Australians believe that personal information should not be used in ways that cause harm, loss or distress.

The OAIC's recommendations in this submission are aimed at addressing these declining levels of trust and responding to the community's desire for more to be done to protect their privacy in the face of new and emerging threats. Restoring trust and confidence in the digital age requires the Privacy Act to be supplemented with protections that create legal obligations aimed at achieving greater fairness and organisational accountability to address privacy risks and harms. The OAIC is proposing amendments to the Privacy Act that:

- Maintain the flexibility and scalability of the existing principles-based approach, supported by enhanced abilities for the Commissioner to make legally binding instruments to provide greater certainty for the regulated community in areas where specific rules or greater clarity is required.
- Enhance and limit the application of privacy-self management tools to ensure that individuals are able to exercise meaningful choice and control by understanding how their personal information is being handled through notice and consent, where appropriate.
- Require regulated entities to ensure that all collections, uses or disclosures of personal information are fair and reasonable while ensuring increased safeguards are in place for certain high-risk information handling activities, or that these are prohibited.
- Introduce additional organisational accountability measures to ensure that entities have implemented actions and controls that demonstrate their compliance with the privacy regulatory framework.
- Enhance the OAIC's ability to regulate in line with community expectations through strengthened enforcement powers and new regulatory measures, including a direct right of action and statutory tort to provide individuals with greater control of their personal information.

- Enshrine global interoperability through proposed reforms that have been informed by international policy, standards and models for data protection and privacy thereby ensuring that personal information is protected wherever it flows.

A key strength of the Privacy Act is that it is principles-based. It sets out general rules which can be applied to a range of situations across the economy based on the risks posed by particular entities or personal information handling practices. To remain fit for purpose, it is essential that the Privacy Act contains flexible protections that can remain relevant as technologies shift and innovation continues, while creating legal obligations that address current and evolving privacy risks and harms. In some circumstances, this principles-based framework may need to be supplemented with more specific or prescriptive rules to address high-risk activities or sectors.

Privacy self-management tools of notice and consent continue to be important transparency mechanisms that help individuals exercise meaningful choice and control over their personal information. However, reliance on consent should be targeted and limited to situations where individuals can and should validly exercise a choice, not expanded and used more broadly to permit data handling practices.

Additional accountability measures can redress the power and information asymmetry between individuals and entities and ensure that the burden of understanding and consenting to complicated practices does not fall solely on individuals. More broadly, by embedding strong accountability measures, entities can build a reputation for reliable, transparent and effective privacy management which is essential to promoting consumer trust and confidence in their brand.

These legislative protections must be reinforced by a strong system of oversight that upholds individuals' rights and holds entities to account. The privacy regulator needs the correct tools to respond efficiently and appropriately to new threats and regulate in line with community expectations.

The current Privacy Act positions the regulator to resolve individual privacy complaints through negotiation, conciliation and determination. This reflects the context in which the Privacy Act was first introduced. In the digital environment, privacy harms can occur on a larger scale. While resolving individual complaints is a necessary part of effective privacy regulation, there must be a greater ability to pursue significant privacy risks and systemic non-compliance through regulatory action.

This shift can be seen in privacy regulation around the world, with privacy regulators being provided with powers that enable efficient and effective action to identify and respond to privacy threats. While Australia's current framework provides some enforcement powers, these need to be strengthened and recalibrated to deter non-compliant behaviour and ensure practices are rectified. The regulator also needs appropriate resources to proactively identify and address existing and emerging risks before serious, widespread or societal harm occurs.

Greater discretion for the Commissioner to focus on systemic risks should not leave individuals without a remedy, and should be complemented with the ability for people to take action directly through the courts, through the introduction of a direct right of action and a statutory tort for serious invasions of privacy.

Finally, the Privacy Act needs to connect with privacy laws around the world and ensure that personal information is protected wherever it flows. Strong privacy and data protection frameworks support innovation and growth in the Australian digital economy and international trade. Globally interoperable data protection laws are increasingly important to protect individuals online and reduce regulatory friction for business.

A summary of the OAIC's submission and outline of recommendations are provided below.

Summary of submission

Our submission is structured in thirteen parts.

- **Part 1: The Objectives of the Privacy Act** seeks to place the Privacy Act and the right of privacy in Australia in context and makes recommendations to amend the objects of the Privacy Act to ensure they remain fit for purpose into the next decade. In particular, this section includes recommendations to elevate the protection of individuals' privacy rights in the objects section of the Act, and recognise the significant public interest in the protection of privacy.
- **Part 2: Definition of personal information** discusses the importance of a flexible definition of personal information and proposes reforms to clarify the scope of this key concept, including in relation to technical data and inferred information.
- **Part 3: Flexibility of the APPs in regulating and protecting privacy** outlines the importance of maintaining the existing principles-based approach to Australia's privacy framework but recommends that the Commissioner is provided with enhanced abilities to make legally binding instruments to address areas of the law that require further certainty or specificity where appropriate. It also makes recommendations to enhance organisational accountability measures, strengthen individual rights and resolve ambiguities in the APPs.
- **Part 4: Exemptions** recommends that the scope of the Privacy Act is expanded to protect personal information held in employee records, and capture acts and practices by small business operators and political parties.
- **Part 5: Notice and consent** considers the strengths and limitations of notice and consent mechanisms in promoting privacy self-management and protecting individuals from privacy risks and harms. This section makes recommendations about how notice and consent requirements can be enhanced but suggests that these reforms should be complimented with the introduction of an overarching fair and reasonable requirement and additional organisational accountability obligations.
- **Part 6: Fairness and reasonableness requirements for entities** discusses the need to introduce additional responsibilities for APP entities, in order to address the limitations of privacy self-management and better protect the privacy rights of individuals. This part recommends the introduction of explicit requirements for APP entities to collect, use and disclose personal information fairly and reasonably and proposes a framework for fully and partially prohibiting certain information handling practices..
- **Part 7**: **Organisational accountability requirements for entities** outlines the importance of accountability requirements in facilitating compliance with privacy

obligations, meeting the expectations of regulators and building consumer trust and confidence in personal information handling practices. This part recommends several enhancements to APP 1 designed to enhance organisational accountability including express obligations to implement, and be able to demonstrate the steps taken to implement, a 'privacy by design' and 'privacy by default' approach. This part also discusses the benefits of an independent third-party certification scheme, which would enable Australians to quickly assess the level of data protection offered by an APP entity and further support organisational accountability.

- **Part 8: Overseas data flows** explores how the Privacy Act can establish an appropriate and interoperable framework that facilitates the efficient movement of data across borders alongside strong protections for individuals' personal information. This section considers the ways in which Australia's framework can be strengthened to ensure it remains globally interoperable and makes recommendations about how the extraterritoriality application of the Privacy Act can be strengthened.
- **Part 9: Enforcement powers under the Privacy Act and the role of the OAIC** provides a snapshot of the OAIC's current enforcement framework and argues that reforms are required to ensure that the OAIC can continue to meet community expectations of a contemporary regulator. This part recommends that the Commissioner be granted more discretion when exercising their regulatory powers in relation to individual complaints and that additional enforcement powers be introduced to enhance the Commissioner's ability to effectively investigate potential breaches of the Privacy Act, deter inappropriate conduct and support privacy best practice.
- **Part 10: Direct right of action** discusses how a direct right of action would complement the OAIC's recommended enhancements to the Commissioner's enforcement powers and makes recommendations about how a direct right of action should be framed under the Privacy Act.
- **Part 11: Statutory tort** recommends that a statutory tort for serious invasions of privacy is introduced, which would enhance Australia's privacy framework and constitute an important addition to the suite of regulatory measures needed to address online harms.
- **Part 12: Notifiable data breach scheme – impact and effectiveness** explores how the NDB scheme has been effective in meeting its key objectives of improving consumer protection and driving better security standards for protecting personal information. This part outlines some recommended enhancements to the NDB scheme designed to support timely notification and engagement with the OAIC.
- **Part 13: Interaction between the Act and other regulatory schemes** provides an overview of the Commissioner's regulatory responsibilities under various Commonwealth laws and the need to ensure that the Commissioner has full jurisdiction over enforcing any privacy protections that are included in other legislative regimes. This part also outlines the importance of harmonising privacy protections commensurate with those under the Privacy Act, which should be a key goal in the design of any federal, state and territory laws that purport to address privacy issues.

Recommendations

The OAIC recommends that the Privacy Act review:

Part 1: Objectives of the Privacy Act

Recommendation 1 – Amend the first object in s2A of the Privacy Act to state that the predominant object of the legislation is to recognise that individuals have a right to privacy and to protect individuals having regard to the collection, use or disclosure of their personal information.

Recommendation 2– Amend s 2A of the Privacy Act to more broadly state that an objective of the legislation is to promote the public interest in protecting privacy rights.

Recommendation 3 – Ensure that national consistency of privacy regulation is a key goal of the Council of Attorneys-General by establishing a working group to consider amendments to State and Territory privacy laws to achieve alignment with the Privacy Act.

Part 2: Definition of Personal Information

Recommendation 4 – Replace the word 'about' with 'relates to' in the definition of personal information to achieve greater clarity and certainty for regulated entities.

Recommendation 5 – Include a non-exhaustive list of technical data that may be captured by the definition of personal information in the explanatory memorandum for these amendments.

Recommendation 6 – Introduce a new subsection in the definition of personal information clarifying that the definition applies whether the information or opinion is provided, collected, created, generated or inferred.

Recommendation 7– Clarify that the concept of collecting personal information under the Privacy Act applies broadly, and includes gathering, acquiring, inferring or obtaining personal information from any source and by any means. This includes collection by 'creation', which may occur when information is created with reference to, or generated from, other information the entity holds.

Recommendation 8 – Replace the term 'de-identified' with 'anonymised' in the Privacy Act.

Recommendation 9 – Amend APP 1 to insert an express obligation that an APP privacy policy must notify individuals that their information may be anonymised and used for purposes other than those permitted for the initial collection.

Recommendation 10 – Extend the obligations of APP 11 to require APP entities to take reasonable steps to protect anonymised information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Recommendation 11 – Introduce a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state, except in order to conduct testing of

the effectiveness of security safeguards that have been put in place to protect the information.

Recommendation 12 – Extend Part IIIC to require notification where:

- there is unauthorised access to or unauthorised disclosure of anonymised information, or a loss of anonymised information, that an entity holds, in circumstances where there is a risk of re-identification of that information
- if this information is re-identified, it is likely to result in serious harm to one or more individuals, and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Recommendation 13 – Amend the Privacy Act to ensure that the definition of personal information extends to deceased individuals for a period of 30 years after death.

Part 3: Flexibility of the APPs in regulating and protecting privacy

Recommendation 14 – Amend the APP code framework in Part IIIB of the Privacy Act to provide the Commissioner with greater flexibility and discretion to develop APP codes. The framework should:

- enable the Commissioner to develop an APP code in the first instance (i.e. without having to first request a code developer to develop an APP code), and
- enable the Commissioner to issue a temporary APP code if it is urgently required and where it is in the public interest to do so, and
- retain the existing power which enables the Commissioner to request that a code developer develop a code, and
- enable the Commissioner to intervene at any point in the code development process where an APP code is being developed by a code developer if satisfied it would be preferable for the Commissioner to develop the code.

Recommendation 15 – Supplement the code-making powers in Part IIIB of the Privacy Act with a general power for the Commissioner to issue legally binding rules about the application of the APPs.

Recommendation 16 – Include a new provision in the Privacy Act that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

Recommendation 17 – Amend APP 3.6 to require an APP entity to take reasonable steps to satisfy itself that personal information that was not collected directly from an individual was originally collected in accordance with APP 3.

Recommendation 18 – Repeal APP 7 and rely on the existing use and disclosure requirements in APP 6 for direct marketing activities.

Recommendation 19 – Ensure that the proposed new right to object includes:

- an absolute right for individuals to object to the use and disclosure of their personal information for direct marketing purposes, and
- the ability for individuals to request an organisation to identify the source of the personal information and the organisation should be required to notify the individual of its source, unless this is unreasonable or impracticable.

Recommendation 20 – Introduce enhanced code-making powers and new powers for the Commissioner to issue legally binding rules to enable the Commissioner to make sector- or threat-specific legislative instruments that support the principles-based approach in APP 11.1.

Recommendation 21 – Introduce enhanced code-making powers and new powers to make legally-binding rules under the Privacy Act to enable the Commissioner to set requirements or standards for destruction and de-identification by legislative instrument where appropriate.

Recommendation 22 – Extend the right to request correction of personal information in APP 13 to personal information that is no longer 'held' by the entity.

Recommendation 23 – Introduce a right to erasure that includes, as a minimum:

- the exceptions recommended in the DPI report
- an exception for 'frivolous or vexatious' requests, consistent with APP 12, or a similar threshold, for example 'manifestly unfounded or excessive requests, consistent with the GDPR
- an appropriate timeframe within which APP entities must respond to erasure requests, for example consistent with APP 12 or the GDPR, and
- extends to personal information that is no longer 'held' by an entity, and to notify others of the erasure request where personal information has been made public, subject to the exceptions outlined at point (a) above.

Recommendation 24 – Introduce a requirement for APP entities to notify individuals of their ability to request the erasure of their personal information. This could be modelled on similar requirements in Article 13 of the GDPR.

Recommendation 25 – Introduce a right to object that includes:

- an absolute right to object in relation to direct marketing
- a limited right to object in relation to processing on other grounds.

Recommendation 26 – Introduce a requirement for APP entities to notify individuals of their ability to object to the handling of their personal information, including the absolute right for individuals to object to the use and disclosure of their personal information for direct marketing.

Part 4: Exemptions

Recommendation 27 – Remove the small business exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Recommendation 28 – Remove the employee records exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Recommendation 29 – Remove the political parties exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Recommendation 30 – Introduce greater enforceability requirements for the privacy safeguards covering media organisations. The review could consider whether the EDR scheme model is appropriate to achieve this outcome.

Part 5: Notice and consent

Recommendation 31 – Strengthen notice and consent requirements in the Privacy Act to address the limitations in these mechanisms, but preserve the use of consent for high privacy risk situations, rather than routine personal information handling.

Recommendation 32 – Introduce requirements that APP 5 notices should be concise, transparent, intelligible and written in clear and plain language.

Recommendation 33 – OAIC supports the development of standardised icons or lexicon through an industry led process to assist individuals make informed decisions about their personal information.

Recommendation 34 – Amend the definition of 'consent' to require a clear affirmative act that is freely given, specific, current, unambiguous and informed.

Recommendation 35 – Amend the Privacy Act to require all settings to be set to privacy protective as default except for collections of personal information that reasonably enable provision of the particular product or service.

Recommendation 36 – Elevate OAIC guidance on withdrawing consent into the Privacy Act, including a requirement that APP entities must notify an individual of their right to withdraw consent, where consent has been required for the personal information handling.

Part 6: Fairness and accountability requirements for entities

Recommendation 37 – Introduce fairness and reasonableness obligations into APPs 3 and 6:

> APP 3 - The collection of personal information by an APP entity under Australian Privacy Principle 3 must be fair and reasonable in the circumstances, even if an individual consents to the collection.
>
> and

APP 6 - The use or disclosure of personal information by an APP entity under Australian Privacy Principle 6 must be fair and reasonable in the circumstances, even if an individual consents to the use or disclosure.

Recommendation 38 – Introduce a non-exhaustive list of factors that the Commissioner will consider when determining whether acts or practices are fair and reasonable.

Recommendation 39 – Amend APP 1 to require APP entities to take steps as are reasonable in the circumstances to implement practices, procedure and systems which will mitigate the risk of unfair and unreasonable information handling practices as a result of the entity's handling of personal information.

Recommendation 40 – Introduce full or partial prohibitions of specified information handling activities into the general privacy framework. These could apply to the following practices:

- profiling, tracking or behavioural monitoring of, or direct advertising targeted at children
- inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices
- scraping of personal information from online platforms
- handling location information about individuals, and
- certain uses of AI technology to make decisions about individuals.

Recommendation 41 - Introduce additional rights that apply specifically to the processing of personal information by AI technologies.

Part 7: Organisational accountability requirements for entities

Recommendation 42 – Amend APP 1 to include express accountability requirements for all regulated entities. At a minimum, APP 1 should require entities to:

- take reasonable steps, and *demonstrate* those reasonable steps, to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP code under APP 1.2
- implement, and be able to demonstrate the steps taken to implement, a 'privacy by design' and 'privacy by default' approach
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code, and to implement a 'privacy by design' and 'privacy by default' approach, and
- appoint a privacy officer or privacy officers and ensure that privacy officer functions are undertaken.

Recommendation 43 – Include a note in the explanatory memorandum that will accompany the amending Bill that an ongoing and demonstrable, comprehensive privacy management program, which includes conducting privacy impact assessments where appropriate, is central to facilitating a 'privacy by design' and 'privacy by default' approach.

Recommendation 44 – Amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the purposes for which the information is to be collected, used or disclosed and to record those purposes.

Recommendation 45 – Introduce a domestic privacy certification scheme into Australia's privacy framework. The certification scheme should:

- be interoperable the APEC CPBR system and other relevant domestic accreditation or certification schemes
- be voluntary across the economy generally, but may be made mandatory in relation to specific high privacy risk sectors or practices through an APP code or rules where appropriate
- be flexible and enable entities to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes
- enable the OAIC to develop and publish accreditation requirements for certification bodies and certification criteria for the scheme
- ensure that an independent third party is responsible for appointing the accreditation body or bodies that will carry out audits of entities seeking certification and approving the use of a trust mark or seal and identify the OAIC as the scheme's regulator for privacy breaches.

Part 8: Overseas data flows

Recommendation 46 – Consider whether additional legislated transfer mechanisms could enhance the APP 8 accountability approach. These could include:

- Contractual safeguards (to support an APP entity's accountability under APP 8.1, rather than an exception to accountability under APP 8.2)
- Certification
- 'Adequacy' or whitelists.

Recommendation 47 – Amend the Privacy Act to address issues with the extraterritoriality of the Act, including:

- Remove the requirement in s 5B(3)(c) for the information to have been collected or held in Australia be removed, and instead the collection or holding of information could be considered an indicator of 'carrying on a business in Australia'.
- Amend s 5B(3) to refer to particular indicators of 'carrying on business in Australia' for the purposes of the Privacy Act.
- Extend the extraterritorial operation of the Privacy Act to a body corporate that has collected Australians' personal information from a related body corporate to which s 5B(3) applies (irrespective of whether it carries on business in Australia in its own right).

Part 9: Enforcement powers under the Privacy Act and role of the OAIC

Recommendation 48 – Amend s 40(1) to replace the words 'shall investigate' with 'may investigate' and clarify in the Explanatory Memorandum that this change is to allow the Commissioner to exercise discretion to investigate based on factors such as the Commissioner's regulatory policies and priorities, whether the resources needed to investigate a complaint are proportionate to the likely outcome or remedy available and whether the substance of the complaint is about matters that fall under the Privacy Act.

Recommendation 49 – Expand s 41(dc) to instances where a complaint has already been adequately dealt with by an EDR scheme.

Recommendation 50 – Introduce the following amendments to the enforcement mechanisms under the Privacy Act:

- empower the Commissioner to issue infringement notices for interferences with privacy and where a person fails to give information to the Commissioner when this has been required under the Privacy Act
- introduce civil penalties for interferences with privacy
- provide the Federal Court with the power to make the conduct orders which are available to the Commissioner through a s 52 determination
- allowing the Commissioner to make order in a s52 determination requiring respondents identify and mitigate foreseeable risks or delete personal information
- enhance the Commissioner's search and seizure powers to allow the OAIC to make copies of information and documents specified in the warrant and operate electronic materials to determine whether the kinds of information and documents specified in the warrant are accessible
- empower the Commissioner to seek a warrant to preserve and secure relevant information and documents.

Part 10: Direct right of action

Recommendation 51 – Ensure that the direct right of action is not limited to 'serious' breaches of the Privacy Act or the APPs.

Recommendation 52 – Ensure that the direct right of action is framed so that individuals are required to make a complaint, or a representative complaint, to the OAIC before applying to the courts.

Recommendation 53 – Ensure that the Commissioner has appropriate powers to decline to investigate a complaint or representative complaint, or continue to investigate a complaint or representative complaint, where the matter is more appropriately dealt with by the courts.

Recommendation 54 – Revise the representative complaint provisions under Part V of the Privacy Act to ensure greater alignment with the powers available to the Federal Court under the Federal Court Act in relation to the management of class actions.

Recommendation 55 – Ensure that damages recoverable under a direct right of action for privacy breaches are not capped.

Recommendation 56 – Supplement the direct right of action with legislative options for the OAIC to exercise:

- a right to intervene in proceedings (or alternatively to seek the leave of the court to intervene)
- a right to seek leave of the court to act in the role of amicus curiae in the proceedings.

Part 11: Statutory tort

Recommendation 57 – Introduce a statutory tort for serious invasions of privacy into Australia's privacy framework.

Recommendation 58 – Supplement the statutory tort with legislative powers for the OAIC to be notified of, to exercise a right to intervene in proceedings, and to seek the leave of the court to act in the role of *amicus curiae* in the proceedings.

Recommendation 59 – Enact a single and comprehensive tort, rather than confining the tort to intrusion upon seclusion and misuse or disclosure of private information.

Recommendation 60 – Enact a tort that does not specify a fault element to ensure it covers intentional, reckless and negligent acts.

Recommendation 61 – Include a requirement to weigh other public interests, including the right to freedom of expression and the public interest in being informed about matters of public concern, as part of the consideration as to whether an individual's privacy has been seriously invaded.

Part 12: Notifiable Data Breaches scheme – impact and effectiveness

Recommendation 62 – Amend s 26WK so that once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, they must notify the Commissioner as soon as practicable, but no later than 30 days, after the entity became aware that there were reasonable grounds to *suspect* that there may have been an eligible data breach.

Recommendation 63 – Amend s 26WL so that an entity must notify individuals as soon practicable, but no later than five days, after notifying the Commissioner.

Recommendation 64 – Amend s 26WR to provide the Commissioner with an express power to direct an entity to continue to investigate a data breach and provide subsequent notification to affected individuals if required in the circumstances.

Recommendation 65 – Enable the Commissioner to issue an infringement notice or apply to the Courts for a civil penalty in circumstances where an entity has failed to comply with the prescribed timeframes.

Recommendation 66 – Include an express requirement for entities to take reasonable steps to mitigate the adverse impacts of risk of harm to individuals whose personal information has been involved in a breach and, to the extent possible, return an individual to the position they would have been in prior to the breach.

Part 13: Interaction between the Act and other regulatory schemes

Recommendation 67 – Ensure that the Commissioner has full jurisdiction over enforcing any privacy protections that are included in other legislative regimes.

Recommendation 68 – Amend the Privacy Act to provide an express power for the Commissioner to share information with other bodies where necessary, including other regulators and government agencies, law enforcement and complaint handling bodies (including State or Territory or foreign bodies if they have functions to protect the privacy of individuals).

Recommendation 69 – Ensure that harmonisation of privacy protections is a key goal in the design of any federal, state or territory laws that purport to address privacy issues.

Recommendation 70 – Ensure that the privacy protections in any laws that purport to address privacy issues are commensurate with those under the Privacy Act.

Part 1: Objectives of the Privacy Act

1. Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

Putting the Privacy Act in context

1.1 Privacy is a fundamental human right recognised in Article 12 of the *UN Declaration of Human Rights*, in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), and in many other international and regional agreements.[4]

1.2 The scope of the right to privacy is broad and contextual. It has been variously recognised as part of the right to life and to be let alone[5] and a prior condition to the exercise of other fundamental rights, including freedom, equality and democracy.[6] The High Court of Australia has recognised that the foundation of what is protected by the right of privacy is human dignity.[7]

1.3 In Australia, the right to privacy has been given effect as a data protection statute, rather than a law that protects or promotes broader concepts of privacy. In addition to the ICCPR, the Privacy Act incorporates the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (OECD Guidelines).

1.4 The Privacy Act therefore seeks to give effect to the fundamental right to privacy in Australian society by preventing individuals from being subject to arbitrary interferences with their personal information and protecting them from harm stemming from the misuse of their personal information.

1.5 This human rights foundation is a key reason why privacy legislation exists in Australia and internationally as a separate and complementary framework to other Australian laws that protect the rights of individuals. For example, while consumer law provides important rights for consumers in trade or commerce, privacy protections apply to individuals beyond a commercial context.

1.6 It is also said that the right to privacy is not an absolute right. While not explicit, Article 17 of the ICCPR recognises that entities may have legitimate reasons to undertake

---

[4] For examples of other international agreements enshrining a right to privacy, see United Nations Human Rights: Office of the High Commissioner (n.d.) *International Standards*, United Nations Website, accessed 23 November 2020.

[5] Warren S and Brandeis L (1980), 'The Right to Privacy', *Harvard Law Review*, 4(5), pp. 193-220.

[6] Office of the Privacy Commissioner of Canada (2020) *2019-2020 Annual Report to Parliament on the Privacy Act and Personal Information Protection and Electronic Documents Act*, Office of the Privacy Commissioner of Canada website, accessed 23 November 2020.

[7] See the judgment of Chief Justice Gleeson in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, [43]. The basis of privacy in human dignity was echoed in the extensive discussion of the right of privacy in the Indian Supreme Court decision *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors* (Writ Petition (Civil) No 494 of 2012), [28] - [40].

projects that may limit or interfere with privacy, provided that any impacts are reasonable, necessary and proportionate to achieve a legitimate objective.

1.7 Similarly, the aim of the OECD Guidelines is to strike a balance between protecting the privacy, rights and freedoms of individuals without creating barriers to trade and allowing the uninterrupted flow of personal data across national borders.

1.8 The current objects in the Privacy Act seek to reflect this balance. The objects recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities. The objects also promote responsible and transparent handling of personal information and support the free flow of information while ensuring that the privacy of individuals is respected.[8] This balance is reflected throughout the Privacy Act, which provides a framework for regulated entities to assess whether any impacts on individuals' privacy rights are necessary, reasonable and proportionate to achieving their legitimate functions and other public interests.

1.9 In its contemporary context, the notion of balance in the objects of the Privacy Act risks being viewed as advantaging one party to the detriment of another. Such a viewpoint entrenches the idea that individuals' privacy rights can only be protected if entities' functions and activities are curtailed, or that allowing entities to go about their business will necessarily have privacy impacts for individuals.

1.10 However, balancing privacy rights with economic, security and other important public interest objectives is not a zero-sum game. There are mutual benefits to individuals and regulated entities if the rights and responsibilities in the Privacy Act are in the correct proportion. Effective privacy laws support economic growth by building trust and confidence that innovative uses of data are occurring within a framework that promotes accountability and sustainable data handling practices. Increasing individuals' confidence in the way their personal information is managed will likely lead to greater support for services and initiatives that propose to handle this information. These are essential ingredients to a vibrant digital economy and digital government.

1.11 The OAIC considers that the Privacy Act review represents an opportunity to enhance the recognition in the Act that strong data protection and privacy rights are necessary to both protect individuals and as a precondition for consumer confidence, economic growth and to meet other societal objectives such as the protection of health, safety and security. The OAIC's Recommendation 2 to amend s 2A to reflect the public interest in protecting privacy rights will help to achieve this outcome. The review could also consider other ways in which the mutual dependence between strong privacy protections and the interests of entities could be reflected in the objects of the Act.

1.12 Introducing a greater focus on the mutual interests in protecting individuals' personal information will engender greater respect for privacy rights and increase individuals'

[8] *Privacy Act 1988* (Cth), s 2A.

trust in the personal information handling practices of entities, which has been in decline in recent years.

> Since 2007, there has been a general downward trend in trust in most of the categories presented. Trust in companies in general is down by 13%. Trust in Federal Government departments is down 14%, with a steady decline in trust over the past 13 years.[9]

Focusing privacy protections on individuals

1.13 The OAIC considers that the Privacy Act review presents an opportunity to place greater emphasis on the rights of individuals and the obligations of entities to protect those rights. A greater focus in the objects on the protection of individuals from privacy harms would support responsible innovation, economic development and other important societal objectives by promoting trust and confidence in government and commercial activities.

1.14 Consequently, the OAIC recommends that the first object of the Privacy Act is amended to reflect this approach. Section 2A(a) currently states that one of the objects of the Act is:

> (a) to promote the protection of the privacy of individuals; and

1.15 The OAIC recommends that this object is amended to clarify that the intention of the Privacy Act is to protect individuals from harms stemming from interferences with privacy. This amendment would direct the Privacy Act towards placing a greater emphasis on the harms it is seeking to prevent.

1.16 This amended object could be modelled on the first objective of the EU General Data Protection Regulation (GDPR) which focuses on the protection of natural persons:

> 1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[10]

1.17 Also relevant is the '*For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*' (ALRC report), in which the Australian Law Reform Commission (ALRC) recommended a greater focus on the individual:

> Recommendation 5-4 The Privacy Act should be amended to include an objects clause. The objects of the Act should be specified to:

---

[9] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, pg. 56.

[10] 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) [2016] OJ L 119/1 ('General Data Protection Regulation'), Article 1.

...

(b) recognise that individuals have a right to privacy and to promote the protection of that right;

Recommendation 1 – Amend the first object in s 2A of the Privacy Act to state that the predominant object of the legislation is to recognise that individuals have a right to privacy and to protect individuals having regard to the collection, use or disclosure of their personal information.

Recognising a public interest in privacy

1.18 The OAIC also considers that there would be value in the Privacy Act recognising that there is a significant public interest in privacy protections.

1.19 A societal interest in privacy protections has long been recognised, including the potential for societal harms to occur through interferences with privacy. For example, the ALRC report stated that:

> Although the right to privacy is an individual right, there is a strong public interest in protecting that right. For example, it is essential that health consumers are confident that their health information will be handled appropriately or they may resist sharing that information with health service providers. This has the potential to have a negative impact on the health of the individual and is also an undesirable public policy outcome, with the potential to impact on the health of the community as a whole.[11]

1.20 It is increasingly clear that individual privacy decisions are capable of impacting other people and the community at large. Practical examples of this include:

- The importance of personal information in the response to the COVID-19 pandemic highlighted the social interest in privacy issues.
- The development of predictive analytics tools that require vast quantities of personal information allows for decisions to be made about an individual, regardless of whether that individual's personal information was used to develop the technology.
- Individual decisions around the use or disclosure of genetic information, which may be the sensitive information of multiple people.[12]

[11] See ALRC (2008), *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* report prepared by the ALRC, Australian Government, 5.123.

[12] Creet Prof. J (2020) *Home genealogy kit sales plummet over data privacy concerns*, The Conversation website, accessed 26 November 2020.

- The disclosure of aggregated location data, which was used to identify confidential military bases.[13]
- Increased political polarisation as a result of personalisation and targeting driven by personal information online.[14]

1.21 This is also demonstrated by the privacy concerns and impacts that flowed from revelations about the activities of Cambridge Analytica or mass-scale emotional manipulation experiments on social networks.[15]

1.22 Despite being driven by personal information, these acts and practices have tested the ability of the Privacy Act to respond in a manner commensurate with the community's expectations. The focus of the privacy framework on enabling individual privacy decisions through transparency and consent mechanisms may not be capable of addressing these collective privacy concerns.

1.23 Recognising this wider public interest in the objects of the Privacy Act would complement the OAIC's Recommendation 1 by ensuring that the Act can address instances where privacy-affecting acts and practices have undesirable public policy outcomes, even if the privacy harms to any one individual are not significant.

1.24 This submission puts forward the view that the existing protections and obligations in the Privacy Act needs to be reconceptualised to better address activities that cause societal harm by undermining key values and fundamental rights in Australian society, in addition to impacting individuals.

Recommendation 2 – Amend s 2A of the Privacy Act to more broadly state that an objective of the legislation is to promote the public interest in protecting privacy rights.

Nationally consistent privacy law

1.25 One of the objects of the Privacy Act is to provide the basis for nationally consistent regulation of privacy and the handling of personal information. We note, however, that to date this has not been achieved, with the individual States and Territories having very different levels of privacy protection.

1.26 This is particularly important given Commonwealth, State and Territory governments are increasingly working together on national initiatives that involve sharing information across jurisdictions. In many instances, these initiatives rely on jurisdictions across Australia having privacy frameworks that are equivalent to the

[13] Hern A (2018) *Fitness tracking app Strava gives away location of secret US army bases*, The Guardian website, accessed 26 November 2020.

[14] Johnson S, Kitchens B and Gray P (2020) *Facebook serves as an echo chamber, especially for conservatives. Blame its algorithm*, The Washington Post website, accessed 26 November 2020.

[15] Meyer R (2014) *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, The Atlantic website, accessed 26 November 2020.

protections afforded by the Commonwealth Privacy Act, including commensurate protections for personal information such as mandatory data breach notification requirements.

1.27 The OAIC recommends that national consistency of privacy regulation should be a key goal of the Council of Attorneys-General (CAG). Alignment of rights and obligations with the Privacy Act would ensure that Australians' personal information is subject to similar requirements, whether that information is being handled by an Australian Government agency, a State or Territory government agency, or private sector organisations. Consistency in regulation across jurisdictions will also reduce compliance burdens and cost and provide clarity and simplicity for regulated entities and the community.

Recommendation 3 – Ensure that national consistency of privacy regulation is a key goal of the Council of Attorneys-General by establishing a working group to consider amendments to State and Territory privacy laws to achieve alignment with the Privacy Act.

Part 2: Definition of Personal Information

Importance of flexibility

2.1 The definition of 'personal information' is a key concept that delineates the scope of what is regulated and sought to be protected under the Privacy Act.

2.2 The current definition does not list specific types of information that constitute 'personal information'. Instead, the definition sets out a test whereby, depending on the circumstances, any type of data can be personal information if it is about an identified individual, or an individual who is reasonably identifiable.

2.3 The definition of personal information is therefore neutral in its application to different sectors, different activities and different technologies. The definition can be applied flexibly in different contexts and to a broad range of information, which ensures it is adaptable as technology and the way data is used evolves.

2.4 The OAIC considers that there are significant benefits in retaining this flexible and broad definition. However, a number of challenges have tested the scope of the current definition and created some uncertainty, particularly around the following issues:

- When personal information will be 'about' an individual
- The application of the definition to technical information
- Whether the definition captures inferred information
- Whether the current threshold is fit for purpose
- Whether the definition should capture individuated information.

2.5 The OAIC's recommendations in this section address these uncertainties, as well as whether reforms should be introduced in relation to de-identified information.

2.6 The definition of personal information is a foundational concept in the Privacy Act. These recommendations will help to ensure that the definition is fit for purpose now and into the future.

Information 'about' an individual

2. What approaches should be considered to ensure the Act protects an appropriate range of technical information?

2.7 The OAIC considers that clarifying when information is 'about' an individual is the most fundamental issue that needs to be addressed in relation to the definition of personal information in the Privacy Act. Addressing issues caused by overly narrow interpretations of this term will assist in resolving other key matters raised in the Issues Paper and promote greater clarity about the circumstances in which information will be in scope.

2.8 As highlighted in the Issues Paper, the Full Federal Court of Australia's decision in *Privacy Commissioner v Telstra Corporation Ltd* (the Grubb case) considered the meaning of personal information and has challenged the application of the definition.[16] In finding that the individual needs to 'be a subject matter' of the information, this judgment risks being interpreted as narrowing the definition of personal information.

2.9 Following this decision, the OAIC is aware of uncertainty in the regulated community around whether the information is 'about' an individual. To a large extent, the need to clarify whether the definition of personal information captures technical information stems from this uncertainty. This is despite the Court noting that it was only deciding a point of law about the meaning of the word 'about' and did *not* decide whether metadata actually met the definition of personal information.

2.10 This uncertainty was highlighted in the Treasury Laws Amendment (Consumer Data Right) Bill 2019, which adopted the word 'relate' rather than 'about' in the definition of CDR data. As explained in the explanatory memorandum to the Bill, this is because:

> [1.106] The concept of 'relates to' is a broader concept than information 'about' an identifiable or reasonably identifiable person under the *Privacy Act 1988*. For example, using this term is intended to capture meta-data of the type found not to be about an individual in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4 (19 January 2017).
>
> [1.107] 'Relates' can include reference to an identifier such as a name, an identification number, location data of the person or of products that would reasonably be expected to be co-located with either the person or their address, an online identifier (including cookie identifiers and internet protocol addresses) or to one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person.

2.11 The OAIC recommends replacing the word 'about' in the definition of personal information with 'relates to', which would promote consistency with the Consumer Data Right (CDR) regime and the GDPR. This amendment would also assist in resolving the uncertainty caused by the Grubb judgment and afford an opportunity to re-engage with the regulated community about the scope of the Privacy Act. It would also support the OAIC's Recommendation 5 about capturing technical information in the definition of personal information.

2.12 The OAIC considers that this would achieve greater clarity and certainty, rather than impose a significant regulatory burden on APP entities.

Recommendation 4 – Replace the word 'about' with 'relates to' in the definition of personal information to achieve greater clarity and certainty for regulated entities.

[16] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.

Other changes to address 'technical information'

2.13 In addition to the key change to the definition of personal information, recommended above, the OAIC recommends that the explanatory memorandum makes clear that the definition of personal information is intended to capture certain types of technical information.

2.14 Online identifiers and device identifiers are increasingly being used to track individuals. This is rivalling names and addresses as key information used to identify people.[17] At the same time, there is often uncertainty about whether technical information can be personal information under the Privacy Act, particularly since the Grubb case.[18]

2.15 The OAIC considers that including an explanation that the definition of personal information is intended to capture technical information in the explanatory memorandum will support ongoing flexibility, while clarifying that this type of data can be personal information in appropriate circumstances. This would also bring the Privacy Act in line with more modern privacy regulations around the world.

2.16 In making this recommendation, the OAIC has considered several factors:

- **Future-proofing the definition** – The technology-neutral nature of the definition is important to allow it to evolve over time, particularly as the types of technical information that may be considered personal information will change with technological developments. An overly prescriptive definition runs the risk of quickly becoming out-of-date. For example, while cookies have commonly been considered an important online identifier, online platforms are already planning to phase this technology out.
- **Capturing appropriate information** – Technical data is often used for essential purposes to the running of the internet such as authentication, session management, security management and network routing. These same types of technical data, however, can also be used for tracking or profiling purposes, meaning that it may be personal information under the current definition. Technical data may even be used for both purposes at the same time or may be repurposed over the life of the identifier. The definition must be flexible enough to capture technical data that is personal information without placing undue obligations on information that does not carry privacy risks.

2.17 Having regard to these issues, the OAIC does not recommend listing specific types of technical data in the definition. Rather, the OAIC recommends that the explanatory memorandum for Recommendation 4 could set out a non-exhaustive list of some of the types of technical information that could be caught within the definition. This

[17] See for example UK Information Commissioner's Office (2019) *Update Report into adtech and real time bidding*, ICO, United Kingdom Government, p. 12, which found that most requests for online advertising contained several types of online identifiers including an IP address, cookie ID, location information and device information.

[18] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.

could be modelled on the explanatory memorandum for the Treasury Laws Amendment (Consumer Data Right) Bill 2019 set out above.[19]

2.18 The Commissioner-issued guidelines could also clarify the types of technical data that may be caught by the definition of personal information.[20]

2.19 Placing this list in the explanatory memorandum clarifies that the definition could capture technical information without detracting from the key aspect of any assessment for personal information, which is whether the information relates to an identified or reasonably identifiable individual (as discussed in paragraphs 2.7-2.12 above). This recommended approach also avoids the likelihood of the definition quickly becoming out of date if specific types of technical data are listed.

2.20 The explanatory memorandum could provide additional clarification about the scope of these terms, for example that online identifiers may include cookies, IP addresses, MAC addresses or user IDs.

2.21 While this recommendation will assist in clarifying the circumstances in which technical data will be personal information, technological advancements are increasingly challenging the concept of personal information beyond the application of the definition to technical data. New developments in the way that data is handled are making it increasingly difficult to draw a bright line between personal and non-personal information.[21] This is particularly true where a third party is able to draw inferences, track, profile or directly impact individuals without being able to identify them. For example, the OAIC understands that individuated information is increasingly being used to target content to individuals online, including advertisements, job offers or political content.[22]

2.22 Online targeting has the potential for individuals to experience harm, including discrimination through preferential pricing or exclusion.[23] To the extent that online targeting is covered under the Privacy Act, these harms may be addressed by the OAIC's Recommendation 37 to introduce fairness and reasonableness obligations on APP entities, which can be further particularised in the planned online platforms code. These issues, however, may go beyond the scope of privacy and may also be more

---

[19] This explanatory memorandum substantially captures the types of data listed in the definition of personal data in Article 4 and Recital 30 of the GDPR.

[20] The OAIC recommends that a new provision is included in the Privacy Act that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act. See Recommendation 16 below.

[21] See also the discussion of the challenges posed by AI technologies to the definition of personal information in Office of the Victorian Information Commissioner (2018), *Artificial intelligence and privacy*, OVIC, Victorian Government, p. 9.

[22] Individuation refers to the ability to disambiguate or single out a person in a crowd, such that that individual could be tracked, profiled, targeted, contacted or subject to a decision or action which impacts upon them, even if that individual's identity was not known or knowable (see discussion from page 9 in Johnson A 2020, Individuation: Re-imagining data privacy laws to protect against digital harms, *Brussels Privacy Hub Working Paper* 6 (24), 1-22).

[23] See discussion from page 41 in Salinger Privacy (2020), *The Definition of Personal Information,* research paper for the Office of the Australian Information Commissioner, Salinger Privacy.

appropriately addressed by other regulatory regimes targeted towards the specific harms experienced.

Recommendation 5 – Include a non-exhaustive list of technical data that may be captured by the definition of personal information in the explanatory memorandum for these amendments.

Inferred personal information

3. Should the definition of personal information be updated to expressly include inferred personal information?

36. Does the definition of 'collection' need updating to reflect that an entity could infer sensitive information?

Clarifying the status of inferred information

2.23 The use of big data and predictive data analytics make it possible to make more accurate inferences and predictions about individuals, which are being used to create increasingly detailed profiles of individuals.[24] These inferences are often about sensitive information that an individual would not expect and may not have disclosed voluntarily.

2.24 The definition of personal information includes 'information or an opinion' about a person, 'whether the information or opinion is true or not'. By explicitly including opinion as well as information, the OAIC suggests that inferred data about an identified or reasonably identifiable individual will already be captured by the definition. This position is reflected in existing OAIC guidance. The OAIC supports this guidance being elevated into law to clarify that the definition of personal information captures inferred information.[25]

2.25 This amendment would also meet the expectations of the Australian community about the protection of inferred information online.

[24] See discussion of inferred information in Office of the Victorian Information Commissioner (2020), *The Internet of Things and Privacy*, OVIC, Victorian Government, p. 5. See examples of the use of inferred data to profile individuals in European Data Protection Board (2 September 2020) Guidelines 8/2020 on the targeting of social media users, EDPB, accessed 18 November 2020, pp. 22-24.

[25] See for example OAIC (May 2017) *The definition of personal information* [online document], OAIC, accessed 18 November 2020 and OAIC (March 2018) *Guide to data analytics* [online document], OAIC, accessed 18 November 2020.

79% of Australians consider an organisation inferring information about them (for example, sexual orientation, mental health, political views) based on what they do online to be misuse.[26]

2.26 The OAIC recommends that a new subsection (c) is introduced to the existing definition of personal information in s 6 of the Privacy Act:

> (c) whether the information or opinion is provided, collected, created, generated or inferred.

2.27 The OAIC's proposed amendment clarifies the existing definition of personal information, rather than broadening its scope. APP entities are already required to assess whether inferred information meets the definition of personal information, however the OAIC considers that including an explicit requirement to do so will provide greater clarity and certainty for entities and individuals.

Collection as creation

2.28 The OAIC does not consider that the definition of 'collects' needs to be updated to reflect that an entity could infer personal or sensitive information, as the issue will be addressed by the OAIC's Recommendation 6. Nonetheless, the OAIC sees merit in amending the definition of 'collects' in s 6 of the Privacy Act to clarify the types of activities that can constitute collection.

2.29 The OAIC recommends adopting the explanation of 'collects' from the OAIC's APP guidelines as the basis for this reform.[27] The guidelines state that the concept of 'collects' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. This includes collection by 'creation', which may occur when information is created with reference to, or generated from, other information that the entity holds.[28]

2.30 Elevating this guidance into the Privacy Act would complement the OAIC's recommended amendment to the definition of personal information to clarify the status of inferred information under the Act.

Recommendation 6 – Introduce a new subsection in the definition of personal information clarifying that the definition applies whether the information or opinion is provided, collected, created, generated or inferred.

Recommendation 7 – Clarify that the concept of collecting personal information under the Privacy Act applies broadly, and includes gathering, acquiring, inferring or obtaining personal information from any source and by any means. This includes collection by 'creation', which

[26] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 36.

[27] OAIC (March 2018) *Guide to data analytics* [online document], OAIC, accessed 18 November 2020.

[28] OAIC (March 2018) *Guide to data analytics* [online document], OAIC, accessed 18 November 2020.

may occur when information is created with reference to, or generated from, other information the entity holds.

De-identified, anonymised and pseudonymised information

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

2.31 The OAIC encourages the use of de-identified information where possible,[29] as an important privacy protective measure. However, technological advancements are continually increasing the risk that information can be re-identified, particularly if the de-identified information is released publicly or the subject of a data breach.

2.32 The Privacy Act is still relevant to de-identified information. In particular, APP entities will have to consider the de-identified information that they hold and their compliance with APPs 6, 8 and 11, as these are the APPs that may apply if the data is to be transferred to another environment or the circumstances in which it is held changes.[30]

2.33 However, the OAIC considers that there is merit in placing additional protections on this type of information. These additional protections should be balanced with the need to ensure that APP entities are not discouraged from relying on this privacy protective measure.

2.34 The OAIC recommends that the term 'de-identified' is replaced with 'anonymised' in the Privacy Act. This would overcome a lack of clarity arising from dual meanings of the term 'de-identified', which is commonly used to describe certain technical processes and also used in a legal sense under the Privacy Act:

- We understand that the term 'de-identified', from a technical standpoint, means data that has been subjected to de-identification techniques (such as the removal of direct identifiers like name, address, etc).[31]
- This is a lower standard than prescribed in the Privacy Act, which means that the information is no longer about an identifiable (or reasonably identifiable) individual.

[29] According to s 6 of the Privacy Act, personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

[30] See discussion of the application of privacy obligations to de-identified information in OAIC (March 2018) *De-identification and the Privacy Act* [online document], OAIC, accessed 18 November 2020.

[31] See for example Department of Premier and Cabinet (2018), *De-identification Guideline,* report prepared by the Chief Data Officer, Department of Premier and Cabinet, Victoria Government, Chapter 4 (De-identification techniques and technologies).

2.35 Using the term 'anonymised' in the Privacy Act and relevant guidance will also bring Australia into closer alignment with other international privacy regimes. International jurisdictions have moved away from the term 'de-identified' to promote clarity in legal standards. Under the GDPR this is referred to as 'anonymised' data and pseudonymisation.[32]

2.36 We also consider that there is merit in providing additional protections for anonymised information. These would include:

- **APP 1** – Amending APP 1 to insert an express obligation in APP privacy policies which require notification to individuals that their information may be anonymised and used for purposes other than those permitted for the initial collection.
- **APP 11** – Extending the obligations of APP 11 to require APP entities to take reasonable steps to protect anonymised information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- **APP 11** – Introducing a prohibition on APP entities taking steps to re-identify information that was collected by them in an anonymised state, except in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.

2.37 In practice, an important part of complying with these obligations would include requiring APP entities to conduct ongoing and regular re-identification risk assessment checks to ensure that information remains anonymised, including whether information becomes available that increases the re-identification risk. As part of taking 'reasonable steps', entities will need to ensure that any measures applied to anonymise the information are proportionate to the purpose for which the information is anonymised and the sensitivity of the personal information. Good data governance should apply throughout all stages of the anonymisation process and be in place before and after anonymisation has occurred.

2.38 The OAIC also recommends an amendment to the NDB scheme requiring notification where an APP entity identifies that:

- there is unauthorised access to or unauthorised disclosure of anonymised information, or a loss of anonymised information, that an entity holds, in circumstances where there is a risk of re-identification of that information
- if this information is re-identified, it is likely to result in serious harm to one or more individuals, and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

2.39 Information will be anonymised where the risk of an individual being re-identified in the data is very low in the relevant context in which it is held or released. In practice,

[32] See GDPR Article 4 and Recital 26.

this means that information may be considered anonymised while held by an APP entity but would be personal information if released publicly.

2.40 This risk of re-identification will shift where the context in which information is held changes, for example, because of loss or unauthorised access or disclosure. Clarifying that notification is required in these circumstances will allow individuals to take steps to protect themselves from serious harm, while also alerting the OAIC to potential breaches of the APP 11 obligation recommended above.

Recommendation 8 – Replace the term 'de-identified' with 'anonymised' in the Privacy Act.

Recommendation 9 – Amend APP 1 to insert an express obligation that an APP privacy policy must notify individuals that their information may be anonymised and used for purposes other than those permitted for the initial collection.

Recommendation 10 – Extend the obligations of APP 11 to require APP entities to take reasonable steps to protect anonymised information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Recommendation 11 – Introduce a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state, except in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.

Recommendation 12 – Extend Part IIIC to require notification where:

- there is unauthorised access to or unauthorised disclosure of anonymised information, or a loss of anonymised information, that an entity holds, in circumstances where there is a risk of re-identification of that information
- if this information is re-identified, it is likely to result in serious harm to one or more individuals, and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Information about deceased individuals

5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

2.41 As observed in the Issues Paper, the definition of personal information relates to information about an 'individual'. This term is defined in the Privacy Act as 'a natural person'. This means that the definition of personal information does not capture information about deceased individuals unless the information is also about a living person.

2.42 The OAIC recommends that the definition of 'individual' is amended to capture deceased individuals. This would have several benefits:

- It would create consistency with the privacy laws in many State privacy jurisdictions, which cover information about deceased individuals, thereby furthering the object of the Privacy Act to provide the basis of nationally consistent regulation of privacy.
- It would allow for the creation of a framework to appropriately and respectfully deal with the information of an individual after they have died. For example, we understand that this has been an issue in relation to social media profiles of deceased individuals.

2.43 The OAIC recommends that the Privacy Act cease to apply to information about an individual who has been dead for more than 30 years. This would promote consistency with privacy legislation in New South Wales and Victoria.[33]

2.44 The OAIC suggests that the Privacy Act review ensure that work on this issue is aligned across Government and consider any implications that this recommended amendment may have on other Commonwealth laws. The OAIC notes that other Commonwealth information laws, the *Freedom of Information Act 1982 (Cth)* (FOI Act) and the *Archives Act 1983* (Cth), already protect against unreasonable disclosure of personal information of deceased individuals in response to requests for access to government documents.[34]

2.45 The OAIC notes that the New South Wales Law Reform Commission recommended enacting a statutory scheme to govern access to digital records of deceased individuals.[35] The Council of Attorney-Generals has agreed to form a Working Group to consider developing a nationally consistent approach to the regulation of access to these digital records.[36] Enacting a national scheme that regulates access to such records will provide greater certainty about when access should be granted and to whom. The OAIC considers that this work should inform the development of a framework for asserting the privacy of deceased individuals under the Privacy Act.

Recommendation 13 – Amend the Privacy Act to ensure that the definition of personal information extends to deceased individuals for a period of 30 years after death.

[33] See the *Privacy and Personal Information Protection Act 1998* (NSW), s4(3)(a) and the *Victorian Health Records Act 2001* (Vic). We note that the limit is set at 25 years in Tasmania, 5 years in the Northern Territory, and 'as far as is practical' in the ACT's Health Records (Privacy and Access) Act 1997.

[34] *Freedom of Information Act 1982* (Cth) s 47F; *Archives Act 1983* (Cth) s 33(1)(g).

[35] New South Wales Law Reform Commission (2019), *Access to digital records upon death or incapacity (Report No 147)*, NSWLRC, accessed 19 November 2020.

[36] See the Council of Attorneys-General (27 July 2020) *Communique*, CAG, accessed 19 November 2020.

Part 3: Flexibility of the APPs in regulating and protecting privacy

6. Is the framework of the Act effective in appropriately balancing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

3.1 While the definition of personal information sets out the scope of what is regulated by the Privacy Act, the APPs form the cornerstone of the privacy protection framework.[37] The APPs are legally binding principles, which provide entities with the flexibility to take a risk-based approach to compliance, based on their particular circumstances, including size, resources and business model, while ensuring the protection of individuals' privacy.

3.2 The principles-based approach therefore enables the APPs to be scalable for entities of various sizes and capabilities across the economy and to be adapted to different acts and practices of those entities. The APPs are also technology neutral, applying equally to paper-based (offline) and digital environments. This allows for greater 'future-proofing', which is intended to preserve the relevance and applicability of the APPs, in a context of continually changing and emerging technologies.[38]

3.3 As outlined in the Objectives section of this submission, a key object of the Privacy Act is to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities.[39] The principles-based approach of the APPs sets overall objectives that must be met to enable APP entities to achieve this balance. By contrast, rules-based regulation is comparatively rigid. Detailed rules impose requirements that are not always appropriate for all entities regulated by the relevant scheme and, further, they do not always cover all of the entities that are intended to be regulated.[40]

3.4 The GDPR similarly enables a flexible approach to compliance based on key principles. Guidance from the United Kingdom Information Commissioner's Office (UK ICO) states:

> Every organisation is different and there is no one-size fits-all answer. Data protection law doesn't set many absolute rules. Instead it takes a risk-based approach, based on some key principles. This means it's flexible and can be applied to a huge range of organisations and situations, and it doesn't act as a barrier to doing new things in new ways.[41]

---

[37] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 52.

[38] OAIC (July 2019) *Australian Privacy Principles guidelines* [online document], OAIC, accessed 26 November 2020.

[39] *Privacy Act 1988* (Cth) s 2A.

[40] ALRC (2008) *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, ALRC, Australian Government, accessed 26 November 2020.

[41] UK ICO (n.d.) *Guide to Data Protection* [online document], accessed 26 November 2020.

3.5 While the principles-based approach is the foundation of Australia's privacy protection framework, the Privacy Act also contains mechanisms that allow the APPs to be supplemented by more specific rules in regulations or other legislative instruments in appropriate circumstances.

3.6 The OAIC considers that the principles, risk-based framework of the Privacy Act continues to be the most effective regulatory model for the protection of personal information in Australia. This approach is also consistent with other data protection laws around the world, including the GDPR, as outlined above.

3.7 However, as noted in the Objectives section, the OAIC considers that the review presents an opportunity to place greater emphasis in the Privacy Act on the rights of individuals and the obligations of entities to protect those rights. The recommended enhancements outlined in this section are designed to achieve this and to resolve ambiguities in the existing APPs.

3.8 The OAIC's recommendations are also aimed at maintaining the flexibility and scalability of the existing principles-based privacy framework, while providing the Commissioner with enhanced abilities to make legally binding instruments to address areas that either require further certainty or specificity in the law, or that merit specific privacy protections.

Legislative flexibility to adapt the APPs

3.9 While the OAIC considers the principles-based approach to the APPs should be retained, we acknowledge that there may be areas that require further certainty or specificity in the law, or that merit specific privacy protections.

3.10 The Issues Paper outlines two existing mechanisms that may be used to prescribe specific requirements or treatments in relation to certain classes of entities, information, or acts and practices. Exempt entities (or classes of entities) or acts and practices can be brought within the regulatory remit of the APPs through delegated legislation, where there is a public interest in doing so.[42] Additionally, Part IIIB of the Act creates a framework for the development, registration and variation of codes of practice about information privacy, called APP codes.

3.11 The Issues Paper notes that the Commissioner may develop an APP code if the Commissioner considers that it is in the public interest to do so. However, this power can only be exercised if the Commissioner has requested a code developer to develop an APP code and the request has not been complied with, or the Commissioner has decided not to register the APP code that was developed as requested. The Commissioner may then develop and register an APP code only after these procedural steps have been followed.[43]

[42] *Privacy Act 1988* (Cth), Div 1, Pt II.

[43] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 4.

3.12 The factors that will be taken into account by the Commissioner in identifying an appropriate code developer include whether an entity, group of entities, or association or body:

- has the capacity to develop a code including whether they have the resources and expertise, and
- is generally representative of the entities in the sector or industry to which the code will apply.[44]

3.13 In certain circumstances, it would be challenging to identify an appropriate entity or group of entities that meet the above criteria. For example, it may be necessary to develop a code to cover a particular activity that is being engaged in across a broad sector of the economy, such as the online sector, that is made up of a diverse range of entities. In these circumstances, it may be difficult to identify a code developer (or developers) that is generally representative of the entities that are intended to be captured. It may also be challenging to identify a developer/s with adequate resources and expertise to develop an APP code that is intended to capture a wide range of entities of various sizes and with different personal-information handling practices.

3.14 Further, a situation may arise where an APP code needs to be developed as a matter of urgency. However, under the existing APP code provisions in the Privacy Act, there are prescribed minimum timeframes that must be complied with during the development of a code. For instance, the Commissioner must provide a code developer a minimum period of 120 days to develop the code.[45] If the Commissioner is required to develop an APP code in the circumstances described above, a further consultation period of at least 28 days must occur.[46]

3.15 The OAIC considers that, in urgent circumstances, it would be beneficial if the Commissioner had the ability to expeditiously issue a temporary APP code where there is a clear public interest in doing so. Importantly, a temporary APP code would be in force for a limited period of time. For example, the response to the pandemic has necessarily required regulated entities to quickly implement new or changed information-handling practices. In these circumstances, a temporary APP code issued quickly in response to changing circumstances could assist affected entities by providing greater clarity and certainty around their privacy obligations. The OAIC notes that this approach aligns with recent amendments to New Zealand's privacy law, which enables the Privacy Commissioner to temporarily issue, amend or revoke a privacy code of practice in urgent circumstances where it is impracticable to follow the regular code-making procedures.[47]

---

[44] OAIC (September 2013) *Guidelines for developing codes* [online document], OAIC, accessed 26 November 2020.

[45] *Privacy Act 1988* (Cth), s 26E(4)(a).

[46] *Privacy Act 1988* (Cth), s 26G(3)(b).

[47] *Privacy Act 2020* (NZ), s 34. See also *Privacy Act 1988* (Cth), Div 2, Pt VI which sets out the process for making temporary public interest determinations.

3.16 Considering the above, the OAIC recommends that the existing APP code framework is amended to provide the Commissioner with greater flexibility and discretion to develop APP codes. Specifically, the framework should:

- enable the Commissioner to develop an APP code in the first instance (i.e. without having to first request a code developer to develop an APP code), and
- enable the Commissioner to issue a temporary APP code if it is urgently required and where it is in the public interest to do so, and
- retain the existing power which enables the Commissioner to request that a code developer develop a code, and
- enable the Commissioner to intervene at any point in the code development process where an APP code is being developed by a code developer if satisfied it would be preferable for the Commissioner to develop the code.

3.17 We consider the proposed amendments would provide the Commissioner with greater flexibility to develop codes, thereby ensuring that greater specificity can be given to the APPs where required, emerging privacy risks can be addressed, and additional clarity and certainty can be provided to regulated entities in exigent circumstances. Enabling the Commissioner to develop a code in the first instance would also address the challenges associated with identifying a code developer where a code is intended to apply to a wide range of entities and personal-information handling activities. The additional discretionary power for the Commissioner to intervene in circumstances where a code developer is developing a code will enable the OAIC to retain leadership over the code development process and ensure any APP code meets its intended objectives.

3.18 In addition, a general rule-making power would provide the Commissioner with the ability to provide the regulated community with further certainty in how to address certain privacy risks and concerns, by providing greater specificity and particularisation around the application of the APPs where necessary. This is similar to the model under the Consumer Data Right regime, which enables the ACCC to issue legally binding rules to provide greater detail around the application of the CDR regime.[48] Accordingly, the OAIC recommends that the code-making powers in the Privacy Act are supplemented by a general power for the Commissioner to issue legally binding rules about the application of the APPs.

3.19 The Commissioner may also currently make guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals.[49] The OAIC has developed APP guidelines, which set out the Commissioner's interpretation of the

[48] The OAIC notes that, in October 2020, draft legislation to amend Part IVD of the *Competition and Consumer Act 2020*, which will reallocate rulemaking functions for the CDR system to the Treasury, was released for public consultation. At the time of writing this submission, the consultation had concluded but the draft legislation had not been introduced to Parliament.

[49] *Privacy Act 1988* (Cth), s 28(1)(a).

APPs, including the matters that may be taken into account when exercising functions and powers relating to the APPs.

3.20 However, these guidelines are not legally binding nor is an entity required to have regard to them when considering how to comply with the Act. By contrast, under s 93A of the *Freedom of Information Act 1982* (FOI Act) the Commissioner may, by instrument in writing, issue guidelines for the purposes of the Act, which an agency must have regard to when performing a function or exercising a power under the Act.[50]

3.21 The OAIC recommends providing further certainty for entities around their compliance obligations by elevating the status of the APP guidelines through a new provision that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

Recommendation 14 – Amend the APP code framework in Part IIIB of the Privacy Act to provide the Commissioner with greater flexibility and discretion to develop APP codes. The framework should:

- enable the Commissioner to develop an APP code in the first instance (i.e. without having to first request a code developer to develop an APP code), and
- enable the Commissioner to issue a temporary APP code if it is urgently required and where it is in the public interest to do so, and
- retain the existing power which enables the Commissioner to request that a code developer develop a code, and
- enable the Commissioner to intervene at any point in the code development process where an APP code is being developed by a code developer if satisfied it would be preferable for the Commissioner to develop the code.

Recommendation 15 – Supplement the code-making powers in Part IIIB of the Privacy Act with a general power for the Commissioner to issue legally binding rules about the application of the APPs.

Recommendation 16 – Include a new provision in the Privacy Act that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

[50] Section 93A(3) of the FOI Act provides that guidelines are not legislative instruments.

Safeguards in the APPs to prevent the misuse of sensitive information

35. Does the Act adequately protect sensitive information? If not, what safeguards should be put in place to protect against the misuse of sensitive information?

3.22 In accordance with the OAIC's APP guidelines, APP entities need to consider the sensitivity of information that they are handling when determining the reasonable steps that they should take to comply with many of the APPs.[51] The OAIC will also consider whether a matter involves sensitive information as a factor in determining whether to take regulatory action.[52]

3.23 The OAIC's recommendation 6, to clarify that inferred information is captured under the definition of personal information (which includes sensitive information), will ensure that existing Privacy Act protections apply to inferred sensitive information. These include notice requirements under APP 5 and the requirements to seek consent when collecting this information under APP 3.

3.24 The OAIC is also considering whether there are categories of information which are considered sensitive by the community that deserve additional protections. An important example of this is location information, which can be used to profile individuals and is difficult to make anonymous.[53] Location information is particularly intrusive in that beyond showing where an individual has been, it can also reveal sensitive information about them such as information about their health or religious beliefs. The OAIC recommends, however, that this issue be dealt with by way of a full or partial prohibition, which is a stronger protection than making this data sensitive information (See Recommendation 40).

3.25 In addition, this submission also recommends the introduction of additional protections to apply to the misuse of sensitive information. These include:

- Recommendation 31 – Strengthen notice and consent requirements in the Privacy Act to address the limitations in these mechanisms, but preserve the use of consent for high privacy risk situations, rather than routine personal information handling.
- Recommendation 37 - Introduce fairness and reasonableness obligations into APPs 3 and 6.
- Recommendation 50 – Introduce several amendments to the enforcement mechanisms under the Privacy Act to ensure that the Commissioner has the correct regulatory tools that provide a credible deterrent against privacy infringements.

---

[51] OAIC (July 2019) *Australian Privacy Principles guidelines* [online document], OAIC, accessed 26 November 2020.

[52] OAIC (May 2018) *Privacy regulatory action policy* [online document], OAIC, accessed 26 November 2020.

[53] Anna Johnston (12 November 2020) 'Location, location, location: online or offline, privacy matters', *Salinger Privacy blog*, accessed 26 November 2020.

Two-thirds (62%) of Australians are uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser. This is higher among females, with two-thirds (65%) feeling uncomfortable compared to males (59%), and highest among older Australians, with three-quarters (72%) feeling uncomfortable compared to only 55% of those aged 18-49 years.[54]

Since the outbreak of COVID-19, Australian's concerns around location information and privacy risks have also increased. Location tracking has become the third biggest privacy risk where it was previously ranked fifth.[55]

Strengthening the APPs

APP 3 – additional obligations for collection from third parties

3.26 APP 3.6 requires personal information about an individual to be collected from that individual unless it is unreasonable or impracticable to do so.

3.27 However, as the Issue Paper observes, it does not place any express obligations on APP entities that rely on this exception to consider the circumstances of the initial collection and ensure that it was in compliance with the requirements in APP 3.

3.28 Personal information is being increasingly shared between third parties (for example, data brokers or through the ad-tech ecosystem) or scraped off social media. As individuals are increasingly excluded from these activities, they are not afforded the opportunity to refuse to participate in the collection (for example, if the individual would not have given up the information if asked directly) and there is an increased likelihood that the information collected will not be accurate, up-to-date, complete and relevant. In these circumstances, there is a need to encourage entities to give greater focus to the context of the original collection and take reasonable steps to satisfy itself that the information was collected in accordance with the requirements of the APPs.

The OAIC has identified instances where the collection of personal information from third parties or public sources has resulted in detriment for individuals in circumstances where it may be readily apparent, or the OAIC later identifies, that this information was collected by unfair or unlawful means:

Collection from third parties – An APP entity purchased personal information from a third party without making enquiries as to how the information had been initially collected. The information was later identified to have been initially collected by unfair or unlawful means.

[54] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 79

[55] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 105

Collection from public sources – An APP entity collects personal information, such as photographs of individuals, from a public internet website where it is reasonably apparent that this information was collected for publication by unfair or unlawful means. This information can then be used to target individuals.

Collection from public sources – An APP entity collects personal information from the dark web or from a public internet website where it appears reasonably apparent that this information was likely published by the perpetrator of a data breach.

3.29 Even with the proposed fairness and reasonableness requirements in Part 6 below, the law would benefit from greater clarity as to the extent these requirements would extend to the original collection in circumstances where personal information has not been collected directly from an individual.

3.30 The OAIC recommends that the Privacy Act is amended to introduce a due diligence requirement that, where personal information was not collected directly from an individual, an APP entity must take reasonable steps to satisfy itself that the information was originally collected in accordance with APP 3.

3.31 This provision creates additional safeguards for individuals where an APP entity collects personal information from a third party. This could be achieved by making a minor addition to APP 3.6:

> (c) If the APP entity does not collect the information from the individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with this principle.

3.32 This obligation would support the OAIC's recommendation 37 to require APP entities to only collect, use or disclose information fairly and reasonably.

3.33 The Commissioner's guidance could then set out examples of reasonable steps that an APP entity can take to satisfy itself that the information was originally collected from individuals in accordance with APP 3. These could include making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with the APPs.

Recommendation 17 – Amend APP 3.6 to require an APP entity to take reasonable steps to satisfy itself that personal information that was not collected directly from an individual was originally collected in accordance with APP 3.

APP 7 – Direct marketing

37. Does the Act strike the right balance between the use of personal information in relation to direct marketing? If not, how could protections for individuals be improved?

3.34 APP 7 sets out specific requirements where personal information is used for direct marketing purposes. Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services.[56]

3.35 The explanatory memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 notes that direct marketing is addressed separately within a discrete principle rather than as a kind of secondary purpose under APP 6 because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing.[57]

3.36 However, it should be noted that APP 7 only applies to certain methods of direct marketing. APP 7.8 states that the principle does not apply to the extent that the *Interactive Gambling Act 2001*, the *Do Not Call Register Act 2006* or the *Spam Act 2003* applies. In other words, APP 7 will only apply to direct marketing communications that are not covered by these Acts. This means, in practice, APP 7 will generally only apply to:

- direct marketing calls or faxes where the number is not listed on the Do Not Call Register, or the call is made by a registered charity
- direct marketing by mail (whether sent by post or hand delivered) and door-to-door direct marketing
- targeted marketing online (including on websites and mobile apps), but only if personal information is used or disclosed to target that marketing.

3.37 While the OAIC acknowledges the policy objective behind APP 7, the privacy risks associated with direct marketing have changed significantly since 2012. Further, the OAIC considers that the current approach, which means entities must comply with different obligations for different channels, creates regulatory fragmentation and confusion. The Australian Communications and Media Authority (ACMA) has also called for broader reform of the regulatory framework for unsolicited communications.[58]

3.38 The protections contained in APP 7 apply to the use and disclosure of personal information for direct marketing. As noted in Part 2, new developments in the way that data is handled makes it increasingly difficult to draw a bright line between personal

[56] OAIC (July 2019) *Australian Privacy Principles guidelines* [online document], OAIC, accessed 26 November 2020.

[57] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, 81.

[58] ACMA (May 2018) *Report on industry self-regulation of commercial electronic messages, the Do Not Call Register and the Integrated Public Number Database*, ACMA, Australian Government.

and non-personal information in the online environment. APP 7 is also expected to apply to increasingly complex methods of targeted marketing involving multiple parties in the online environment using cookies and other online identifiers. This enables the individual user of a device to be targeted to receive a particular ad, offered personalised content or recommendations, sent political messaging, or subjected to automated decisions such as differential pricing.

3.39 The application of APP 7 in the circumstances described above is not clear, nor is it clear which entity or entities in the ad tech ecosystem are responsible for compliance with APP 7 requirements.

3.40 Accordingly, the OAIC considers that APP 7 is no longer fit for purpose and recommends that APP 7 should be repealed. If APP 7 was repealed, the use and disclosure of personal information for direct marketing purposes and related activities would then be subject to the existing requirements contained in APP 6. That is, an entity could only use or disclose personal information for direct marketing with consent, or if one of the exceptions in APP 6.2 applies. This approach would be enhanced by the OAIC's recommendation 37 to introduce a requirement for APP entities to use and disclose personal information 'fairly and reasonably'.

3.41 In addition, to ensure that individuals have the ability to request not to receive direct marketing as currently required by APP 7, the OAIC recommends that the right to object (discussed below) includes an absolute right for individuals to object to the use and disclosure of their personal information for direct marketing purposes. That is, an entity would not be able to rely on any of the proposed exceptions to the right to object to continue to use and disclose an individual's personal information for direct marketing. This is consistent with the approach taken under the GDPR, which equips data subjects with an absolute right to stop their data being processed for direct marketing purposes. To ensure the existing protections of APP 7 are preserved, the right to object should also include the ability for individuals to request an organisation to identify the source of the personal information that is uses or discloses for direct marketing. An entity should be required to notify the individual of its source, unless this is unreasonable or impracticable.

Recommendation 18 – Repeal APP 7 and rely on the existing use and disclosure requirements in APP 6 for direct marketing activities.

Recommendation 19 – Ensure that the proposed new right to object includes:

- an absolute right for individuals to object to the use and disclosure of their personal information for direct marketing purposes, and
- the ability for individuals to request an organisation to identify the source of the personal information and the organisation should be required to notify the individual of its source, unless this is unreasonable or impracticable.

APP 11 – Security of personal information

43. Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?

3.42 APP 11.1 requires APP entities to take reasonable steps to protect the personal information that they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

3.43 The security obligations in APP 11 encompass personal information held both online and offline and require entities to protect personal information against a wide range of threats, including cyber security threats, human error, theft, inadvertent loss of physical or electronic information, or information being improperly used or accessed by employees or external third parties.

3.44 The principles-based framing of APP 11 enables entities to scale their responsibilities proportionally to the volume and type of personal information that they hold. Where the volume or sensitivity of personal information held by an entity increases, so too will the expectations placed upon the entity to protect that information. In particular, there is an expectation that in complying with APP 11, entities will actively monitor their risk environment for emerging threats and take reasonable steps to protect personal information by mitigating those risks.

3.45 Similarly, when considering what steps are reasonable under the Privacy Act, APP 11 requires entities to take account of the broader security environment in which they operate and apply any security obligations imposed under other frameworks.

3.46 Under APP 11, entities must also take steps beyond technical security measures in order to protect and ensure the integrity of personal information throughout the information lifecycle, including implementing strategies in relation to governance, internal practices, processes and systems, and dealing with third party providers.

3.47 The framing of APP 11 acknowledges that security threats and the responsibilities of entities to respond to those threats are not static and require consideration of obligations that go beyond those set out in the Privacy Act. Requiring entities to take 'reasonable steps' to secure personal information can help to ensure that the security standards applied are commensurate to the risk of the data handling activity. A café that needs to secure hard copy contact details presents a different risk profile to a GP office or a multinational corporation.

3.48 The OAIC therefore considers that it is important to retain the principles-based approach in APP 11, to ensure that entities are able to apply their obligations flexibly to respond to emerging threats, new and broad obligations, and the specific risk environment that they operate in.

3.49 The need for flexibility in responding to security threats is noted in the Government's 2020 Cyber Security Strategy, which says, in relation to a proposed new regulatory framework for critical infrastructure and systems of national significance:

> One size does not fit all. The framework will balance objectives for cyber, physical, personnel and supply chain protections across all sectors, while recognising sector-specific differences. This is why the framework will be built around principles-based outcomes, underpinned by guidance and advice proportionate to the risks and circumstances in each sector.

3.50 As acknowledged in the ALRC Report, the principles-based approach of the APPs 'does not foreclose the possibility of technology specific regulation or legislative instruments in certain circumstances'.

3.51 The OAIC supports opportunities to enhance the current privacy framework through the introduction of additional and specific measures in relation to information security. The OAIC considers that Recommendations 14 and 15 to enhance the Commissioner's code-making powers and introduce a new general power for the Commissioner to issue legally binding rules is the most appropriate way of achieving this outcome.

3.52 These powers could be used by the Commissioner to further enhance requirements that prevent information loss attributable to specific threats, such as cyber intrusion, specific industries, or in relation to specific technologies. For example, as per Recommendation 15, the Commissioner could use a new legally binding rule-making power to develop rules for a specific industry to provide greater clarity around the 'reasonable steps' that they should take to meet their compliance obligations under APP 11.1. This could be modelled on the approach under Article 32 of the GDPR, which sets out specific measures to ensure a level of security appropriate to the risk, including (as appropriate): the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

3.53 There is already precedent for this approach, with existing sector specific frameworks used to add specificity and clarity in relation to certain parts of the economy. For instance, there are particular privacy security requirements relating to credit information and credit eligibility information,[59] and tax file number information.[60] There are specific personal information security requirements relating to My Health Records and retained data under the *Telecommunications (Interception and Access) Act 1979* (Cth).[61] Further, there are specific information security requirements relating to 'CDR data' under the Consumer Data Right system. These may differ across sectors and classes of persons.[62]

---

[59] *Privacy Act 1988* (Cth), Part IIIA.

[60] Privacy (Tax File Number) Rule 2015, r 11.

[61] My Health Records Rules 2016, r 44; *Telecommunications (Interception and Access) Act 1979* (Cth), s 187LA.

[62] Under s 56EO(1) of the *Competition and Consumer Act 2010* (Cth) entities must take the steps specified in consumer data rules to protect CDR data. The consumer data rules may prescribe different information security requirements for different sectors and classes of persons in the CDR system (for example, see s 56BB(a) of the *Competition and Consumer Act 2010*).

3.54 Proposals to introduce a certification framework under the Privacy Act would also support entities to meet their APP 11 security obligations. This proposal is considered further in Part 7 below. For example, an accreditation scheme has been created under the CDR model, which provides a safe mechanism for individuals and businesses to direct data holders to share their data with accredited third parties.

Recommendation 20 – Introduce enhanced code-making powers and new powers for the Commissioner to issue legally binding rules to enable the Commissioner to make sector- or threat-specific legislative instruments that support the principles-based approach in APP 11.1.

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

3.55 APP 11.2 requires entities to take such steps as are reasonable in the circumstances to destroy or de-identify personal information when it is no longer needed for any purpose for which it may be used or disclosed under the APPs (and if the information is not contained in a Commonwealth record or legally required to be retained by the entity).

3.56 Destroying and de-identifying personal information that is no longer needed is an important strategy to help mitigate security risks. For example, holding large amounts of personal information for longer than is needed may increase the risk of unauthorised access by staff or contractors. 'Honey pots' containing vast amounts of valuable data may increase the risk that an entity's information systems may be hacked.[63]

3.57 The principles-based framing of APP 11.2 enables entities to scale and tailor their approach to destruction and de-identification based on their circumstances. Similar to the considerations outlined above for APP 11.1, more rigorous steps may be required by an entity to destroy or de-identify personal information based on the amount or sensitivity of its personal information holdings.

3.58 The OAIC considers that the principles-based approach to APP 11.2 should be retained, rather than prescribing greater requirements for entities to destroy or de-identify personal information. Additional requirements may not be applicable or appropriate in all circumstances given entities hold personal information for a variety of different purposes. This necessarily means there is no 'one size fits all approach', as personal information may need to be retained longer by some entities than others.

3.59 As outlined at Recommendations 14 and 15, the proposed enhancements to the Commissioner's code-making powers and the introduction of a new power to make legally-binding rules would enable the Commissioner the flexibility to place greater

[63] OAIC (March 2018) *Guide to data analytics and the Australian Privacy Principles* [online document], OAIC, accessed 26 November 2020.

requirements around the destruction or de-identification of personal information where appropriate. For example, rules could be issued that set standards around the destruction or de-identification of personal information for a particular industry.

Recommendation 21 – Introduce enhanced code-making powers and new powers to make legally-binding rules under the Privacy Act to enable the Commissioner to set requirements or standards for destruction and de-identification by legislative instrument where appropriate.

Individual rights under the APPs

3.60 Individual privacy rights are an important component of privacy self-management and, more broadly, facilitate the enjoyment of other rights and freedoms including freedom of association, thought and expression, as well as freedom from discrimination.[64] As noted above, effective rights for individuals to exercise control over their personal information are also crucial build confidence in the privacy framework; a necessary precondition to create the trust and confidence in entities handling personal information to carry out their activities.

3.61 To this end, the existing rights of access (APP 12) and correction (APP 13) are well-established rights in Australia's privacy framework. The proposed additional right of erasure and right to object are intended to complement the existing rights under the Act and are also tied to the broader obligations under the APPs. For example, entities already have an existing obligation under APP 11.2 to destroy or de-identify personal information when it is no longer necessary for any purpose for which it may be used or disclosed under the APPs. Accordingly, entities should already have practices, procedures and systems in place to give effect to this requirement. The right to erasure enables individuals to initiate this process on request.

3.62 This section makes recommendations to enhance the existing rights in the APPs and introduce new rights to further support privacy self-management.

Existing rights – access and correction

45. Should amendments be made to the Act to enhance: a. transparency to individuals about what personal information is being collected and used by entities? b. the ability for personal information to be kept up to date or corrected?

3.63 APP 12.1 provides that if an APP entity (including an agency) holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

3.64 APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not

[64] OAIC (n.d) *What is privacy?*, OAIC website, accessed 26 November 2020.

misleading, having regard to the purpose for which it is held. The requirement to take reasonable steps applies in two circumstances:

- where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or
- where an individual requests an APP entity to correct their personal information.

3.65 APPs 12 and 13 operate alongside, and do not replace, other informal and legal processes by which an individual can be provided access to personal information, or by which they may seek correction of their personal information. For example, the FOI Act provides a complementary procedure that gives individuals a legally enforceable right of access to documents (under Part III) and the right to request correction or update (Part V) of their personal information in agency records or the official documents of a minister. It is also open to individuals to seek access or correction of their personal information informally through administrative processes.

3.66 The intended benefits behind providing individuals with an alternative means of accessing personal information held by Australian Government agencies under APP 12 include enabling agencies to process requests for personal information promptly and at the lowest reasonable cost, by allowing agencies to focus on personal information rather than documents (to which exemptions under the FOI Act might otherwise apply). The Privacy Act also provides the ability to seek remedies where access to personal information is denied in breach of the Act. In contrast, a denial of access under the FOI Act permits an application for internal and external review of the administrative decision.

3.67 As outlined above, an individual may request that an entity corrects personal information that it 'holds' about them. An entity 'holds' personal information if 'the entity has possession or control of a 'record' that contains the personal information. [65] Accordingly, entities are not required to correct personal information that they do not have possession or control of (for example, personal information that has been published on social media).

3.68 The OAIC recommends that the right to request correction of personal information should extend to require further steps to be taken in relation to personal information that is no longer 'held' by the entity such as publicly available information that has been posted online. In addition to the proposed right of erasure discussed further below, this will provide individuals with greater control of their personal information and mitigate the risk of harm that may arise from incorrect information being widely available online.

Recommendation 22 – Extend the right to request correction of personal information in APP 13 to personal information that is no longer 'held' by the entity.

[65] *Privacy Act 1988* (Cth), s 6(1).

New rights

46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

Right to erasure

3.69 The OAIC supports the introduction of a right to enable individuals to request the erasure of their personal information into the Act, subject to some exceptions.

3.70 As recommended in the DPI report, under a right to erasure, APP entities would be required to comply with a request to erase personal information without undue delay, unless there is an overriding reason for the information to be retained.[66]

3.71 This would bring the Australian privacy framework into line with other international jurisdictions including the United Kingdom and European Union. It would also be consistent with the direction taken by other domestic legislative frameworks, such as the Consumer Data Right and My Health Records systems, which allow individuals to request the deletion of their data in certain circumstances.[67]

3.72 The OAIC's 2020 ACAPS results demonstrated that there is also community support for the introduction of a right to erasure. The survey found that 84% of respondents would like to have increased rights around certain issues such as asking businesses to delete information, while 64% of respondents want the right to ask a government agency to delete their personal information.

3.73 The potential for implementation challenges and regulatory impact would need to be carefully considered when determining the most appropriate scope for a new right to erasure to ensure the protection of individuals' privacy alongside the interests of entities in carrying out their functions and activities. These challenges have been highlighted in the GDPR context, for example, in relation to the requirement that an entity that is obliged to erase personal data must inform other organisations of the erasure of personal data where that data has been disclosed to others or has been made public in an online environment.[68] Although this is qualified by a reasonable steps test, and an entity may take into account implementation cost in discharging

[66] Issues paper, p. [55], citing Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 470.

[67] Section 56BAA of the *Competition and Consumer Act 2010* (Cth), which provides that the Consumer Data Right Rules must include a requirement on an accredited data recipient to delete all or part of the CDR data where requested by a consumer; and s 17(3) of the *My Health Records Act 2012* (Cth), which requires the destruction of records containing health information in a My Health Record upon request by the individual.

[68] Article 17(2) and Recital 66 of the GDPR.

this obligation, we understand this requirement may pose technical, cost and other resource challenges for entities.[69]

3.74 The OAIC considers that a right to erasure would complement APP 11.2, which requires APP entities to destroy or de-identify personal information that they no longer need. The processes and procedures that APP entities have in place to meet this obligation would ease the burden of complying with a new right of erasure.

3.75 The OAIC recommends that the right to erasure should apply to personal information that is no longer 'held' by an entity (for example, publicly available information on social networks). This would extend the application of this right to the online environment. However, the obligation to erase personal information, and to notify others of an erasure request where the entity has made the personal information public, should be subject to appropriate exceptions.

3.76 The OAIC recommends that the right to erasure should include the following key features, as a minimum:

- The exceptions recommended in the DPI report ('unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason').[70]
- An exception for 'frivolous or vexatious' requests, consistent with APP 12,[71] or a similar threshold, for example 'manifestly unfounded or excessive requests, consistent with the GDPR.[72]
- An exception for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing, consistent with the GDPR.[73]
- An appropriate timeframe within which APP entities must respond to erasure requests, for example consistent with APP 12[74] or the GDPR.[75]

---

[69] DataGrail, *The Age of Privacy: The Cost of Continuous Compliance – Benchmarking the Ongoing Operational Impact of GDPR and CCPA* (Report, February 2020) 5; European Network and Information Security Agency, *The right to be forgotten – between expectations and practice* (Report, October 2011) 8.

[70] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry* (Final Report, June 2019) p. 470.

[71] Under APP 12.3(c), entities are not required to give individuals access to personal information to the extent that the request is frivolous or vexatious.

[72] Article 12(5) of the GDPR provides that a controller may refuse to act on an erasure request from a data subject where the request is 'manifestly unfounded or excessive, in particular because of [its] repetitive character'.

[73] For this exception to apply under Article 17(3)(d) of the GDPR, such processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes must be done in accordance with Article 89(1), which requires such processing to be subject to appropriate safeguards.

[74] Under APP 12.4, an APP entity must respond to access requests within: 30 days (for an agency); or a 'reasonable period after the request is made' (for an organisation).

[75] Recital 59 of the GDPR provides that '[t]he controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month'. See also Article 17(1).

3.77 In addition, the OAIC recommends that any right to erasure be complemented by:

- A requirement for APP entities to notify individuals of their ability to request the erasure of their personal information. This could be modelled on similar requirements in Article 13 of the GDPR.
- A right for individuals to object to the handling of their personal information for specific purposes. Under a right to object, an individual may stop or prevent certain types of data processing without requiring the erasure of their personal information, which is important where individuals wish to continue using a service. This right should apply prospectively, not retrospectively.

Right to object

3.78 While the 'right to object' is not explored in the Issues Paper, the OAIC considers that it is an important reform that supports the ability of individuals to have control over their personal information.

3.79 Under a right to object, individuals would be able to object to the handling of their personal information for certain purposes at any time. This would allow individuals to stop APP entities from handling their personal information, unless an exception applies.

3.80 Individuals are provided with a right to object under Article 21 of the GDPR. This includes an absolute right to object to processing for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.[76] Upon receiving an objection to processing for direct marketing, the organisation must cease processing of the data for that purpose from that time onwards.[77] It also includes limited rights to object to processing on several other grounds, subject to exceptions.[78]

3.81 As outlined above, a right to object would also complement a right to erasure by allowing an individual to stop certain types of data processing without requiring the erasure of their personal information, which is important where individuals wish to continue using a service. The OAIC's 2020 ACAPS results demonstrated that there is community support in this regard: 77% of respondents would like the right to object to certain data practices while still being able to access and use the service.

---

[76] Article 21(2) of the GDPR.

[77] Article 21(3) of the GDPR.

[78] There is a limited right to object to processing that is: necessary for the performance of a task carried out in the public interest or in the exercise of official authority (including profiling); necessary for the purposes of legitimate interests of the controller or a third party (including profiling). These limited rights do not apply where the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims: Article 21(1) of the GDPR.

There is a further limited right to object to processing for scientific or historical research purposes or statistical purposes, except where processing is necessary for the performance of a task carried out for reasons of public interest: Article 21(6) of the GDPR.

3.82 A right to object should also be considered as part of the OAIC's Recommendation 18 for the review to consider whether APP 7 (direct marketing) is still fit for purpose. A right to object, if formulated on similar terms to the GDPR right, would allow an individual to object not only to the handling of their personal information for direct marketing purposes. As outlined in the 'APP 7 – Direct marketing' section of this submission, APP 7 may be not be sufficient to mitigate the privacy harms posed by increasingly complex methods of targeted marketing in the current online environment, which may include profiling. The right to object, if implemented, would achieve the same outcome as APP 7 but go further, by not only allowing an individual to in effect 'opt out' of receiving direct marketing communications, but also requiring the APP entity to stop handling the personal information for that purpose.

3.83 The OAIC therefore recommends that a right to object is introduced into the Privacy Act, modelled off Article 21 of the GDPR as a starting point. In a similar vein to the GDPR right, the OAIC considers it appropriate for individuals to have an absolute right to object in relation to direct marketing, but a limited right to object in relation to processing on other grounds.

Recommendation 23 – Introduce a right to erasure that includes, as a minimum:

- the exceptions recommended in the DPI report
- an exception for 'frivolous or vexatious' requests, consistent with APP 12, or a similar threshold, for example 'manifestly unfounded or excessive requests, consistent with the GDPR
- an appropriate timeframe within which APP entities must respond to erasure requests, for example consistent with APP 12 or the GDPR, and
- extends to personal information that is no longer 'held' by an entity, and to notify others of the erasure request where personal information has been made public, subject to the exceptions outlined at point (a) above.

Recommendation 24 – Introduce a requirement for APP entities to notify individuals of their ability to request the erasure of their personal information. This could be modelled on similar requirements in Article 13 of the GDPR.

Recommendation 25 – Introduce a right to object that includes:

- an absolute right to object in relation to direct marketing
- a limited right to object in relation to processing on other grounds.

Recommendation 26 – Introduce a requirement for APP entities to notify individuals of their ability to object to the handling of their personal information, including the absolute right for individuals to object to the use and disclosure of their personal information for direct marketing.

Emergency Declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

3.84 APP entities are ordinarily required to comply with the APPs when handling personal information. When an emergency declaration is in force, Part VIA allows agencies and organisations to collect, use and disclose personal information about an individual impacted by an emergency for several purposes that may not otherwise be permitted under the APPs. Agencies and organisations will still need to comply with other obligations under the Privacy Act, including notice and information security requirements.

3.85 As noted in the Issues Paper, the explanatory memorandum to the Bill that introduced the emergency declaration provisions states:

> Part VIA of the Privacy Act was introduced to provide a clear and certain legal basis for the collection, use and disclosure of personal information about deceased, injured and missing Australians in an emergency or disaster situation in Australia or overseas... [The provisions] place beyond doubt the capacity of the Australian Government and others to lawfully exchange personal information in an emergency or disaster situation.[79]

3.86 As these provisions override the ordinary purposes for which personal information may be collected, used or disclosed under the APPs, the OAIC considers that it is appropriate that Part VIA is only relied upon in limited circumstances. The OAIC notes that in many cases, exceptions to APPs 3 and 6 would be sufficient to enable APP entities to collect, use or disclose personal information in emergency situations.[80]

3.87 The OAIC is not making recommendations about changes to the emergency declaration provisions at this stage. The OAIC will consider relevant information submitted by stakeholders as part of the Issues Paper consultation before making final recommendations on this issue.

3.88 However, the OAIC suggests that the Privacy Act review ensure that any amendments to these provisions are aligned across Government. In particular, the OAIC notes that the Government has committed to creating a new law concerning the declaration of

[79] Explanatory memorandum to the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006.

[80] The APPs allow for the collection, use or disclosure of personal information where a permitted general situations under s16A or a permitted health situation under 16B exists. For example, s16A this allows for the collection, use and disclosure of personal information where it is unreasonable or impracticable to obtain the individual's consent, and the APP entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to life, health or safety of an individual, or to public health and safety.

natural disasters[81] as a result of the recommendations made by the Royal Commission into National Natural Disaster Arrangements. These relevantly including that:

- Australian, State and Territory governments should restructure and reinvigorate ministerial forums with a view to enabling timely and informed strategic decision-making in respect of the response to, and recovery from, natural disasters of national scale or consequence[82]
- Australian, state and territory governments should ensure that personal information of individuals affected by a natural disaster is able to be appropriately shared between all levels of government, agencies, insurers, charities and organisations delivering recovery services, taking account of all necessary safeguards to ensure the sharing is only for recovery purposes.[83]

3.89 Part VIA allows for sharing of information from Commonwealth agencies to State & Territory government bodies. Information handling by State & Territory government bodies during an emergency, however, must be handled in accordance with the applicable laws in that jurisdiction.

3.90 These recommendations by the Royal Commission will promote an object of the Privacy Act to provide the basis for the nationally consistent regulation of privacy and handling of personal information. The OAIC's recommendation 3 suggests that the Council of Attorney-Generals could establish a working group to consider amendments to State and Territory privacy laws to ensure alignment with the Privacy Act. These recommendations could be considered in this forum.

[81] Henderson A & Hitch G (13 November 2020) 'Federal Government responds to bushfire royal commission, will create national state of emergency' *ABC News*, accessed 16 November 2020.

[82] The Royal Commission into National Natural Disaster Arrangements Report (2020) *The Royal Commission into National Natural Disaster Arrangements Report*, Australian Government, Recommendation 3.1.

[83] The Royal Commission into National Natural Disaster Arrangements Report (2020) *The Royal Commission into National Natural Disaster Arrangements Report*, Australian Government, Recommendation 22.2.

Part 4: Exemptions

4.1 As outlined in the Issues Paper, the Privacy Act currently includes exemptions in relation to small businesses, employee records, registered political parties and political acts and practices and journalism.

4.2 The protections provided by the Privacy Act therefore do not apply to the way that exempt entities handle personal information, including sensitive information. Importantly, this means that individuals have no means of recourse if their personal information is mishandled, and exempt entities are not required to notify individuals or the OAIC about eligible data breaches under the NDB scheme.

4.3 As noted in the Issues Paper, the exemptions were introduced in 2000 when the Privacy Act was extended to the private sector. The OAIC considers that the privacy risks that have emerged in the last 20 years have changed to the extent that it is no longer justifiable to exempt major parts of the economy from the operation of the Act. Personal and sensitive information held by small businesses, employers and political parties is not immune to the substantial risks that exist in the digital environment. The existence of the exemptions may also impact on the ability of overseas entities to transfer data to Australian entities.[84]

4.4 The OAIC therefore recommends removing the current exemptions in the Privacy Act relating to small businesses, employers and employee records and political parties. It is appropriate to consider more comprehensive privacy protections for all Australians, including through the NDB scheme, regardless of the type of entity that holds their information or particular purpose for which it is held. A more detailed explanation of this recommendation is included for each exemption below.

4.5 At this stage, the OAIC is not recommending the removal of the journalism exemption, however we will consider the submissions made to the review by other stakeholders and may revise this position in our future engagements with the review process.

Small Business Exemption

7. Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on small business?

8. Is the current threshold appropriately pitched or should the definition of small business be amended?

a. If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as

[84] Note that the predecessor to the European Data Protection Board, the Article 29 Working Party issued an Opinion that raised concerns that the exemptions under the Privacy Act meant that Australia could only be considered adequate if appropriate safeguards were introduced to meet the Working Party's concerns. See Article 29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. This issue is discussed further in the Overseas data flows section, below.

number of employees or value of assets or should the definition be amended in another way?

9. Are there businesses or acts and practices that should or should not be covered by the small business exemption?

10. Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?

a. If so, what obligations should be placed on small businesses?

b. What would be the financial implications for small business?

11. Would there be benefits to small business if they were required to comply with some or all of the APPs?

12. Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their personal information?

4.6 The OAIC considers that the small business exemption is no longer appropriate in light of the privacy risks posed by entities of all sizes and the regulatory uncertainty created by the application of the exemption.

4.7 As noted in the Issues Paper, the small business exemption was introduced in 2000 in recognition of the potentially unreasonable compliance costs for certain small businesses. These businesses were considered to pose little or no risk to the privacy of individuals.

4.8 The Issues Paper asks whether the exemption strikes the right balance between protecting the privacy rights of individuals and avoiding unnecessary compliance costs on small business. This question implies that there is a trade-off between the protection of personal information and the cost to business. Rather, the OAIC considers that the protection of personal information is a vital part of doing business and creating a level playing field both between entities and individuals. Appropriate privacy protections create the consumer trust and confidence needed to support economic and social engagement with the product or service, regardless of an entity's size.

4.9 The small business exemption does not apply to specific business types, listed in ss 6D(4)-(9), recognising that these types of business were seen to pose a higher privacy risk at the time. However as noted in the Issues Paper, there is a lack of certainty about which small businesses are brought into the Privacy Act, particularly in relation to businesses that trade in personal information.

4.10 There is also confusion and concern in the community about the application of the Privacy Act to these entities.

The OAIC's 2020 ACAPS results found that 85% of respondents either mistakenly believed that the Privacy Act applied to small Australian businesses or did not know whether small Australian businesses were covered.

The survey also found that this exemption runs counter to community expectations, with 71% of respondents considering that small businesses should be covered by the Privacy Act.[85]

4.11 Small businesses are now increasingly collecting, holding and handling personal information in connection with their activities and in order to deliver their services. However, as at 30 June 2019, small businesses with a turnover of $3 million or less comprised 95.2% of the 2,375,753 businesses actively trading in the Australian economy.[86] The OAIC receives hundreds of enquiries and complaints each year about the conduct of small business operators, with the highest numbers of complaints relating to real estate agencies, property management businesses (property/construction/architects/surveyors) and professional services firms, including legal, accounting and management services.

A common complaint received by the OAIC is where an entity discloses an individual's personal information (which can include the name and address of the individual) in response to a negative review of the business. The information disclosed sometimes include sensitive information. The OAIC is often unable to address these matters as the respondent is a small business operator.

In another case, the personal information of an individual involved in a family violence dispute was disclosed to the offender. As a result of the disclosure, the individual feared for their safety. The OAIC could not investigate the matter as the entity that disclosed the information was a small business operator under the Privacy Act.

In another case, an ICT provider held personal information on behalf of a business that was subject to a data breach. The ICT provider did not meet the $3 million threshold, destroyed evidence relating to the data breach and refused to cooperate with the OAIC.

4.12 The small business exemption is also an anomaly amongst international privacy laws. No other comparable international jurisdiction exempts small businesses from the coverage of privacy legislation. The small business exemption has proved to be one of the major issues for Australia in seeking adequacy under the GDPR, due to the lack of privacy requirements in relation to a large section of the economy. The recent decision of the Court of Justice of the European Union (the Schrems Decision) has highlighted the importance of EU Adequacy decisions as a means of enabling transfers of data from the EU to overseas jurisdictions.[87]

---

[85] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, pp. 58-60.

[86] Australian Bureau of Statistics, 8165.0 Counts of Australian Businesses, including Entries and Exits, Jun 2015 to Jun 2019, prepared for the OAIC in April 2020. This figure does not take account of entities that are treated as 'organisations' regardless of their turnover, by virtue of ss 6D(4)-(9), or small businesses that have opted in to the Privacy Act under s 6EA (650 businesses, as at 11 November 2020).

[87] *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems,* (2020) C-3111/18. The Schrems Decision found that where an EU entity was relying on standard contractual clauses under Article 46 of the GDPR,

4.13 The OAIC therefore considers that there is strong justification for removing this exemption, and recommends that all businesses, regardless of size and activity, are covered by the Privacy Act.

4.14 As noted above, the principles-based approach established by the Privacy Act enables the APPs to apply to entities across the economy. The APPs provide entities with the flexibility to take a risk-based approach to compliance, based on their particular circumstances, including size, resources and business model, while ensuring the protection of individuals' personal information. This means that the way that a small business complies with the APPs will be different to the way in which a large multinational corporation will comply.

4.15 The OAIC does not consider that it is sufficient to amend the definition of small business to introduce a new threshold, or to cover or exclude specific acts or practices of small businesses. Businesses of all sizes can pose privacy risks, regardless of their turnover, as demonstrated by the examples set out above. Likewise, new privacy risks are constantly emerging, and there is a risk that expanding the list of entities that are not considered to be 'small business operators' under s 6D of the Privacy Act will quickly become out of date. The OAIC considers that this approach would not be consistent with the flexible and technology neutral framework of the Privacy Act and does not support the community in knowing whether their information is required to be protected.

4.16 Similarly, the OAIC does not consider that it would be appropriate for small businesses to be required to comply with some, but not all, of the APPs. The APPs are structured to reflect the cycle that occurs as entities collect, hold, use, disclose, and destroy / de-identify personal information. In other words, the APPs are designed to protect personal information throughout the information lifecycle. Accordingly, individual APPs cannot be read, or apply, in isolation. A holistic approach to compliance with the APPs is required to give full effect to the privacy protection framework set out in the Act.

4.17 The OAIC has experience with assisting small business to achieve compliance with the Privacy Act, regardless of any human or financial resource limitations. The OAIC is therefore well placed to support small businesses to meet their compliance obligations should the Privacy Act be extended to these entities.

---

they must consider the broader environment of the overseas recipient, and the impact that might have on their ability to provide essentially equivalent protections. The Schrems Decision is likely to have implications for the international flow of data because it requires a rigorous assessment of not just the privacy frameworks, but also the broader cultural environment in which the transferred data is subject to determine whether essentially equivalent protections are provided. A formal EU Adequacy Decision would alleviate the need for EU and Australian entities to take further steps in assessing the effectiveness of the Article 46 GDPR transfer tool being used and considering whether additional safeguards are needed. The Schrems Decision is discussed further in the Overseas data flows section below.

Recommendation 27 – Remove the small business exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Employee records exemption

13. Is the personal information of employees adequately protected by the current scope of the employee records exemption?

14. If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

15. Should some but not all of the APPs apply to employee records, or certain types of employee records?

4.18 The OAIC supports the removal of the employee records exemption. As with the small business exemption, the OAIC considers that removing the exemption will address the risks posed to the personal information of employees and create benefits to employers by increasing trust and confidence in their personal information handling practices and addressing regulatory uncertainty about the scope of the exemption.

4.19 The OAIC considers that the most important policy objective is to ensure that an individual's personal information is protected to the same standard, whether they are employed in the public sector, or in the private sector.

The OAIC's 2020 ACAPS results show that 73% of Australians agree that businesses collecting work-related information about employees should be required to protect personal information in the same ways that government and larger businesses are required to.[88]

4.20 Employers often hold sensitive information about their employees, including health information, which is generally subject to a higher standard of protection under the Privacy Act. Exempting this information from protection poses a significant risk to the individuals the information is about.

An employee's personal information was mishandled and stolen from the respondent's offices. The personal information was then used to commit identity fraud. The OAIC could not investigate whether the personal information had been

[88] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 60.

appropriately secured by the respondent as the information was contained in an employee record.

The OAIC received a complaint that a former employer allegedly disclosed that the complainant had been suspended from their job through an autoreply email that was connected to their work address. The OAIC could not investigate this matter due to the employee records exemption.

4.21 The introduction of the employee records exemption was justified on the basis that the handling of employee records is better dealt with under workplace relations legislation. The OAIC acknowledges that it is important to ensure that there is not regulatory duplication, however the OAIC does not consider that the two frameworks are inconsistent. Record keeping requirements under other regimes complement the Privacy Act and should enable employers to easily meet their compliance obligations under the APPs.

4.22 The employee records exemption is limited in its scope, applying only to an organisation acting in its capacity as an employer or former employer of an individual, in relation to acts or practices that are directly related to the employment relationship and an employee record held by the organisation. Employers who are 'organisations' under the Privacy Act are therefore required to comply with the Act for all personal information handling that falls outside the scope of the exemption. As noted in the Issues Paper, a recent decision by a Full Bench of the Fair Work Commission found that the exemption will only apply once an employee record has been generated, meaning that the requirements of the APPs with regard to collection and notice currently continue to apply.[89]

4.23 The OAIC considers that it is likely to create a greater compliance burden for employers to determine when the Privacy Act does or does not apply to their particular personal information handling activity, than to have it apply to all the personal information that it holds.

4.24 As with the small business exemption, there is no comparable employee records exemption in international privacy jurisdictions.

4.25 As outlined in relation to the small business exemption, the APPs offer sufficient flexibility to businesses to take a risk-based approach to compliance, based on factors including their size and the number of employees that they have. It is important that all the APPs apply, given that they are designed to provide protections to personal information throughout the information lifecycle. The review should consider the exceptions in APP 12 in light of the removal of the employee records exemption, to ensure that they remain appropriate and fit for purpose in an employment context.

4.26 Further, the OAIC considers that the compliance costs for employers would be relatively low, given they will likely have obligations under the Privacy Act in relation

[89] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946; 286 IR 368.

to any other personal information handling activities they carry out as part of their business.

4.27 The Issues Paper raises concerns about an employer's ability to rely on the consent of an employee to the collection, use or disclosure of their personal or sensitive information, given the power asymmetry that may be found between employers and employees. The OAIC agrees that power asymmetries in any relationship affect the validity of consent, whether that is between employers and employees,[90] or in some circumstances, between businesses and consumers. This is a key limitation of consent, as outlined in Part 5, below. However, this limitation would not preclude an employer from being able to collect, use or disclose an employee's personal or sensitive information, where there is a genuine business need for it to do so. There are exceptions to the requirement for consent to the collection of their sensitive information in APP 3, for example, where the employee is required or authorised by law to collect this information. Similarly, an employer could use or disclose the personal information of an employee under APP 6 in situations where they did not have the express consent of the employee, for example, where the employee would have a reasonable expectation that the employer would use or disclose the information in a particular way. The OAIC has made a number of recommendations in this submission that seek to address the limitations of the consent model.

Recommendation 28 – Remove the employee records exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Political exemption

16. Should political acts and practices continue to be exempted from the operation of some or all of the APPs?

4.28 Political parties are neither government agencies nor commercial entities. They perform unique and essential roles in political recruitment, policy development and political socialisation and mobilisation. Political parties are the mechanisms that define electoral competition and political identification.

4.29 One view is that the processing of personal data by parties for the purposes of 'democratic engagement' is different to general personal information handling and

[90] The Article 29 Data Protection Working Group noted that when processing employees' personal data, consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence. Instead, processing may be necessary for the performance of a contract, in accordance with legal obligations imposed by employment law, or based on legitimate interest. See Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work - wp249, accessed on 19 November 2020.

the public interest in 'knowing the electorate' should allow a wide latitude to process personal data to educate and mobilise voters.

4.30 However, this assertion is being called into question. Parallels can be drawn between many activities of political parties and those of marketing organisations (for example, online and offline advertising, employing data analytics companies, using social media space, testing and retesting political messaging).

4.31 Modern political campaigns around the world have become 'data-driven' to consolidate existing support and target new voters and donors. Some campaigns create detailed profiles of individual voters to 'micro target' increasingly precise messages to increasingly refined segments of the electorate. Skilled data analytics tools were employed in the two elections won by Barack Obama in 2008 and 2012, leading to a general assumption that all campaigns must now be data-driven to be successful.

4.32 The effects of 'data-driven' elections have been apparent in countries where political parties are not covered by data protection laws. For example, the European Council noted that the Cambridge Analytica case demonstrates that data protection 'has become a key issue not only for individuals but also for the functioning of our democracies because it constitutes a serious threat to a fair, democratic electoral process and has the potential to undermine open debate, fairness and transparency'.[91]

4.33 This also illustrates how potential infringements on the right to protection of personal information could affect other fundamental rights, such as freedom of expression, freedom to hold opinions and to think freely without manipulation.

4.34 The OAIC has opposed the political parties exemption since its introduction, on the grounds that there are still few well-articulated policy reasons why the exemption should apply to political parties and political acts and practices, at least in its blanket form. There is also a risk that the exemption's effect on political transparency may damage Australia's system of representative democracy, as well as the public's trust in Australia's privacy protections.

The OAIC's 2020 ACAPS results revealed that 62% of the Australian public incorrectly believed that political parties were covered by the Privacy Act, with 74 % of respondents stating that political parties should be subject to the Act. These results indicate that there is also a disconnect with community expectations in this area.[92]

[91] European Commission, *Free and Fair elections: Guidance Document: Commission guidance on the application of Union data protection law in the electoral context; A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*, Brussels, 12.9.2018 COM(2018) 638 final.

[92] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 60.

Recommendation 29 – Remove the political parties exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

Journalism exemption

17. Does the journalism exemption appropriately balance freedom of the media to report on matters of public interest with individuals' interests in protecting their privacy?

18. Should the scope of organisations covered by the journalism exemption be altered?

19. Should any acts and practices of media organisations be covered by the operation of some or all of the APPs?

4.35 As outlined in the Issues Paper, the journalism exemption was introduced into the Privacy Act in recognition of the public interest in providing adequate safeguards for the handling of personal information and the public interest in allowing a free flow of information to the public through the media.

4.36 The exemption is limited to a media organisation's activities in the course of journalism and does not extend to the media organisation's other functions and activities, such as advertising, website functions, competitions and surveys or subscriptions. Any personal information handling that occurs in the course of these activities will be regulated by the Privacy Act.

4.37 The journalism exemption can be distinguished from the other exemptions in the Privacy Act, as it only applies to media organisations who have publicly committed to published privacy standards. Personal information handled in the course of journalism is therefore subject to some level of privacy protection and oversight, for example, by bodies such as the Australian Press Council or codes of practice overseen by the Australian Communications and Media Authority. The journalism exemption is also consistent with other global privacy legislation, including New Zealand, Canada and the GDPR.

4.38 The OAIC considers that it may be appropriate to introduce enforceability requirements in relation to the oversight bodies of media organisations by shifting their operation to an external dispute resolution (EDR) scheme model. They could then be recognised under s 35A as the Privacy Act, thereby enabling a greater level of oversight by the Commissioner.

4.39 The OAIC will consider relevant information submitted by stakeholders as part of the Issues Paper consultation before making any further recommendations about the journalism exemption.

Recommendation 30 – Introduce greater enforceability requirements for the privacy safeguards covering media organisations. The review could consider whether the EDR scheme model is appropriate to achieve this outcome.

Part 5: Notice and consent

20. Does notice help people to understand and manage their personal information?

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

26. Is consent an effective way for people to manage their personal information?

5.1 Notice and consent provide foundational protections in privacy law across the world, including in the Privacy Act. Their purpose is to ensure that individuals have knowledge of, and choice and control over, how information about them is handled by organisations. Transparency obligations, through privacy policies (APP 1.3), collection notices (APP 5), and obligations to obtain consent when collecting sensitive information and handling personal information beyond the primary purpose of collection (APPs 3.3 and APP 6.1) are aimed at privacy self-management.

5.2 Privacy self-management empowers individuals to make choices and exercise control around their personal information. This can be a way of addressing power imbalances and information asymmetries between individuals and APP entities. This is particularly the case where a person is able to make choices within the service on offer, or to choose between services and decide whether to engage with a business, based on their information handling practices. Where alternative choices, product or services exist, privacy self-management mechanisms can influence the market to increase privacy protection in accordance with consumer demand.

5.3 While the discrete transparency and notice requirements in APPs 1 and 5 underpin the exercise of individual choice and control, they also support the accountability of APP entities. Through transparency, an individual may decide to exercise control in how they deal with a service (such as adjusting privacy settings) or decide not to engage with the business. The transparency obligations also assist regulators to hold entities to account.

5.4 Privacy self-management relies on entities making information about their personal information handling practices accessible and understandable. Privacy policies and notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. However, the complexity of today's information ecosystem, where unprecedented amounts of personal information are collected and shared for a range of different purposes, makes it challenging to give individuals' clear information about how their personal information will be handled.

5.5 APP 1 privacy policies and APP 5 notices were not intended to be consent mechanisms that amount to contractual terms and conditions for consumers. There has, however, been a shift towards bundling privacy policies and notices into one document, sometimes called 'terms and conditions' and purporting to use them to seek 'agreement' to broad data handling practices. This has likely been driven by global, USA-based corporations operating in Australia, which have imported and spread American norms where privacy is a matter of contractual negotiation.

5.6 Rather, the objective of APP 1 is to ensure APP entities mange personal information in an open and transparent way. An APP 1 privacy policy provides higher level information to the world at large about how an organisation generally handles personal information, how to access personal information and make a complaint. APP 5 notices play a complementary role as a transparency measure and in promoting individual participation in decision making about their personal information by explaining in clear terms how their personal information is collected, used and disclosed in the particular circumstances. In contrast to the more general privacy policy under APP 1, an APP 5 notice is designed to provide specific information relevant to a particular collection of personal information.[93]

5.7 Consent is also an important part of privacy self-management, supporting transparency, choice and control for individuals. As observed in the Issues Paper, there are specific circumstances in the APPs where an APP entity must seek consent to collect, use or disclose information. In particular, the Privacy Act seeks to establish consent as basis for collection, use or disclosure in circumstances that are higher risk, for example, where an APP entity collects 'sensitive information' or uses or discloses personal information for a purpose that is different to the primary purpose for which it was collected.

5.8 However APP entities are currently permitted to collect, use or disclose personal information without the consent of individuals. Collection of personal information is permitted where it is reasonably necessary for, or, for agencies, directly related to, the entity's functions or activities. Use or disclosure is permitted without consent if, for example, the use or disclosure is for the primary purpose that the information was collected, or if the purpose of the use or disclosure is for a purpose that is related to the primary purpose and the individual would reasonably expect the entity to use or disclose their information in this way.

5.9 This recognition that consent is not necessary or appropriate in all circumstances reflects the fact that many instances of personal information handling in the economy are reasonably expected by individuals. Requiring consent in these expected circumstances may make this mechanism into a tick-box exercise which will detract the value of consent in higher-risk situations where it will actually be valuable. .

5.10 The OAIC supports the need to strengthen notice and consent requirements in the Privacy Act, however this should occur by introducing measures to address the limitations of notice and consent to ensure they are likely to be understood and valid, rather than expanding the use of these privacy self-management tools. These limitations, and recommendations to address them, are discussed below.

5.11 The complexities of data practices are now such that reforms to notice and consent should be complimented with the introduction of an overarching fair and reasonable requirement and additional organisational accountability obligations that will redress the imbalance in knowledge and power between individuals and organisations. Discussion and recommendations about these measures is below at Parts 6 and 7.

---

[93] OAIC (May 2017) '*The definition of personal information*' [online document], OAIC, accessed 18 November 2020, [1.10].

Recommendation 31 – Strengthen notice and consent requirements in the Privacy Act to address the limitations in these mechanisms, but preserve the use of consent for high privacy risk situations, rather than routine personal information handling.

Limitations of notice and consent

5.12 Notice and consent only achieve their goal of giving individuals choice and control if they are used effectively and in appropriate circumstances. In the OAIC's view, the overuse of these mechanisms will place an unrealistic burden of understanding the risks of complicated information handling practices on individuals. This will not address the privacy risks and harms facing individuals in the digital age.

5.13 There are several important practical limitations on the use of notice within the privacy framework. A fundamental dilemma of notice is that it usually comes to a choice between making notice simple and easy to understand or fully informing an individual of the consequences of handing over data, which can be quite complex if explained in meaningful detail.

5.14 APP 5 notices are increasingly being embedded within long and complex statements of terms of provision and use of service, while other privacy information is 'incorporated' by reference to a general privacy policy. Individuals may want to know how their personal information will be handled, but including these descriptions in long complex notices, often drafted with legal obligations in mind, fails to deliver on this objective.

The results of OAIC's 2020 ACAPS survey found that:

- 69% of individuals do not read privacy policies attached to any internet site.
- The key reasons Australians don't read privacy policies attached to internet sites is because of the length (77%) followed by their complexity (52%).
- Even among those who normally read the privacy policy attached to a site, 41% sometimes don't because it is too long and 26% sometimes don't because it is too hard to read.
- When Australians do read privacy policies, comprehension difficulties are widespread. Fewer than 2 in 5 Australians (37%) are confident they have understood them when they read them, and 53% are not confident. The remaining 10% never read privacy policies.[94]

5.15 Emerging, innovative technologies, such as artificial intelligence tools, may use personal information as the basis for a decision that could have significant effects for

[94] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 70.

the individual, but do so in a way that is often invisible or difficult to comprehend, and may be challenging for APP entities to clearly explain.

5.16 The practical consequence of these issues is that the descriptions of more impactful or unusual privacy affecting acts or practices are often 'lost in the noise' of descriptions of more generic or expected information handling activities.

5.17 Expanding transparency requirements could have the effect of further increasing the length of notices, which may make them more difficult to interpret and be less useful in informing individuals, particularly of unusual or unexpected information handling practices. It is also important to note that the notice and consent model does not scale, meaning that while transparency reforms may make it easier for individuals to read and understand a few privacy policies or notices, it is unreasonable to expect individuals to engage meaningfully with notices from the large (and likely increasing) number of APP entities seeking to handle their personal information.

5.18 Consent is also a privacy self-management tool that has its limitations, particularly in light of the various challenges and complexities created by digital technologies. These limitations constrain the usefulness of consent as a privacy protection:

- Consent is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information. In many cases, consumers may feel resigned to consenting to the use of their information to access online services, as they do not consider there is any alternative.
- The challenge faced by APP entities in seeking consent will vary depending on how necessary the individual considers the relevant product or service. Anecdotal evidence suggests that individuals already feel that they are dependent on the services offered by global social media platforms, search engines and e-commerce sites, which typically offer all-or-nothing terms and conditions. As these products or services become more entrenched in individuals' lives, not engaging with a product or service, even where an individual holds privacy concerns, may not be a realistic option without having a significant impact on an individual's ability to engage online.
- Consent must be freely given, specific, unambiguous, and informed, which can be particularly difficult to achieve in the digital environment where data flows and data practices are increasingly complex and difficult to understand. It is becoming increasingly apparent that individuals are not always well placed to assess the risks and benefits of allowing their personal information to be shared. For example, at the moment of sharing, individuals cannot always know what other personal information can be derived about them, and what other information it may be combined with in the future to develop additional insights about them. This is supported by studies that have suggested that there are cognitive limitations that impact the ability of individuals to accurately assess risks when deciding whether to consent to privacy terms. For example, individuals have been shown to overvalue immediate benefits and costs (for example, the benefits of immediate access to a desired online service),

while struggling to accurately assess more delayed benefits and costs (for example, privacy risks).[95]

- The notice and consent model is predicated on consumers making individual privacy decisions about their own personal information. However, recent privacy issues in relation to COVID-19 or attempts to manipulate political processes are illustrating that privacy decisions by individuals are increasingly impacting the community or the wider Australian public.[96]
- Research suggests that some APP entities operating online use so-called 'dark patterns' designed to nudge individuals to consenting to more collections and broader uses of personal information.[97]

5.19 As noted, consent is only required under the Privacy Act for higher risk information handling activities. This is why there is a high threshold for valid consent. If consent became the primary basis for personal information handling, this high threshold would place an unnecessary compliance burden on entities for much of their information handling across the online and offline environment. For example, APP entities will be required to seek informed, voluntary, current and specific consent for standard business activities, such as providing records that contain personal information to an accountant or reviewing records for auditing purposes. It would also require individuals to 'consent' to a myriad of information handling practices that they do not currently need to consent to and which they would reasonably expect.

5.20 As noted above, the OAIC is supportive of reforms to the notice and consent framework in the Privacy Act, particularly to prevent overly broad, unfair or unreasonable information handling practices. This submission recommends several reforms to further strengthen and clarify notice and consent requirements.

5.21 However, the OAIC does not consider that the privacy risks and harms facing individuals in the digital age will be addressed by expanding APP entities' notice obligations, or the circumstances where consent is required.

5.22 The burden of understanding and consenting to complicated practices should not fall on individuals but must be supported by enhanced obligations for APP entities that promote fair and reasonable personal information handling and organisational accountability. The OAIC sees one of the key goals of the law reform process as being to ensure that the APPs provide a framework for the handling of personal information that is fair and reasonable, with consent only required in limited circumstances that will be of most benefit to individuals. Recommendations 37, 38, 39 and 40 in this submission are aimed at addressing this key issue.

---

[95] See discussion of bounded rationality at Taylor M & Paterson J (in press) Protecting privacy in India: The role of consent and fairness in data protection *Indian Journal of Law and Technology*, p. 18.

[96] See the discussion of these limitations with the notice and consent model in Susser, D (2019), 'Notice After Notice-and-Consent: Why Privacy Disclosures are Valuable Even if Consent Framework's Aren't', *Journal of Information Policy*, 9, pp 37-62

[97] Oyvind H. Kaldestad (2018) *Report: Deceived by design*, Forbruker Rådet website, accessed 26 November 2020

Recommendations to strengthen notice requirements

22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?

24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

Countering information overload

5.23 The OAIC considers that an appropriate balance must be struck between strengthened notice requirements and the practical consequences of increased provision of notices to consumers, which could include increased notification fatigue.

5.24 Developments in technology present the opportunity for more dynamic, multi-layered and user-centric privacy policies and notices in the online environment. The OAIC supports innovative approaches to privacy notices, for example, 'just-in-time' notices,[98] video notices, privacy dashboards and multi-layered privacy policies[99] to assist with readability and navigability. The OAIC considers that the proposed Online Platforms code provides an appropriate instrument to include such measures.

5.25 The OAIC considers that the following measures would assist to address the limitations of notice outlined above and strengthen the utility of notice under the Privacy Act. These measures could be introduced into the Privacy Act, in industry-specific codes, legally-binding rules supported by Commissioner-issued guidelines.[100]

Language and accessibility

5.26 The OAIC recommends that requirements should be introduced for APP 5 notices to be concise, transparent, intelligible and written in clear and plain language.[101]

---

[98] Just-in-time notices can be used across digital devices; for example, when the consumer is using an application, and the entity managing the application is collecting information via the application's settings, a pop-up window can alert the consumer with a summary of their data being collected. Particularly in relation to information handling that an individual would not reasonably collect, the OAIC supports point in time notifications during specific interactions with consumers.

[99] A notice can be presented in a layered format, which can link to other documents and may assist in reducing information overload for consumers.

[100] See OAIC Recommendation 16, which recommends including a new provision in the Privacy Act that would require entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

[101] In its submission to the Australian Government in response to the ACCC's DPI, the OAIC argued for striking a balance between appropriate, strengthened notice requirements, whilst also recognising that excessive use of these would create a 'notification fatigue' (See OAIC (2019) *Digital Platforms Inquiry final report — submission to*

5.27 The OAIC also recommends the practical application of the enhanced obligations in APP 5 could be supported through the use of codes, legally-binding rules or Commissioner-issued guidelines addressing the following requirement:

- Formatting notices in a way that will draw the consumer's attention to it at the time of collection, or before the point of collection
- Ensuring readability across multiple digital devices, including smaller screens
- Require notices to be written at a level that can be readily understood by the minimum age of the reasonably likely audience of affected individuals[102]
- Notices should be reasonably accessible, particularly for those with disabilities.[103]

5.28 These requirements would ensure that APP entities create succinct and transparent notices that narrow the focus of what must be addressed, and ensure the notice is manageable to for individuals.

Recommendation 32 – Introduce requirements that APP 5 notices should be concise, transparent, intelligible and written in clear and plain language.

Standardised icons or lexicon

5.29 The OAIC supports measures to create a common language to assist individuals make informed decisions about their personal information, for example, through the use of standardised icons or phrases, as recommended in the ACCC's DPI report. This will allow individuals to readily identify the information handling practices of most relevance to them, and to compare products and services in order to make consumer choices based on privacy credentials. It may also allow the development of a 'traffic light' system to compare privacy settings across products and services.

5.30 The use of standardised language and icons will also streamline compliance by all entities when developing privacy policies, notices and consent mechanisms. This will also support compliance by small business if the exemption is removed from the Privacy Act (see OAIC Recommendation 27).

5.31 The OAIC considers that, initially, sector-specific standard icons or lexicons, developed in collaboration between the OAIC, industry and consumer groups, will be most effective. This process was used in the CDR regime, where Data61 developed the consumer experience standards and the mandatory data language standards in

---

the Australian Government [online document], OAIC website, accessed 4 November 2020) . The ACCC recommended that one way to counteract this would be through not require consent when personal information is being processed in accordance with a contract to which the consumer is a party.

[102] See discussion of transparency at Chapter 4 of UK ICO (2020) *Age appropriate design: a code of practice for online services,* ICO Website, accessed 25 November 2020.

[103] These could be modelled on § 999.305 of the California Consumer Privacy Act Regulations which came into force on 14 August 2020.

collaboration with the OAIC, ACCC and industry. These standards were subject to extensive user testing.[104]

5.32 Recommendations 14, 15 and 16 will provide the Commissioner with greater regulatory options to operationalise such measures, for example through a code, legally-binding rules and Commissioner-issued guidelines. This could facilitate an industry-led, collaborative process to develop standard icons or language that are flexible and tailored to the specific needs of the sector. These standardised icons and lexicons can be refined and iterated based on consumer experience and as the needs of the sector evolve. This would complement similar measures that will be included in the upcoming code aimed at digital platforms.

5.33 However, in order to assist individuals to understand the specific information handling practices of the entity they are dealing with, standardised icons and phrases may need to be supported by additional information where required. This is primary because it is important that APP 5 notices remain context specific with a clear goal of explaining the particular purpose for which a specific entity is proposing to collect an individual's personal information.

Recommendation 33 – OAIC supports the development of standardised icons or lexicon through an industry led process to assist individuals make informed decisions about their personal information.

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

5.34 APP 5 requires an APP entity to take reasonable steps to notify an individual about the collection of their personal information, regardless of whether the APP entity has collected the personal information directly from the individual or from a third party.

5.35 The OAIC's APP guidelines outline a limited number of scenarios in which not providing notice under APP 5 may be reasonable, such as where an individual is aware that the personal information is being collected, the purpose of the collection and other APP 5 matters relating to collection; when notification may jeopardise the purpose of collection or the integrity of the personal information; when notification may pose a serious threat to life or safety; or if notification would be inconsistent with other legal obligations. It is the responsibility of the collecting APP entity to be able to justify not taking any steps.

5.36 The OAIC considers that Recommendation 37 to introduce a fairness and reasonableness requirement in relation to collections, uses or disclosures of personal

[104] Data61 was required to make data standards in s 56FA of the *Competition and Consumer Act 2010* (Cth) and Rule 8.11 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth).

information will serve to address the privacy risks that may arise if an APP entity does not notify an individual about the collection of their personal information under APP 5. Additionally, the OAIC considers that strengthening the obligations on APP entities collecting from third parties (as outlined in paragraphs 3.26-3.33) will further serve to reduce privacy risks in these circumstances.

Recommendations to enhance the use of consent

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

29. Are the existing protections effective to stop the unnecessary collection of personal information?

a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?

30. What requirements should be considered to manage 'consent fatigue' of individuals?

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

33. Should specific requirements be introduced in relation to how entities seek consent from children?

5.37 The OAIC considers that it is important to preserve the use of consent for situations in which the impact on an individual's privacy is greatest, and not require consent for uses of personal information for purposes that individuals would expect or consider reasonable.[105] Seeking consent for routine purposes may undermine the quality of consents obtained from consumers, and result in consent fatigue. It is also essential that consent be relied on only where an individual is actually being given meaningful control over their personal information.

5.38 Rather than expanding the use of consent broadly, the OAIC recommends a number of measures that will ensure that consent is meaningful and relied on by entities in appropriate circumstances.

[105] This aligns with the position of the Canadian Government, as set out in Innovation, Science and Economic Development Canada (2019) *Strengthening Privacy for the Digital Age*, Government of Canada website, accessed 20 November 2020.

5.39 The OAIC supports the ACCC's recommendation in the DPI report that consent should be defined to require a clear affirmative act that is freely given, specific, unambiguous and informed. This reform would align the definition of consent more closely with the GDPR.[106]

5.40 As noted in paragraphs 5.48-5.51 below, consent must also be current. This means that an individual's consent will only last as long as is reasonable, having regard to the particular circumstances. The OAIC recommends elevating this requirement for consent from the APP guidelines into law.

Recommendation 34 – Amend the definition of 'consent' to require a clear affirmative act that is freely given, specific, current, unambiguous and informed.

Specific and purpose-based consent

5.41 Consent will only be valid if an individual understands what they are consenting to and is given the opportunity to consent to specific personal information handling practices. As noted in the OAIC's APP guidelines, consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. An APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures.' Requesting broad or 'bundled' consents has the potential to undermine the voluntary nature of consent.[107]

5.42 An amended definition of consent, as per Recommendation 32 above, could be supported by Commissioner-issued guidance that sets out expectations for ensuring specific and purpose-based consent,[108] including that:

- Consent is not freely given when the provision of service is conditional on consent to personal information handling that is not necessary for the provision of the service, as per Article 7(4) of the GDPR.
- APP entities must clearly and narrowly define the purposes for which the personal information will be handled and consent is being sought.

[106] Article 4(11) of the General Data Protection Regulation defines 'consent' of the data subject as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[107] Bundled consent refers to the practice of an APP entity 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

[108] As per the OAIC's Recommendation 16, entities would be required to take account of Commissioner-issued guidance when carrying out their functions and activities under the Privacy Act.

- Consent must be specific and granular.[109]
- APP entities should consider the use of graduated consent and tiered consent, similar to the approach to consent currently being proposed under the CDR regime.[110]

Pro-privacy default settings

5.43 Default settings provided by entities nudge users towards privacy intrusive options as research shows most users do not look at/change their default settings.[111] These are known as 'dark patterns'.[112]

5.44 Research suggests some entities may use design choices and language to manipulate users to choose the less privacy-friendly options, and ultimately discourage them from making an active choice. For example, through the:

- Use of salient colours, buttons or options, playing towards the consumer's tendency to choose the easier road.
- Need for significantly more clicks to adjust away from default settings.
- Focusing on positive aspects of one choice whilst glossing over potentially negative aspects, assisting consumers to comply with the service provider's wishes.
- Giving consumers the illusion of control, making them more susceptible to taking risks with sharing information.[113]

5.45 The OAIC considers that default settings that aim for data maximisation run counter to the policy intentions of the Privacy Act and increase the risk of harm to individuals. This is particularly the case where this information is being used to facilitate direct marketing through online advertising as part of an entity's business model and is not necessary to reasonably enable the provision of the particular product or service in a manner reasonably contemplated by the user. They are also counter to community expectations, as evidenced in the OAIC's 2020 ACAPS results, which found that 85% of

---

[109] For example, see UK ICO, *Guide to the General Data Protection Regulation (GDPR): Lawful Basis of Processing: Consent*, ICO website, accessed 20 November 2020.

[110] Graduated consent: where a consumer can give consent to different uses of their data throughout the relationship with the entity. Tiered consent: where the consumer agrees to disclose increasing amounts of personal information in exchange for different products and levels of services, which can occur 'just-in-time'. Under the Consumer Data Right (CDR) system, an entity must ask a consumer to consent to specific uses of their CDR data: Rule 4.11(1)(a)(ii) of the CDR Rules. The ACCC is proposing to amend the CDR Rules so that a consumer may 'amend' this consent at a later point in time, for example where they wish to consent to additional/fewer/different uses of their data and/or consent to the collection of additional/fewer/different types of data (see, for example, subdivision 4.3.2A of the exposure draft for 3rd amendment of the CDR Rules, available on the consultation page on proposed changes to the CDR Rules, which closed on 29 October 2020)

[111] It was found that Facebook and Google default settings pre-selected the use of personal data for ads based on third-party data/personalisation, and users were required to actively disable these settings. See Oyvind H. Kaldestad (2018) *Report: Deceived by design*, Forbruker Rådet website, accessed 26 November 2020.

[112] Forbruker Rådet (2018) *'Every Step You Take: How deceptive design lets Google track users 24/7'*, Forbruker Rådet website, accessed 26 November 2020, p 12 [3.8].

[113] Oyvind H. Kaldestad (2018) *Report: Deceived by design*, Forbruker Rådet website, accessed 26 November 2020.

Australians considered that digital platforms should only collect information needed to provide their product and/or service.

5.46 Pro-privacy default settings require a higher level of user engagement before APP entities can collect and use personal data for a secondary purpose. For an entity to collect personal data for a secondary purpose, they will need explicit opt-in from the consumer.

5.47 While this will cause some regulatory burden on entities such as the digital platforms which rely on data collection for their business model, this is an essential protection for individuals. It will also incentivise entities to design consumer friendly, easy to use privacy controls and place the responsibility on these entities to provide clear notices that persuade individuals why positively electing to change these default settings is in their best interests.

Recommendation 35 – Amend the Privacy Act to require all settings to be set to privacy protective as default except for collections of personal information that reasonably enable provision of the particular product or service.

Refreshing and withdrawing consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

39. Should entities be required to expressly provide individuals with the option of withdrawing consent?

5.48 The OAIC's APP guidelines indicate that consent must be current and specific. This includes enabling an individual to withdraw their consent at any time, which should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

5.49 The OAIC recommends that this guidance is elevated into law, including a requirement that an individual be notified of their right to withdraw consent, where consent has been required for the personal information handling. This could be modelled on current requirements in the CDR.[114] This would complement the OAIC's recommendations to introduce a right to erasure and right to object, as outlined in Part 3.

5.50 The OAIC's APP guidelines also note that consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice

[114] CDR Rules, Rule 4.11(3)(g)

to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

5.51 The OAIC is supportive of APP entities having processes in place to check whether the consent that an individual has provided remains current. This must be balanced with issues around information overload and consent fatigue, as discussed above.

Recommendation 36 – Elevate OAIC guidance on withdrawing consent into the Privacy Act, including a requirement that APP entities must notify an individual of their right to withdraw consent, where consent has been required for the personal information handling.

Emerging technologies and privacy self-management

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

5.52 IoT devices and services offer great benefits and opportunities to individuals and the Australian economy. However, as these devices become more widespread and interconnected, they are becoming increasingly capable of collecting more significant volumes of personal, and often sensitive, information. This can create significant security and privacy risks.[115]

5.53 IoT devices may appear in various contexts, ranging from consumer items such as smart speakers or smart appliances, devices used as part of smart city initiatives as well as industrial applications of this technology. Of particular risk are IoT devices used in toys or devices that will be used by children.

In 2016, the OAIC and other members of the Global Privacy Enforcement Network undertook a global sweep of IoT products, which identified several problems with the privacy practices of IoT devices. The results of the sweep found that:

- 71% of devices and services considered failed to properly explain how information was stored
- 69% did not adequately explain how customers could delete their information off the device
- 38% failed to include easily identifiable contact details if customers had privacy concerns

[115] See the discussion of the privacy risks associated with IoT devices in Office of the Victorian Information Commissioner (2020), *The Internet of Things and Privacy*, OVIC, Victorian Government.

- 91% did not advise customers to customise their privacy settings.[116]

5.54 Transparency obligations are particularly important for IoT devices and can present compliance challenges. Under the Privacy Act, APP entities are required to ensure that individuals have access to information about the types of personal information that will be collected, and the ways it will be used and disclosed. Where IoT devices do not have screens or other interfaces, APP entities will have to take other steps to ensure compliance with their transparency obligations.

5.55 IoT devices also pose challenges for seeking valid consent where required, particularly ensuring that consent is voluntary and informed.[117] Devices that collect personal information in public spaces automatically may rely on individuals to opt-out of collection. To the extent that individuals are aware of the use of these devices, the non-interactive nature of IoT devices means that opting-out may be challenging. This may also result in an individual simply having to move to a different area.[118] Obtaining informed consent will require APP entities to place notices prominently so that individuals are aware of how their personal information will be handled.[119]

5.56 The OAIC's recommendations about notice and consent and ensuring that all settings to be set to privacy protective as default in the above section will assist in addressing the challenges to these privacy self-management tools that are posed by IoT devices.[120] The OAIC also recommends amending APP 1 to expressly require entities to adopt a 'privacy by design' and 'privacy by default' approach, which will require APP entities to consider privacy compliance while developing and designing IoT devices (see Recommendation 42).[121]

5.57 Given the challenges that IoT devices pose to privacy self-management requirements, ensuring that APP entities deploying this technology act fairly and reasonably, and comply with other appropriate organisational accountability requirements, is

---

[116] For more information, see the Office of the Australian Information Commissioner (23 September 2016) Privacy Commissioners reveal the hidden risks of the Internet of Things [media release], Australian Government, accessed 21 November 2020.

[117] For a detailed consideration of challenges in seeking valid consent in relation to IoT devices in Office of the Victorian Information Commissioner (2020), *The Internet of Things and Privacy*, OVIC, Victorian Government, pp. 6-8.

[118] Office of the Victorian Information Commissioner (2020), *The Internet of Things and Privacy*, OVIC, Victorian Government, p. 10.

[119] These issues will arise where IoT devices collect personal information passively, including for example, vehicles that are connected to the internet. The European Data Protection Board has provided guidance on privacy issues in the context of connected vehicles and other mobility related applications.

[120] For example:

- Recommendation 32: Requiring notices to be concise, transparent, intelligible and written in clear and plain language.
- Recommendation 34: Strengthen requirements for valid consent to ensure that it is informed, freely given, voluntary, current and specific and individuals must have capacity to give consent.
- Recommendation 35: Settings for IoT devices should be set at the most privacy protective by default.

[121] See OAIC (March 2020), *Voluntary Code of Practice Securing the Internet of Things for Consumers — submission to the Department of Home Affairs*, OAIC website, accessed on 24 November 2020, [15]-[17].

particularly important. This submission recommends several requirements that will be relevant protecting individuals in the context of IoT devices:

- Introducing requirements for APP entities to collect, use and disclose personal information fairly and reasonably to ensure that APP entities providing IoT devices handle information in a manner that meets Australian community expectations (see Recommendation 37)
- Implementing full or partial prohibitions for certain acts or practices in relation to IoT, particularly in relation to children, as well as the surveillance of individuals through their personal devices (see Recommendation 40)[122]
- Introducing a right to erasure which, subject to exceptions, would allow individuals to request the deletion of their personal information, particularly where there is a transfer of ownership of an IoT device (see Recommendation 23)[123]

5.58 IoT devices may often collect technical data which may be used for purposes such as profiling individuals. The granularity of information collected by IoT devices may also allow increasingly accurate inferences about individuals. The OAIC's recommendations about the definition of personal information to clarify that technical data and inferred information are captured will address this issue (see Recommendations 4, 5 and 6).

5.59 Finally, information security obligations under APP 11 are particularly important in relation to IoT devices, given the volume of personal information that may be collected by this technology.

[122] See also OAIC (March 2020), Voluntary Code of Practice Securing the Internet of Things for Consumers — submission to the Department of Home Affairs, [49]-[59].

[123] See also OAIC (March 2020), Voluntary Code of Practice Securing the Internet of Things for Consumers — submission to the Department of Home Affairs, [40]-[42].

Part 6: Fairness and reasonableness requirements for entities

40. Should there be some acts or practices that are prohibited regardless of consent?

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

6.1 As discussed in the Objectives section of this submission, this review represents an opportunity to recognise that strong data protection and privacy rights are both necessary to prevent erosion of our human right to dignity in the digital age, and also a precondition for consumer confidence, economic growth and to meet other societal objectives such as the protection of health, safety and security. A greater emphasis on the rights of individuals and the obligations of entities to protect those rights is necessary to ensure the public interest is served by privacy law into the next decade. This includes creating a more central focus on protecting individuals from harms that are associated with the collection, use or disclosure of their personal information.

6.2 As noted in Part 3 above, to remain fit for purpose into the next decade, it is essential that the Privacy Act contains flexible protections that are able to evolve and respond as technologies shift, while creating legal obligations that can address current and evolving privacy risks and harms. In some circumstances, this principles-based framework will need to be supplemented with codes, legally-binding rules and Commissioner-issued guidelines to address high risk activities or sectors.[124]

6.3 To achieve these goals, the OAIC recommends a number of measures aimed at achieving greater fairness and more accountability in the personal information handling activities of APP entities:

- introducing specific obligations around the fair and reasonable handling of personal information
- restraining broad collections of personal information
- prohibiting certain information handling through no go zones
- introducing an independent third-party certification scheme.

6.4 These measures will assist in protecting individuals' privacy rights, thereby helping APP entities to build trust and confidence in their personal information handling practices. It will not impose undue compliance burdens on APP entities who are already committed to good privacy practices. These measures are discussed in more detail below.

[124] See the OAIC's Recommendations 14, 15 and 16 to enhance the existing code-making powers in Part IIIC of the Privacy Act and introduce new powers to make legally-binding rules and a requirement for entities to take Commissioner-issued guidance into account when undertaking their functions or activities under the Privacy Act.

Introducing fairness and reasonableness standards for the collection, use and disclosure of personal information

6.5 Fairness and reasonableness have always been key concepts underlying the protections in the Privacy Act. An objective of the legislation is to ensure the fair handling of personal information.[125] Similarly, a reasonableness standard is used throughout the APPs and is a widely understood legal threshold.[126] The fairness concept is given limited recognition in APP 3, which requires personal information to only be collected by fair and lawful means. However, the OAIC's regulatory experience indicates that this protection does not go far enough.

6.6 By only applying to the means of collection, this requirement, that personal information may only be collected by fair and lawful means, may not prevent other inappropriate practices. While a collection may not reach an unfair "means" threshold such as collection through deception, there are collection practices which are nonetheless are unfair in that they adversely affect rights and interests. Examples may include the targeted collection of personal information from children or vulnerable people. In addition, determining whether conduct is unlawful may be a complex task for the OAIC without the assistance of a decision of a court or finding of a relevant decision-making body.

6.7 Crucially, this protection does not apply to the uses and disclosures of personal information.[127]

6.8 The practical implication of this limited protection is that the APPs will not prevent all unfair or unreasonable collections, uses or disclosures of personal information, even where these practices do not meet community expectations and may cause harms to individuals. Accordingly, the OAIC considers that a new approach should be taken to replace APP 3.5 with expanded obligations that will have a greater focus on protecting individuals.

Examples of unfair or unreasonable conduct that may be permitted under the APPs

The consequence of the current formulation of the APPs is that acts or practices may be permissible if they comply with the APPs, even if these acts or practices are unfair and unreasonable. For example:

- **APP entities can breach APP 3 when collecting personal information but comply with APP 6 when using or disclosing this information**: An APP entity

[125] See for example page 16 of the explanatory memorandum to the *Privacy Amendments (Private Sector) Bill 2000* which extended the operation of the Privacy Act to the private sector. This document highlighted that an objective of the legislation was to develop a scheme for the fair handling of consumers' personal information.

[126] A reasonableness standard is used regularly in relation to the collection, use and disclosure of personal information (see for example APP 3, APP 6.2, s 16A & 16B), the eligible data breach scheme at Part IIIC and in relation to the security of personal information (APP 11).

[127] This builds on recommendation 17(c) in the Australian Competition and Consumer Commission's Digital Platforms Inquiry, p. 478.

providing a mobile phone application collects personal information from mobile phones for the purpose of on selling it to advertisers. While this may breach APP 3, it may not clearly breach APP 6 as the personal information is being disclosed for the primary purpose for which it was collected. An example of this was a flashlight mobile application which secretly collected personal information, including location information, which was shared with advertisers.

- **APP entities may broadly define and obscure their purposes for disclosure**: An APP entity may define its primary purpose for collection to include profiling of individuals. This conduct may result in uses or disclosures that go far beyond the individual's expectations and may not be in the individual's best interests. This has included information being used for political or research purposes without the individual's knowledge.
- **APP entities can make privacy controls difficult to locate**: Although an APP entity's website may provide notifications about its privacy practices, the controls to actually opt-out of information sharing activities may be difficult to locate. While this practice may be unfair, unreasonable and cause harms to consumers, it may not be prohibited under APP 3 (for example, where the type of information collected is not 'sensitive' information and therefore does not require consent for collection).
- **APP entities can directly or indirectly use personal information to show vulnerable individuals' inappropriate content**: An APP entity can use personal information to target individuals, including vulnerable people, with inappropriate or adult content such as gambling advertisements. This may cause financial or other harms to individuals.
- **APP entities can define their purposes for handling information to include unfair or unreasonable purposes**: An APP entity can define its purpose to include publishing personal information, including addresses and photos, to facilitate targeting of individuals. Publication for this purpose will likely comply with APP 6 (use and disclosure) even though it may lead to harms such as stalking or targeting individuals at their homes.

6.9 The OAIC recommends introducing fairness and reasonableness obligations into APP 3 and APP 6 as follows:

> APP 3 - The collection of personal information by an APP entity under Australian Privacy Principle 3 must be fair and reasonable in the circumstances, even if an individual consents to the collection.
>
> and
>
> APP 6 - The use or disclosure of personal information by an APP entity under Australian Privacy Principle 6 must be fair and reasonable in the circumstances, even if an individual consents to the use or disclosure.

6.10 This would create a proactive requirement for APP entities that is aimed at preventing unfair and unreasonable activities that may result in harms to individuals. These

obligations should be overarching requirements that qualify other requirements in the APPs, including whether an individual has consented to the act or practice. Although consent would likely have constrained unfair or unreasonable personal information handling in the past, this protection has been eroded in the online environment.[128]

6.11 The proposed amendments would supplement the proposed Online Platforms code by enabling it to target the unfair or unreasonable behaviours of entities covered by the code more effectively. It will also capture entities across the economy who may be operating online, but are not covered by the online platforms code.

6.12 The OAIC recommend that the legislation set out a non-exhaustive list of factors that the Commissioner will consider when determining whether acts or practices are fair and reasonable in the circumstances. The OAIC considers it important that these factors be defined to promote regulatory certainty and guide interpretation of these terms in a privacy context. These considerations could be drawn from similar requirements in other jurisdictions, which could, for example, include:

- The primary purpose or reasonably anticipated secondary purposes for which the personal information was collected, used and disclosed will have unjustified adverse impacts on any individuals.[129]
- The primary purpose or reasonably anticipated secondary purposes for which the personal information was collected, used and disclosed is reasonable, necessary and proportionate.[130]

---

[128] A similar requirement in Canadian *Personal Information Protection and Electronic Documents Act 2000* s 5 has been found by their Federal Court to be an overarching requirement that is superimposed on an organisation's other obligations (see Office of the Privacy Commissioner of Canada (2018*) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* [online document], Office of the Privacy Commissioner of Canada website, accessed 6 November 2020).

[129] The UK Information Commissioner Office, *Principle (a): Lawfulness, fairness and transparency* [online document], UK ICO website, accessed 12 November 2020 guidance states that entities must not use information in ways that will have unjustified adverse impacts on individuals. This requires entities to consider not just how they can use personal data, but whether they should use it in these ways. Similarly, under s 18 of the *Personal Data Protection Act 2012* (Singapore), a purpose that is harmful to an individual concerned is unlikely to be considered appropriate by a reasonable person (see Personal Data Protection Commission Singapore (2013), *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, PDPC, Singaporean Government, accessed on 26 November 2020, p. 58

[130] While privacy is a human right, it is not an absolute right. As set out in the Parliament Joint Committee on Human Rights (2015) *Guide to Human Rights*, Australian Government, reasonableness, necessity and proportionality are key concepts when determining whether limitations on non-absolute human rights are justifiable (see also Attorney-General's Department, *Permissible limitations: Public sector guidance sheet* [online document], Attorney-General's Department website, Accessed 12 November 2020). Accordingly, the OAIC generally recommends that Government agencies ensure that their collection, use or disclosure is reasonable, necessary and proportionate to achieve a legitimate policy aim when designing legislation that may infringe on privacy rights (see for example OAIC (2019) *Data Sharing and Release legislative reforms discussion paper — submission to Prime Minister and Cabinet* [online document], OAIC website, accessed 7 November 2020). These principles have also been recognised by European regulators as fundamental to the interpretation of the GDPR. Principles of necessity and proportionality have been recognised as a part of the principles for processing under Article 5 by the European Data Protection Board (see European Data Protection Board (2020) *Guidelines 08/2020 on the targeting of social media users*, EDPB, European Government). These concepts are also important elements of the balancing test required by the UK ICO to determine whether processing fits within the legitimate interests basis for processing (UK ICO, *Legitimate interests*, UK ICO website [online document], accessed 7

- The collection, use or disclosure of personal information will not intrude to an unreasonable extent on the personal affairs of any individual.[131]
- The collection, use or disclosure of personal information is within the reasonable expectations of the individual to whom the information relates.[132]

6.13 We also recommend that APP 1 is amended to require APP entities to take steps as are reasonable in the circumstances to implement practices, procedure and systems that will mitigate the risk of unfair and unreasonable information handling practices as a result of the entity's handling of personal information.[133]

6.14 These provisions will be flexible and apply to APP entities depending on the particular facts and circumstances.[134] They will also only have significant impacts on the small amount of APP entities whose acts or practices do not meet these standards of fairness and reasonableness.

6.15 While the OAIC considers a fairness and reasonableness obligation to be the preferable approach, an alternative model that could be considered is creating a statutory duty of care on APP entities to protect individuals from harms stemming from the use of their personal information.

Recommendation 37 – Introduce fairness and reasonableness obligations into APPs 3 and 6:

> APP 3 - The collection of personal information by an APP entity under Australian Privacy Principle 3 must be fair and reasonable in the circumstances, even if an individual consents to the collection.
> and
> APP 6 - The use or disclosure of personal information by an APP entity under Australian

November 2020). These principles have also been found to be important elements in interpreting a similar right in Canada's privacy legislation (see Privacy Commissioner of Canada (2018*) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* [online document], Office of the Privacy Commissioner of Canada website, accessed 7 November 2020) of several judgments setting out the key considerations when evaluating a organisation's purpose under s 5(3) of the *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA)).

[131] This consideration is modelled on Information Privacy Principle 4 of the New Zealand *Privacy Act 2020*. See also the Office of the Privacy Commissioner of Canada's interpretation of *Wansink v. Telus Communications Inc*. 2007 FCA 21 in the Canadian Federal Court of Appeal which held that evaluating if a purpose is an appropriate purpose under s 5 of the PIPEDA requires an assessment of whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits.

[132] The UK ICO states that fairness obligations under the GDPR requires that entities to not use information in ways that an individual would not reasonably expect (UK Information Commissioner Office, *Principle (a): Lawfulness, fairness and transparency* [online document], UK ICO website, accessed 12 November 2020).

[133] A similar requirement to consider the risks of harms to individuals is contained in Article 24 of the General Data Protection Regulation. This requires controllers and processors to implement appropriate controls technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation, having regard to risks of varying likelihood and severity for the rights and freedoms of natural persons.

[134] Taylor M and Paterson J (*in press*) Protecting privacy in India: The role of consent and fairness in data protection *Indian Journal of Law and Technology*, p. 12.

Privacy Principle 6 must be fair and reasonable in the circumstances, even if an individual consents to the use or disclosure.

Recommendation 38 – Introduce a non-exhaustive list of factors that the Commissioner will consider when determining whether acts or practices are fair and reasonable.

Recommendation 39 – Amend APP 1 to require APP entities to take steps as are reasonable in the circumstances to implement practices, procedure and systems which will mitigate the risk of unfair and unreasonable information handling practices as a result of the entity's handling of personal information.

Interactions with the consumer protection regime

6.16 As noted in the Objectives section of this submission, a foundation in human rights is a key reason why privacy protections in Australia and internationally exist as a separate but complementary legal framework to other Australian laws that protect the rights of individuals. The Australian Consumer Law (ACL) is a key example of a separate but complementary legal regime to the Privacy Act.

6.17 Introducing obligations of fairness and reasonableness in the Privacy Act would strengthen and complement existing ACL protections, as well as the proposed restrictions on unfair trading practices proposed at Recommendation 21 of the ACCC's DPI final report.

6.18 Fairness and reasonableness are important concepts in both the Privacy Act and the ACL, and the OAIC anticipates that APP entities will be able to be guided by existing precedents on these principles.

6.19 However, the proposed non-exhaustive list of factors that the OAIC will consider when determining whether acts or practices are fair and reasonable draws on foundational privacy concepts. In effect, this means that these obligations will respond to unfair or unreasonable practices through a data protection lens which seeks to uphold the right to privacy where personal information is used by business, health practitioners and government. This is separate to the objectives of unfair consumer law protections which seek to safeguard consumers' ability to make free and informed choices that further their own interests.[135]

6.20 Similarly, the Privacy Act applies to personal information wherever it flows, meaning that it will provide important protections in instances where consumer protections may not apply:

- While some personal information handling activities are pursuant to a contract, this will not always be the case. In the OAIC's view, privacy policies and information

[135] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 139.

collection statements in of themselves, are not intended to constitute binding legal contracts. This limits the application of unfair contract provisions under the ACL.

- In an information economy, personal information is increasingly being shared between third parties. In this business-to-business context, these third parties may not have any direct relationship with the data subject. This may limit the application of several consumer protections.
- While fairness and reasonableness incorporate transparency, conduct may be unfair or unreasonable, even if an APP entity is transparent. This suggests that prohibitions on misleading, deceptive or false conduct will not always apply in a personal information handling context.

6.21 The OAIC considers that the best result for Australians and the regulated community is for the privacy framework to apply to all issues of personal information handling. Introducing fairness and reasonableness obligations will be an important factor in allowing the OAIC to approach personal information handling issues holistically.

6.22 To the extent that consumer law and privacy law operate concurrently, the OAIC and the ACCC will continue to work together on issues that fall under both regimes, building on the memorandum of understanding on exchanges of information between these two agencies.[136]

Restraining broad collections of personal information

6.23 The digital age has seen the rise of business models built around monetising the collection, use and disclosure of personal information. This has incentivised increasingly extensive collections of personal information by a wide range of private entities, led by the major online platforms, data brokers and the adtech industry. This increase in the collection of personal information has naturally resulted in increased privacy risk.

6.24 Information collection is addressed in APP 3 of the Privacy Act. This principle limits collection to what is reasonably necessary (or directly related for Australian Government agencies) for one or more of the entity's functions or activities. Many privacy frameworks globally contain substantially similar data minimisation principles.[137]

6.25 For more traditional businesses, where the handling of personal information is incidental to their functions or activities, APP 3 is an effective constraint on information collection.

6.26 However, where an entity's functions or activities focus on the collection, use and disclosure of personal information, APP 3 will have a more limited effect. This is

[136] OAIC (August 2020) *MOU with ACCC — exchange of information* [online document], OAIC website, accessed 20 November 2020.

[137] See for example GDPR, Article 5(1)(c); *Privacy Act 2020* (New Zealand), s. 22, Information Privacy Principle 1; *Personal Data (Privacy) Ordinance (Cap. 486)* (Hong Kong), Schedule 1, Principle 1; *Personal Information Protection and Electronic Documents Act, SC 2000* (Canada), Fair Information Principle 4.

particularly because the Privacy Act also permits private organisations to define their own functions or activities and provides limited mechanism for this to be challenged.

6.27 The OAIC's Recommendation 37 to introduce fairness and reasonableness obligations on APP entities may help prevent some inappropriate information collection practices. However, it is unlikely that it will address the root cause of this issue which is whether these data-driven business models and associated expansive information collecting activities themselves meet Australian community expectations.

81% consider it a misuse for an organisation to ask for information that does not seem relevant to the purpose of the transaction, up 7% since 2017.[138]

6.28 The Privacy Act provides the Commissioner with little ability to challenge the legitimacy of an APP entity's stated business model. Regardless, it would be difficult for the Commissioner to make this assessment, as the relevant considerations go beyond privacy issues. Many of these data-driven companies are highly innovative, and provide benefits for society, even if they carry potentially substantial privacy risks.

6.29 To address increasingly expansive personal information activities, the review provides an opportunity for the Government to consider whether some of these practices, and the associated data-driven business models, remain appropriate for Australia. This assessment should have regard to the need to protect individuals, the legitimate interests of private industry and the public interest in privacy.

6.30 If there is a public interest in specifically regulating these practices or business models, this could be implemented through full or partial prohibitions in the Privacy Act, as per the OAIC's Recommendation 40. In some instances, however, these activities and business models may be more appropriately regulated through other legislative frameworks.

Prohibiting certain information handling: No-go zones

6.31 Some types of information handling practices simply do not meet the expectations of the Australian community.

6.32 The OAIC considers that the worst of these practices should be prohibited, even if an entity has purported to have sought consent to the collection, use or disclosure. APP entities engaging in other high-risk activities should be subject to additional organisational accountability obligations that require them to 'proceed with caution' to ensure that individuals are protected from harms arising from those practices.

6.33 To this end, the OAIC recommends the creation of no-go zones and proceed with caution zones under the general privacy framework. These full and partial prohibitions could be introduced directly into the Privacy Act or be implemented through codes,

[138] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 7.

legally-binding rules and Commissioner-issued guidelines on fairness and reasonableness requirements.[139]

6.34 Prohibitions on information handling activities are common features of other Australian privacy-related laws. The specialist regimes under the *My Health Records Act 2012*,[140] credit reporting provisions in Part IIIA of the Privacy Act[141] and CDR scheme[142] all contain restrictions of this kind.

6.35 The Privacy Act review process could be an effective forum to consult with the community on the types of acts or practices that Australians think should be prohibited or where additional restrictions are warranted.

6.36 Based on the OAIC's regulatory experience, the following types of acts or practices should be considered for full or partial prohibitions:

- Profiling, tracking or behaviourally monitoring of, or directing targeted advertising at, children. The majority of parents consider that children should have the right to grow up without being profiled and targeted (84% agree, 59% strongly agree).[143]
- An APP entity undertaking inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices. This prohibition would have to be carefully drafted to ensure it does not place blanket prohibitions on personal devices such as smart speakers. The majority of Australians (83%) feel their personal devices listening to their conversations and sharing data with other organisations without their knowledge would be a misuse of personal information.[144]
- The scraping of personal information from online platforms. Online platforms should also be required to proactively take reasonable steps to prevent scraping and the risks flowing from this conduct. The community considers the social media industry the

[139] See the OAIC's Recommendations 14, 15 and 16. The no-go zones in the Canadian framework are implemented through guidance in Office of the Privacy Commissioner of Canada (2018*) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)* [online document], Office of the Privacy Commissioner of Canada website, accessed 12 November 2020.

[140] *My Health Records Act 2012* (Cth), s 70A which defines prohibited purposes for the use of My Health Records which includes underwriting a contract of insurance for a healthcare recipient, determining whether a contract of insurance covers a healthcare recipient and determining the employment of a healthcare recipient.

[141] See for example s 20E which prohibits all uses of credit reporting information except in certain circumstances, such as where the disclosure is a permitted CRB disclosure under s 20F. Similarly, certain types of entities are prohibited from being an access seeker under the Part IIIA (see s 6L(2)).

[142] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), r. 4.12(3) and r. 7.5(2) which prohibit an accredited person from selling CDR unless it is de-identified in accordance with the rules or use CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless this is required to provide the consumer with the requested goods or services and the consumer has consented.

[143] OAIC, *Australian Community Attitudes to Privacy Survey 2020*, p. 90.

[144] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 36.

most untrustworthy in how they protect or use their personal information (70% consider this industry untrustworthy).[145]

- The collection, use and disclosure of location information about individuals can be used to profile individuals and is difficult to make anonymous. This information is often considered particularly invasive by the community where its collection, use or disclosure is not reasonably necessary for the operation of the relevant service or product or is not reasonably expected by the user. Around 72% of older Australians were uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser.[146]
- Certain uses of AI technology to make decisions about individuals. This is discussed in more detail below.

6.37 For 'proceed with caution' zones, we recommend the Privacy Act review consider whether to specifically define these zones or whether it is more appropriate to create a risk-based assessment. The latter option has the benefit of ensuring that emerging risky activities can still be identified as requiring additional care.

Recommendation 40 – Introduce full or partial prohibitions of specified information handling activities into the general privacy framework. These could apply to the following practices:

- profiling, tracking or behavioural monitoring of, or direct advertising targeted at children
- inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices
- scraping of personal information from online platforms
- handling location information about individuals, and
- certain uses of AI technology to make decisions about individuals.

Restrictions on use or disclosure in relation to the use of artificial intelligence

6.38 Artificial Intelligence (AI) technologies are increasingly being used by private and public entities. This has the potential to generate significant opportunities and efficiencies for business, government and the community. However, the use of these technologies also creates risks, including to privacy.

[145] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 55.

[146] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 79.

6.39 Privacy frameworks around the world have highlighted the processing of personal information using AI tools as an area where enhanced privacy protections are warranted. This will allow the benefits of AI technologies to be realised while managing the risks.

6.40 The Privacy Act applies to AI technologies that use personal information. The current APPs address some of the risks posed by this technology, for example, through requirements to have practices, procedures and systems in place to ensure compliance with the APPs, notice and consent requirements, and obligations to take reasonable steps to ensure the accuracy and quality of personal information.

6.41 The enhancements to the current Privacy Act framework recommended by the OAIC in this submission will therefore also be relevant to information processing by way of AI. These include recommendations around notice and consent requirements,[147] mandating 'privacy by design' and 'privacy by default',[148] providing individuals with new rights, such as a right to object to information handling and to erasure of personal information,[149] and promoting provable accountability, including through a certification scheme.[150]

6.42 Given that AI is a modern technology that is being deployed by APP entities to handle personal information in increasingly innovative ways, the OAIC also considers that introducing obligations requiring the fair and reasonable handling of information will ensure that the Privacy Act is able to apply flexibly to address this evolving risk.[151] The OAIC's Recommendation 40 about the introduction of full or partial prohibitions in relation to the profiling, tracking or behaviourally monitoring of, or directing targeted advertising at, children will also be relevant.[152]

Overwhelmingly, Australians are seeking more rights in relation to the use of AI technologies. The OAIC's 2020 ACAPS results found that:

- 84% of Australians think that individuals should have a right to know if a decision affecting them is made using AI technology.
- 78% of Australians believe that when AI technology is used to make or assist in making decisions, people should be told what factors and personal information are considered by the algorithm and how these factors are weighted.

6.43 The OAIC recommends introducing additional rights that apply specifically to the processing of personal information by AI technologies. These could apply as a partial prohibition or 'proceed with caution' zone as discussed in paragraph 6.31-6.37 above.

[147] See Recommendations 32 and 34.

[148] See Recommendation 42.

[149] See Recommendations 23 and 25.

[150] See Recommendations 42, 43, 44 and 45.

[151] See Recommendation 37.

[152] See discussion of full and partial prohibitions of certain information handling activities at paragraph 6.31-6.37.

6.44 Several jurisdictions have legislated or are considering introducing a specific protection in relation to automated decision-making. These protections are often modelled on Article 22 of the GDPR.[153] While this could be an appropriate starting point, the review should closely consider whether all aspects of this clause are appropriate in an Australian context.

6.45 These AI-specific rights must be drafted with care to ensure that the interests of individuals are appropriately protected while allowing APP entities to deploy this technology. The OAIC suggests the Privacy Act review has regard to the experiences of other international jurisdictions, as well as the other Commonwealth projects and reviews in respect to AI that are currently underway.[154]

6.46 These domestic and international reviews have highlighted areas where Article 22 of the GDPR could be potentially improved.

6.47 For example, there has been uncertainty around the use of the word 'solely' in this provision,[155] and the Office of the Privacy Commissioner of Canada has recently recommended an AI-specific right that does not include this term, or similar terms

---

[153] Article 22 of the GDPR states:

> *1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
>
> *2. Paragraph 1 shall not apply if the decision:*
>
> *(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
>
> *(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
>
> *(c) is based on the data subject's explicit consent.*
>
> *3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
>
> *4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

A similar right is contained at s 71 of South Africa's Protection of Personal Information Act. A right modelled on the GDPR is also being considered in the United States of America which has looked to clarify this language from the GDPR. See for example Consumer Rights to Personal Data Processing Bill SF 2912 (Minnesota) (proposed legislation); New York Privacy Bill SB 5642 (New York) (proposed legislation); Protecting Consumer. Data Bill SB 5376 – 2019-20 (Washington State) (proposed legislation which is confined to profiling based on facial recognition).

[154] For example, the Department of Industry has published an AI Ethics Framework and is currently developing an AI Intelligence Action Plan. The Australian Human Rights Commission is undertaking a Human Rights and Technology project which has focused on AI and human rights.

[155] See Castan Centre for Human Rights Law, Faculty of Law, Monash University (2020), *Submission to the Human Rights Commission Discussion Paper on Human Rights and Technology*, submission to the AHRC, p. 1-2.

such as 'exclusively', due to concerns they would narrowly circumscribe this protection.[156]

6.48 The AHRC's Human Rights and Technology discussion paper has recently considered this issue and proposed the definition 'AI-informed decision-making'. This refers to decisions that have a legal or similarly significant effect and AI has materially assisted in the process of making this decision.[157]

6.49 The OAIC is generally supportive of this definition as a positive adaptation of the threshold proposed in Article 22 of the GDPR. However, the OAIC also notes that there has been some uncertainty around the meaning of 'similarly significant effects' in the GDPR.[158] Some draft privacy legislation in the United States has sought to provide additional clarification for this term proposing a non-exhaustive list of significant effects which includes, but is not limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities and health care services.[159] This additional clarification could provide a useful model in the Australian context.

6.50 The OAIC also notes that this threshold is not likely to capture many instances of targeting of online content, including advertisements, job postings, media articles or political content. In order to apply to algorithms that use personal information in those contexts, a broader definition will be necessary.

6.51 AI-specific protections for individuals must also be supported by appropriate transparency measures to require APP entities to provide further information and an explanation of AI-informed decision-making.[160]

6.52 This information should be sufficiently meaningful to enable an individual to understand the nature of the decision being made about them. It may also include the types of personal information involved and the weighting of this information.[161]

6.53 A requirement for entities to provide more technical information as part of their notification obligations could provide a basis for individuals (with expert assistance where required) to contest decisions. However, consideration will need to be given to how such an obligation will address issues of commercial confidence. For example,

---

[156] Office of the Privacy Commissioner of Canada (2018) *A Regulatory Framework for AI: Recommendations for PIPEDA Reform* [online document], Office of the Privacy Commissioner of Canada website, accessed 1 December 2020.

[157] See AHRC (December 2019) *Human Rights and Technology: Discussion Paper*, AHRC, Australian Government, pp. 61-71.

[158] See Castan Centre for Human Rights Law, Faculty of Law, Monash University (2020), *Submission to the Human Rights Commission Discussion Paper on Human Rights and Technology*, submission to the ARHC, pp. 4-5.

[159] Consumer Rights to Personal Data Processing Bill SF 2912 (Minnesota); New York Privacy Bill SB 5642 (New York); Protecting Consumer. Data Bill SB 5376 – 2019-20 (Washington State).

[160] Such a right could be modelled on Article 13(2)(f) of the GDPR.

[161] The UK ICO states that similar information should be provided under Article 13 of the GDRP. See UK ICO (n.d.) *What else do we need to consider if Article 22 applies?* [online document], ICO website, accessed on 16 November 2020. See also the discussion of a meaningful explanation in Office of the Privacy Commissioner of Canada (2018) *A Regulatory Framework for AI: Recommendations for PIPEDA Reform* [online document], Office of the Privacy Commissioner of Canada website, accessed 1 December 2020.

the Privacy Act currently provides an exception to entities where an individual requests access to their personal information, and its provision would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

6.54 In considering appropriate notice obligations in relation to AI-informed decision-making, the OAIC suggests that the review draw on the work done by other regulators including the UK ICO and the Office of the Victorian Information Commissioner.[162]

Recommendation 41 – Introduce additional rights that apply specifically to the processing of personal information by AI technologies.

[162] For example, UK ICO and the Turing Institute (n.d.) *Explaining decisions made with AI* [online document], ICO website, accessed on 16 November 2020 as well as the Office of the Victorian Information Commissioner (2019), '*Closer to the Machine: AI e-book*', OVIC, Victorian Government.

Part 7: Organisational accountability requirements for entities

7.1 Accountability is globally recognised as a key building block for effective privacy regulation and management.[163] While the concept of 'accountability' can mean different things in different contexts, for the present purposes, it can be described broadly as the different actions and controls that an entity must implement to comply, and demonstrate compliance, with the privacy regulatory framework.

7.2 As outlined in Part 5, it is important that reforms to privacy self-management mechanisms are complimented by appropriate organisational accountability obligations to ensure that the burden of understanding and consenting to complicated practices does not fall solely on individuals.

7.3 The concept of accountability focusses on whether a regulated entity has translated its privacy obligations into internal privacy management processes that are commensurate with, and scalable to, the risks and threats associated with its personal information handling activities. The specific measures an entity should implement as part of its privacy management program will necessarily depend on its particular circumstances, including size, resources and business model.

7.4 More broadly, while strong accountability mechanisms facilitate compliance with privacy obligations, they can also improve business productivity and help to develop more efficient business processes, for example, by providing certainty and confidence for employees around the appropriate way to handle personal information, reducing the number and cost of data breaches, and improving overall operational efficiencies.[164] Entities with established internal processes are also better able to anticipate and adapt to different business and regulatory changes, as well as to crisis situations.[165]

7.5 By embedding strong accountability measures, entities can build a reputation for strong and effective privacy management, which is essential to realising the benefits of the personal information they hold and meeting their corporate social responsibilities. Accountability enables entities to not only meet the expectations of regulators, but to build consumer trust and confidence in their personal information handling practices.

---

[163] Centre for Information Policy Leadership (CIPL) (May 2020) *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework* [online document], CIPL, accessed 26 November 2020, 35.

[164] CIPL (May 2020) *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework* [online document], CIPL, accessed 26 November 2020, 7.

[165] CIPL (May 2020) *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework* [online document], CIPL, accessed 26 November 2020, 7.

Accountability under the Privacy Act

7.6 Accountability is at the core of APP 1, which requires entities to manage personal information in an open and transparent way. APP 1 does this in two key ways:

- by requiring entities to take reasonable steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs (APP 1.2), and
- by requiring entities to have a clearly expressed and up to date APP privacy policy describing how it manages personal information (APP 1.3).

7.7 By complying with APP 1, entities will establish a culture and set of processes to assist with compliance with all the other APPs. In this way, APP 1 can be described as the 'bedrock' privacy principle.

7.8 However, unlike other data protection regimes with accountability requirements, APP 1 does not prescribe specific measures or practical steps that entities must take to ensure compliance with the APPs.[166] For instance, the OECD Guidelines require data controllers to be accountable for complying with measures which give effect to the basic data processing principles in the Guidelines.

7.9 Similarly, the GDPR has formally embedded accountability requirements into its data protection legislative framework with the inclusion of express obligations on data controllers to:

- implement appropriate technical and organisational measures to ensure compliance with the GDPR (Article 24)
- implement data protection by design and by default (Article 25)
- maintain records of processing activities (Article 30)
- carry out data protection impact assessments (Article 35)
- designate a data protection officer (Article 37).

7.10 Domestically, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the Australian Government Agencies Privacy Code) sets out specific requirements and steps that Australian Government agencies must take as part of complying with APP 1.2. The Code requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management. In particular, the Code requires agencies to:

- have a privacy management plan
- appoint a Privacy Officer, or Privacy Officers, and ensure that particular Privacy Officer functions are undertaken

[166] The OAIC has published a non-binding *Privacy management framework* guidance document that sets out the steps the Commissioner expects entities to take to meet their ongoing compliance obligations under APP 1.2.

- appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information
- undertake a written Privacy Impact Assessment (PIA) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information
- keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites
- take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information.

Recommended enhancements to APP 1

7.11 The OAIC considers that APP 1 should include express accountability requirements for all regulated entities. This will provide further clarity to entities about the steps they should take to meet their ongoing compliance obligations under APP 1, which will support increased trust in their information handling practices among individuals.

7.12 The OAIC recommends that the Privacy Act is amended to include similar accountability measures to those required under GDPR and the Australian Government Agencies Privacy Code. At a minimum, APP 1 should be amended to expressly require entities to:

- take reasonable steps, and *demonstrate* those reasonable steps, to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP code under APP 1.2
- implement, and be able to demonstrate the steps taken to implement, a 'privacy by design' and 'privacy by default' approach
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code, and to implement a 'privacy by design' and 'privacy by default' approach, and
- appoint a privacy officer or privacy officers and ensure that privacy officer functions are undertaken.

7.13 The requirement under APP 1 to implement practices, procedures and systems to ensure compliance with the APPs implicitly requires a 'privacy by design' approach by APP entities. Essentially, 'privacy by design' is an approach where privacy compliance is designed into projects, activities and initiatives dealing with personal information right from the start, and then throughout the information lifecycle, rather than being bolted on afterwards.

7.14 A 'privacy by default' approach requires entities to ensure that, by default, personal information is handled with the highest privacy protections.[167] For example, a 'privacy

[167] European Commission (n.d.) *What does data protection 'by design' and 'by default' mean?*, European Commission website, accessed 26 November 2020.

by default' approach requires entities to design new projects, activities or initiatives to ensure that they only collect the minimum amount of personal information that is necessary for a specific purpose. This links to the obligations in APP 3 and APP 6, which, respectively, require entities to only collect personal information that is reasonably necessary for their functions and activities, and to only use and disclose personal information for the primary purpose for which it was collected (or a secondary purpose if an exception applies).

7.15 'Privacy by design' and 'privacy by default' are complementary concepts, which mutually reinforce each other.[168] APP entities will be better placed to meet their privacy obligations under the Privacy Act by adopting a 'privacy by design' and 'privacy by default' approach to their personal information handling practices.

7.16 In some instances, the OAIC has also observed that entities have not fully or comprehensively documented the steps they have taken to ensure compliance with APP 1.2.[169] Accordingly, the requirement that entities must be able to demonstrate that they have taken reasonable steps to implement practices, procedures and systems to ensure compliance, and a 'privacy by design' and 'privacy by default' approach, will necessarily require entities to document their controls and activities, which adds accountability to the process.[170]

7.17 Similarly, the requirement to provide evidence, on request, of the steps taken to meet these requirements will ensure the OAIC is able to verify that entities are complying with their privacy obligations where appropriate in the circumstances.[171] For instance, the Commissioner may request an entity or entities involved in certain 'high privacy risk' activities, such as the use of facial recognition technology, to provide evidence of the steps taken to meet their compliance obligations. As a matter of best practice, the OAIC may also encourage the use of external auditors to verify compliance in these circumstances.

7.18 More broadly, it is not possible for the OAIC to check compliance economy-wide, which means regulatory action can be reactive. Accreditation can be a proactive and effective way to verify that an entity is compliant with regulatory requirements to prevent harms, without direct intervention from the regulator. For example, under the CDR, any person who wishes to receive CDR data to provide products or services to consumers under the CDR regime must be accredited. Further, demonstrating accountability through accreditation promotes consumer confidence. It shifts some of the burden that is currently on individuals to assess and verify an entity's privacy and

---

[168] European Data Protection Board (EDPB) (October 2020) *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* [online document], EDPB, accessed 26 November 2020.

[169] For example, see the OAIC's summary privacy assessment reports of 14 pharmacies and eight diagnostic imaging services access security governance for the My Health Record system and five Registered Training Organisations and their management of personal information.

[170] Solove, Daniel J and Schwartz, P.M., "ALI Data Privacy: Overview and Black Letter Text" (January 24, 2020), (2020) UCLA Law Review, Vol. 68, pg 27 as cited in Leonard P (2020) *Privacy harms*, report to the OAIC, Data Synergies.

[171] A similar requirement can be found in cl 10 of Canada's new privacy Bill C-11, which requires an organisation to, on request of the Commissioner, provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program.

security credentials to the entities seeking accreditation. An accreditation can be relied on by a consumer in deciding whether to trust one business over another.

7.19 There may be value in the future for the Privacy Act to make provision for a similar accreditation or audit model that could apply to entities seeking to engage in other high privacy risk activities and/or sectors that were specified in the Act or through delegated legislation.

7.20 The OAIC considers that a holistic, demonstrable and ongoing approach to privacy management is central to meeting the requirements of APP 1 and implementing a 'privacy by design' and 'privacy by default' approach. The focus for all regulated entities should be on the quality, reliability and verifiability of a holistic and ongoing privacy management framework that addresses privacy risks throughout the information handling lifecycle. The OAIC's *Privacy Management Framework* sets out the steps that entities can take to establish a privacy management framework and meet their ongoing compliance obligations.

7.21 A central component of a privacy management program is a process for conducting privacy impact assessments, which are critical to facilitating a 'privacy by design' and 'privacy by default' approach. For clarity, the OAIC recommends that the Explanatory Memorandum that will accompany the amending Bill notes that an ongoing and demonstrable privacy management program, which includes conducting privacy impact assessments where appropriate, is central to facilitating a 'privacy by design' and 'privacy by default' approach.

7.22 The objective of enhancing accountability of APP entities for their personal information handling practices is similarly supported by the requirement to appoint a privacy officer or privacy officers. A privacy officer is the first point of contact for privacy matters within an entity and is responsible for ensuring day-to-day operational privacy activities are undertaken. Appointing a privacy officer is a key governance measure to foster a culture of respect for privacy and the value of personal information.

Recommendation 42 – Amend APP 1 to include express accountability requirements for all regulated entities. At a minimum, APP 1 should require entities to:

- take reasonable steps, and *demonstrate* those reasonable steps, to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP code under APP 1.2
- implement, and be able to demonstrate the steps taken to implement, a 'privacy by design' and 'privacy by default' approach
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code, and to implement a 'privacy by design' and 'privacy by default' approach, and
- appoint a privacy officer or privacy officers and ensure that privacy officer functions are undertaken.

Recommendation 43 – Include a note in the explanatory memorandum that will accompany the amending Bill that an ongoing and demonstrable, comprehensive privacy management program, which includes conducting privacy impact assessments where appropriate, is central to facilitating a 'privacy by design' and 'privacy by default' approach.

Accountability in relation to 'purpose'

7.23 Under APP 5.2, entities must notify individuals of, amongst other things, the purposes for which the entity collects the personal information. This includes the primary purpose of collection, that is, the specific function or activity for which particular personal information is collected.

7.24 The purposes of collection is relevant to how the information may be subsequently used and disclosed and if an entity seeks to rely on the 'reasonable expectations' exception in APP 6.2(a) to authorise a secondary purpose. However, there is no requirement in APP 3, which deals with the collection of personal information, for entities to identify and record, at or before the time of collection, the purposes for which they handle personal information.

7.25 A requirement to record information in this way would assist entities to ensure that they have a clear and specific purpose in mind for the subsequent handling of the information. It would encourage entities to consider the purposes of collecting the information earlier and not just in the context of the notification requirements in APP 5, which is consistent with a 'privacy by design' approach to privacy compliance. It would also assist entities to formulate and document the information they must provide to individuals through their APP 1 privacy policy and APP 5 notices.

7.26 Accordingly, to support the accountability requirements in APP 1, the OAIC recommends that APP 3 is amended to expressly require entities to determine, at or before the time of collection, each of the purposes for which the information is to be collected, used or disclosed and to record those purposes.[172]

Recommendation 44 – Amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the purposes for which the information is to be collected, used or disclosed and to record those purposes.

[172] A similar requirement can be found in cl 12(3) of Canada's new privacy Bill C-11, which requires an organisation to determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.

Certification

51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

7.27 The OAIC supports the introduction of an independent third-party certification scheme. Privacy certification schemes have a role to play in facilitating overseas transfers of personal information. However, an independent certification mechanism could also significantly increase the transparency of organisations' data practices by enabling Australians to quickly assess the level of data protection offered by an APP entity, as noted in the ACCC's Digital Platforms Inquiry final report.[173]

7.28 The OAIC considers that an independent third-party certification scheme could assist in ensuring that regulated entities are meeting their obligations under the Privacy Act without the need to substantially increase regulatory action. It also provides consumers with evidence-based information about the privacy credentials of entities with which they may engage.

7.29 There are benefits for entities that obtain certification as well. For example, certified entities may obtain a competitive advantage over non-certified entities. Additionally, certification may assist entities to mitigate against potential enforcement action by creating effective safeguards to address risks around personal information handling activities.

7.30 Several jurisdictions around the world, including Japan,[174] New Zealand[175] and Singapore[176] have implemented privacy certification schemes. While these schemes differ in their nature, scope and requirements, they ultimately enable entities that meet the relevant requirements and certification criteria to display a 'seal' or 'trustmark' as evidence of certification. The GDPR also makes provision for the introduction of data protection certification mechanisms, including data protection seals and marks, at both the member-state level or at the European Union level for the purposes of demonstrating compliance with the requirements of the GDPR.[177]

7.31 Additionally, the APEC CBPR System operates as a regional certification scheme and requires certified businesses to demonstrate compliance with a commonly understood set of privacy standards. The APEC Joint Oversight Panel of the Data Privacy Subgroup endorsed Australia's application to participate in the CBPR System in 2018.

---

[173] Australian Competition and Consumer Commissioner, *Digital Platforms Inquiry Final Report* (June, 2019), 480.

[174] More information about Japan's PrivacyMark System can be found at https://privacymark.org/

[175] More information about New Zealand's Privacy Trust Mark can be found at https://www.privacy.org.nz/resources-2/applying-for-a-privacy-trust-mark/

[176] More information about Singapore's Data Protection Trustmark can be found at https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification

[177] Articles 42, 43 and Recital 100 of the GDPR. At the time of writing, there are no approved certification criteria or accredited certification bodies for issuing GDPR certificates.

7.32 The OAIC considers that there are benefits to implementing a domestic privacy certification scheme in addition to the CBPR System.

7.33 As noted in the Issues Paper, some participating economies in the CBPR System also maintain a domestic certification scheme, including Singapore's Data Protection Trustmark and Japan's Privacy Mark. Additionally, the CBPR System is focussed on facilitating overseas transfers by 'controllers' of personal information, so certification will likely only be relevant and feasible for those entities with significant cross-border disclosure practices to participating economies.[178] A domestic privacy certification scheme could operate to certify a wide range of personal information handling activities or circumstances against the broader requirements of the APPs.

Key issues for consideration for a new certification scheme

Voluntary or mandatory scheme

7.34 The Issues Paper notes that a key issue for an Australian certification scheme is whether it should be voluntary or mandatory. The OAIC considers that a domestic privacy certification scheme should be voluntary for APP entities. However, it may be necessary in the future to consider whether mandatory certification or accreditation requirements should be required for certain high privacy risk activities, such as the use of facial recognition technology, or sectors of the economy.

7.35 Internationally, most existing privacy certifications are voluntary, including the CBPR system, certification schemes in Japan, Singapore and New Zealand, and the GDPR's data protection certification scheme.

7.36 A voluntary scheme would also reduce some of the concerns raised by submitters to the ACCC's Digital Platforms Inquiry that a mandatory certification scheme would carry significant compliance costs and likely be cost-prohibitive for smaller APP entities.

Scope of the scheme

7.37 Another key issue is whether a certification scheme should be broad or narrow. That is, should entities be able to seek enterprise-wide certification or should certification be limited to certain specific products, data types or business processes.

7.38 Under the CBPR system, the scope of the certification is flexible and is determined by the organisation wishing to obtain a certification to participate in the CBPR system.

7.39 The OAIC considers that a domestic certification scheme should enable entities to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes. This will help to ensure that the scheme is flexible and scalable for APP entities of different sizes and with different personal-information handling activities.

[178] There are currently nine participating economies in the CBPR system: USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei and the Phillippines.

Certification criteria

7.40 Certification criteria forms an integral part of any certification mechanism. The Issues Paper notes that developing a privacy certification scheme requires consideration of whether criteria should be based on regional standards, such as the requirements of the CBPR, or standards that have been developed by a private standard-setting organisation.

7.41 The OAIC considers that certification criteria should maintain and build upon the protections and obligations set out in the Privacy Act and reflect community expectations of privacy.

7.42 As highlighted in the ACCC's DPI report, a domestic certification scheme will need to take into account the broader reforms to Australia's privacy regulatory framework. Accordingly, the underlying privacy regulatory framework will need to be settled before key elements like certification criteria can be designed in more detail.

7.43 The Issues Paper also highlights that another consideration is the extent to which a certification scheme could operate consistently with existing accreditations in Australia that incorporate privacy safeguard requirements, such as the CDR and the proposed Data Availability and Transparency scheme. The OAIC agrees that a privacy certification should be interoperable with existing Australian accreditations to the extent possible, in order to minimise the fragmentation of privacy certifications and accreditations for which regulated entities may wish to apply.

7.44 Guidance on general considerations for designing certification criteria may be drawn from the Certification Guidelines issued by the European Data Protection Board, which state that certification criteria should:

- be uniform and verifiable
- auditable in order to facilitate the evaluation of processing operations under the GDPR
- be relevant to the business model of different entities (e.g. business to business and business to customer)
- take into account and where appropriate be interoperable with other standards (such as ISO standards), and
- be flexible and scalable for application to different types and sizes of organisations.[179]

Role of the OAIC

7.45 The key participants, and the functions of those participants in other existing certification schemes, can be broadly described as follows:

[179] European Data Protection Board (EDPB) (June 2019) *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation* [online document], EDPB, accessed 26 November 2020.

- a certification or assessment body that assesses and approves applications from entities seeking certification
- a body that accredits certification or assessment bodies
- entities seeking certification.

7.46 The role of the regulator in these activities varies across international jurisdictions. For instance, in Singapore the data protection authority is involved in accrediting assessment/certification bodies and in New Zealand, the Privacy Commissioner's Office is responsible for issuing certifications directly. However, as noted above, the nature, scope and requirements of these schemes differ significantly.

7.47 The OAIC suggests it would be preferable for an independent third party to administer the scheme to ensure the functional independence of the OAIC. As an independent, statutory regulator, the OAIC is concerned to ensure both the fact and perception of independence are maintained by retaining separation between the certification of entities and the broader regulation of the scheme. The OAIC suggests further consideration could be given, as part of the implementation process, to whether there is a current government body that could undertake the certification function.

7.48 The GDPR does not make the issuance of certifications a mandatory task of the supervisory authorities. Instead, it provides for a number of different models which enable a supervisory authority to decide to, for example, issue certification itself, in respect of its own certification scheme; create its own certification scheme and entrust certification bodies with the certification procedure which issue the certification; or encourage the market to develop certification mechanisms.

7.49 The OAIC considers that the model adopted by the UK ICO could be adopted for a domestic privacy certification scheme. Specifically, in the UK, the certification framework will involve:

- the ICO publishing accreditation requirements for certification bodies to meet
- the UK's national accreditation body, UKAS, accrediting bodies and maintaining a public register
- the ICO approving and publishing certification criteria
- accredited certification bodies issuing certification against those criteria, and
- controllers and processors applying for certification and using it to demonstrate compliance.

7.50 The OAIC should be identified as the scheme's regulator for privacy breaches. It is important to note that any domestic certification scheme does not prove compliance but rather forms an element that can be used to demonstrate compliance. Accordingly, a domestic certification scheme should be carefully designed to ensure that it does not reduce the responsibility of APP entities for compliance with the Privacy Act, or fetter the OAIC's discretion in the exercise of its regulatory powers.

Recommendation 45 – Introduce a domestic privacy certification scheme into Australia's privacy framework. The certification scheme should:

- be interoperable the APEC CPBR system and other relevant domestic accreditation or certification schemes
- be voluntary across the economy generally, but may be made mandatory in relation to specific high privacy risk sectors or practices through an APP code or rules where appropriate
- be flexible and enable entities to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes
- enable the OAIC to develop and publish accreditation requirements for certification bodies and certification criteria for the scheme
- ensure that an independent third party is responsible for appointing the accreditation body or bodies that will carry out audits of entities seeking certification and approving the use of a trust mark or seal and identify the OAIC as the scheme's regulator for privacy breaches.

Part 8: Overseas data flows

8.1 Today's global digital economy relies on data being able to flow securely and efficiently across borders.[180] According to the Export Council of Australia, Australia's digital exports were worth around $6 billion in 2017, equivalent to Australia's fourth largest export sector, and this figure is set to grow.[181] At the same time, cross-border data flows are subject to increased concern and scrutiny around the world.[182]

8.2 Data flows do not recognise geographical borders, and these data flows have made us more interconnected than ever before. It is therefore essential for international privacy laws to set up appropriate and interoperable frameworks that facilitate the efficient movement of data across borders while providing strong protections for individuals' personal information. Global interoperability does not require all countries to have identical frameworks. Instead, it allows for bridges to be built across frameworks that reflect the cultural, social and legal norms of their society. These bridges should allow data to flow safely and efficiently.

8.3 Under the Privacy Act, the framework for cross-border data flows is established in two ways:

- Cross-border disclosures of personal information by APP entities are enabled by APP 8, which relies on an accountability approach.
- The extraterritoriality provisions in s 5B, which set out when the Act will apply to acts or practices engaged in outside Australia and the external Territories.

8.4 This review also presents an opportunity to consider how Australia can facilitate the safe and efficient disclosure of personal information from overseas entities to entities based in Australia. Many of the cross-border disclosure mechanisms in global privacy laws allow data to be transferred to other jurisdictions with comparable privacy protections. It is therefore important to consider the ways in which the Privacy Act can be reformed to facilitate this. The role of 'adequacy' status and certification are considerations here.

8.5 The accountability approach, extraterritoriality and adequacy are discussed further below. Certification is discussed in Part 7 of this submission, above.

---

[180] By some estimates, cross-border data flows contribute around $USD 2.8 trillion to global economic activity, or 3.5% of global GDP. See: McKinsey Global Institute (MGI), 'Digital Globalization: The new era of global flows', McKinsey & Company (2016).

[181] Export Council of Australia, *From Resource Boom to Digital Boom: Capturing Australia's Digital Trade Opportunity at Home and Abroad*, 2018, pg. 6.

[182] 92% of Australians are somewhat to very concerned about their data being sent overseas, see OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 39.

Over recent years there have been numerous cases in the EU regarding the transfer of data from the EU to the US under a range of mechanisms including the Safe Harbour Agreement, the Privacy Shield and Standard Contractual Clauses, see: *Maximilian Schrems v Data Protection Commissioner* (2015) C-362/14, *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems,* (2020) C-3111/18;

UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development', (2016) See: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

The accountability approach

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?

a. Are APP8 and section 16C still appropriately framed?

8.6 The Privacy Act creates a framework for the cross-border disclosure of personal information through the operation of APP 8 and s 16C. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs and makes the APP entity accountable if the overseas recipient mishandles the information.[183]

8.7 This accountability approach reflects a central object of the Privacy Act to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected.[184] Personal information is protected because it requires the disclosing APP entity to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[185] The APP entity also remains accountable for acts or practices done by the overseas recipient.[186] This approach gives substance to the general principle of accountability by ensuring that individuals have a meaningful way of seeking redress under the Privacy Act against the disclosing APP entity.

8.8 APP 8.2 establishes some exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C. For example, an APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- The APP entity reasonably believes that the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to the APPs, and individuals can access mechanisms to enforce those protections.
- The APP entity expressly informs an individual that if they consent to the disclosure, this principle will not apply, and the individual then consents to the disclosure.

8.9 APP 8 only applies to cross border disclosures of personal information. That is, it applies to circumstances in which an APP entity has released the personal information from its effective control. APP 8 does not cover circumstances in which an APP entity 'uses' personal information overseas, that is, where it handles, or undertakes an activity with the personal information, within the entity's effective control. For example, routing personal information, in transit, through servers located outside Australia, would usually be considered a 'use'. In these instances, the APP entity would still remain accountable for any breach of the APPs against the information it 'uses'

[183] *Privacy Act 1988* (Cth), s 16C, APP 8.1.

[184] *Privacy Act 1988* (Cth), s 2A(f).

[185] *Privacy Act 1988* (Cth), APP 8.1

[186] *Privacy Act 1988* (Cth), s 16C

overseas, as it is still considered to 'hold' the personal information and is thus subject to the Privacy Act.

8.10 The OAIC considers that the accountability approach established by APP 8 and s 16C remains an appropriate way of enabling personal information to flow overseas, whilst ensuring there are meaningful redress mechanisms available to Australians. This is an important mechanism to ensure that individuals' personal information is still protected in situations where the Privacy Act may not have extraterritorial jurisdiction.

8.11 The Privacy Act review presents an important opportunity to consult with businesses to understand how they operationalise cross-border disclosures in their business activities. For example, there may be some businesses that are currently not subject to the Privacy Act who are nonetheless disclosing personal information overseas. These businesses may be required to comply with the privacy laws of other jurisdictions, whilst not having obligations to Australians' whose personal information they are handling. The OAIC's recommendation 27 to remove the small business exemption would address this inconsistency.

8.12 The review may also wish to consider whether additional legislated transfer mechanisms that are found in other global privacy laws should be introduced into legislation to assist businesses in complying with the requirements under APP 8. Three examples of these mechanisms, discussed in more detail below, are:

- Contractual safeguards
- Certification
- 'Adequacy' or whitelists

Contractual safeguards

8.13 One way that APP entities can comply with APP 8.1 is through a contractual agreement that requires the overseas recipient to comply with the APPs. These contractual arrangements provide substance to the accountability approach by ensuring that the APP entity has an enforceable arrangement to require the overseas recipient to comply with the APPs. Contractual arrangements are widely recognised across the EU and Asian frameworks as a valid means for an organisation to discharge their obligations under privacy legislation.[187]

8.14 Many jurisdictions have developed model clauses, or standard contractual clauses to facilitate cross border data flows. Under New Zealand's reformed Privacy Act, personal information may be disclosed overseas once a due diligence process establishes that

[187] General Data Protection Regulation, Article 46; According to the Australian Business Law Institute, at least 10 jurisdictions across Asia (Australia, Hong Kong SAR, Japan, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, South Korea, and Thailand) explicitly or implicitly recognise that appropriate safeguards may be provided by 'transfer contracts' or ad hoc contractual provisions where processing is the purpose of data transfer. see Asian Business Law Institute, '*Transferring Personal Data in Asia: Carving a path to legal certainty and convergence between Asian frameworks on cross-border data flows'* May 2020, page 38.

certain privacy standards are met. The Office of the Privacy Commissioner New Zealand has published model clauses that assist entities in meeting these obligations.

8.15 It may be appropriate to consider whether Australia should develop model clauses for disclosing APP entities to use in complying with APP 8.1. The OAIC recommends that such model clauses remain a tool to support an APP entity's accountability under APP 8.1, as opposed to an exception to accountability under APP 8.2.

8.16 The recent decision of the Court of Justice of the European Union (the Schrems Decision) has highlighted the importance of entities being able to satisfy themselves that the receiving entity is able to comply with the Standard Contractual Clauses in a way which provides meaningful equivalent protections.[188] The Schrems Decision established that where transfers are being made under Article 46, EU based entities must also take due account of the surrounding environment in which transferred data is subject to and make an assessment as to whether the implemented safeguards provide an equivalent standard of protection in reality. In particular, the Schrems Decision places the onus on data controllers, exporters and importers to:

- assess the laws and practices of third country jurisdictions, with regard to powers that enable public authorities to access EU citizens' data, before a transfer of data from the EU to a third country is made
- determine whether supplementary measures need to be in place, in addition Standard Contractual Clauses, to ensure protection meets the EU standard.

8.17 Implications from the Schrems Decision suggest that organisations may need to implement additional supplementary measures, beyond Standard Contractual Clauses, to satisfy themselves that the data is protected to an essentially equivalent standard. This decision will have implications for EU entities wishing to transfer personal information to Australia (discussed further in the Adequacy section below), but the Privacy Act review should also consider whether APP entities relying on an exception under APP 8.2 should similarly be required to take account of the broader environmental context into which they are disclosing personal information.

Certification schemes

8.18 Many international frameworks provide for certifications as a transfer mechanism.[189] Certification schemes are likely provided for under the APP 8.2(a) exception, where the certification has a binding effect, and provides mechanisms for individuals to seek redress.

---

[188] *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems,* (2020) C-3111/18.

[189] The GDPR provides for certification, see General Data Protection Regulation, Article 46(2)(f). Certification is also provided for in a number of Asian countries, according to the Asian Business Law Institute, certification is explicitly provided for in Japan, Singapore, and in the amended legislation of New Zealand. It is further implicit in Philippines and Thailand. For now, such an admission is unclear but conceivable in the laws of Hong Kong SAR, Macau SAR, and the Data Protection Bill of Indonesia. It is also conceivable, although more remotely, in the Data Protection Bill of India. See: Asian Business Law Institute, '*Transferring Personal Data in Asia: Carving a path to legal certainty and convergence between Asian frameworks on cross-border data flows'* May 2020, page 49.

8.19 Certification schemes present an opportunity for global interoperability if multiple jurisdictions were to recognise the same certification scheme as a valid transfer mechanism. If this was to occur, certification schemes could act as a bridge connecting different regional frameworks.

8.20 The APEC CBPR is operational and has the potential to provide this. However, the lack of business uptake has limited its success.[190] Australia was endorsed as a participating economy in 2018. The review presents an opportunity for Government to consult businesses to determine whether CBPR certification would assist entities in complying with APP 8. The OAIC recommends that the CBPR Program Requirements be carefully assessed to determine whether they satisfy the APP 8.2(a) requirement of 'protecting in information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information'.[191]

8.21 Certification is discussed further in Part 7 of this submission.

'Adequacy' or whitelists

8.22 One of the exceptions in APP 8.2 is where information is subject to a law with substantially similar protections.[192] Currently, Australian businesses are required to make this assessment based on their own due diligence. It may assist APP entities, if the Australian Government were to establish a whitelist of countries that satisfy the requirements of APP 8.2(a).

8.23 The OAIC notes the European experience of creating 'adequacy' lists, which suggests that there are practical difficulties in establishing such a list. EU Adequacy Decisions have been subject to long and costly negotiations. To date, only 12 countries have received an Adequacy Decision from the EU Commission.

8.24 If the Australian Government were to develop a whitelist, it would be important to give due consideration to the available mechanisms for an individual to enforce protection as required under APP 8.2(a)(ii). The Schrems Decision draws attention to the need to consider the broader legal frameworks and practices that the receiving country's privacy framework is subject to in order to accurately assess whether an equivalent standard of protection is reached. The Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield as a mechanism for transferring data between the EU and the US.[193] The CJEU found that the ability of US public authorities to access personal data were not sufficiently limited or subject to effective redress mechanisms made available to data subjects. As such, the CJEU found that the EU Commission's Adequacy Decision in relation to the EU-US Privacy Shield disregarded the requirements of providing an adequate level of protection required under the GDPR

[190] Currently there are around 36 CBPR certified companies. See directory of CBPR certified companies at: http://cbprs.org/compliance-directory/cbpr-system/.

[191] *Privacy Act 1988* (Cth) APP 8.2(a)(i).

[192] *Privacy Act 1988* (Cth) APP 8.2(a).

[193] *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems,* (2020) C-3111/18

and the rights established under the EU Charter of Fundamental Rights of the European Union.

8.25 This Decision highlights the importance of maintaining contemporary privacy frameworks and actively monitoring legal and cultural developments that might impact the effectiveness of data protection standards.

Recommendation 46 – Consider whether additional legislated transfer mechanisms could enhance the APP 8 accountability approach. These could include:

- Contractual safeguards (to support an APP entity's accountability under APP 8.1, rather than an exception to accountability under APP 8.2)
- Certification
- 'Adequacy' or whitelists

Extraterritorial application of the Act

49. Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?

8.26 Section 5B of the Privacy Act establishes the extraterritorial reach of the Act. In particular, the Privacy Act will extend to an act done or practice engaged in outside Australia by an organisation that has an Australian link. One way of establishing that an organisation has an Australian link is if the organisation carries on business in Australia (s 5B(3)(b)) and collected or held the personal information in Australia at the time of the breach (s 5B(3)(c)).

8.27 It should be noted that an act or practice of an organisation done or engaged in outside Australia and an external Territory will not be an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country (s 13D). The review may wish to consider if this provision is remains fit for purpose.

8.28 As the Issues Paper notes, the extraterritorial application of the Act is intended to capture multinational corporations based overseas with offices in Australia, as well as entities with an online presence, but no physical presence in Australia. An increasing number of the matters being considered by the Commissioner present factual situations that enliven s 5B(3) of the Privacy Act.

8.29 Large multinational companies often provide services to Australian customers through an entity in the corporate group located overseas. Often, the personal information collected from those customers by the original company is transferred to other company group members in different overseas jurisdictions for processing and storage. Such transfers are generally permitted by s 13B of the Privacy Act. When a

breach of the Privacy Act occurs, there could potentially be multiple companies within the multinational group involved, in different locations and performing different functions.

8.30 Similarly, foreign businesses may collect and trade in data about Australians but may not collect Australians' information directly from Australia. They may collect personal information from a digital platform that does not have servers in Australia. When a breach of the Privacy Act occurs, a threshold issue will be to establish that these businesses collect or hold personal information in Australia.

8.31 It can be resource intensive to establish jurisdiction under s 5B(3), particularly against motivated and well-resourced international companies. The OAIC therefore considers that there are opportunities for the extraterritorial operation of the Privacy Act to be enhanced, to more effectively address the privacy risks posed to Australians by overseas companies.

8.32 It is particularly important to ensure that there is certainty about the entities that the Privacy Act applies to in light of the proposed online platforms code, which will apply to social media services, data brokerage companies and other entities that trade in personal information.

8.33 The OAIC has identified options for potential reform of the extraterritorial operation of the Privacy Act, which we consider could address the issues raised above. The OAIC recommends that the Privacy Act review consider these options further:

- Remove the requirement in s 5B(3)(c) for the information to have been collected or held in Australia be removed, and instead the collection or holding of information could be considered an indicator of 'carrying on a business in Australia' (discussed further below). The effect of removing this provision would be that the Commissioner would only need to establish that a foreign company carries on business in Australia. This would generally align with the extra-territorial operation of the *Competition and Consumer Act 2010 (Cth)*,[194] and would be closer to the extraterritorial operation of the New Zealand Privacy Act.
- Amend s 5B(3) to refer to particular indicators of 'carrying on business in Australia' for the purposes of the Privacy Act. For example, an entity is considered to be 'carrying on business in Australia' if the entity collects and/or holds personal information about an individual who is located in Australia. Additionally, some of the elements in the Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 could be elevated into s 5B(3) as indicators. For example, the Explanatory Memorandum says 'a collection is taken to have occurred "in Australia" where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the Privacy Act, entities such as those described above who have an online presence (but no physical presence in Australia), and collect personal

[194] *Competition and Consumer Act 2010* (Cth) s 5.

information from people who are physically in Australia, carry on a "business in Australia or an external Territory".'

- To address the issue of disclosures within a corporate group, where the recipient entity is not covered by the Privacy Act, the review could consider extending the extra-territorial operation of the Privacy Act to a body corporate that has collected Australians' personal information from a related body corporate to which s 5B(3) applies (irrespective of whether it carries on business in Australia in its own right). This approach appears to be consistent with the intention with the note in s 13B of the Privacy Act, which indicates that related bodies corporate that receive personal information from a related entity should be covered by the Privacy Act.

8.34 The OAIC considers that the extraterritoriality provisions in s 4 of the new Privacy Act 2020 (NZ) provide a good model for reform of the Privacy Act. The NZ Act builds on the Australian extraterritoriality framework with some of the clarifications or additions proposed above, for example:

- Section 4(1)(b) says the NZ Act applies to an overseas entity (B) 'in relation to any action taken by B in the course of carrying on business in New Zealand in respect of personal information collected or held by B.'
- Section 4(2)(a) and (b) of the NZ Act clarify that it does not matter where the personal information was collected or held by the agency in order for it be carrying on business in New Zealand (in contrast to s 5B(3)(c) of the Australian Privacy Act).
- Section 4(3) of the NZ Act clarifies that certain elements do not have to be present in order for an entity to be treated as carrying on business in New Zealand, for example, it does not have to have a place of business in New Zealand (section 4(3)(a)) or receive any monetary payment for the supply of goods or services (section 4(3)(c)).

Recommendation 47 – Amend the Privacy Act to address issues with the extraterritoriality of the Act, including:

- Remove the requirement in s 5B(3)(c) for the information to have been collected or held in Australia be removed, and instead the collection or holding of information could be considered an indicator of 'carrying on a business in Australia'.
- Amend s 5B(3) to refer to particular indicators of 'carrying on business in Australia' for the purposes of the Privacy Act.
- Extend the extraterritorial operation of the Privacy Act to a body corporate that has collected Australians' personal information from a related body corporate to which s 5B(3) applies (irrespective of whether it carries on business in Australia in its own right).

Adequacy

52. What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

8.35 Many international privacy frameworks prohibit the flow of personal data to jurisdictions that do not provide a sufficient level of protection. It is therefore important to ensure that Australia's privacy framework does not fall behind international standards in order to support Australian businesses competitive participation in the global digital economy.

8.36 Across the globe, the GDPR is considered a high standard of data protection, and many jurisdictions that are introducing privacy legislation for the first time are looking to the GDPR as a model. However, Australia has a well-established privacy framework, which is a product of our culture and norms. A formal EU Adequacy Decision does not require Australia's framework to be a mirror of the GDPR. Instead, a formal EU Adequacy Decision recognises that Australia provides a comparable level of protection.[195]

8.37 Many of the OAIC's recommendations throughout this submission support the interoperability of the Privacy Act with global privacy laws, including the GDPR, and assist Australian entities to satisfy their global counterparts that Australia's privacy framework provides similar levels of coverage and protection. For example, the OAIC's recommendations 27, 28 and 29 to extend the Privacy Act to small businesses, employee records and political parties would assist in demonstrating comparability and in efforts to achieve an EU Adequacy Decision, should the Australian Government decide to seek this.[196]

8.38 A formal EU Adequacy Decision may also elevate the international perception of Australia's privacy framework and assist in establishing Australia's framework as providing an adequate level of protection, and thus being interoperable, with jurisdictions beyond the EU. This may have an added benefit in assisting other countries that are evaluating Australia's privacy framework.

8.39 Regardless of whether Australia seeks an Adequacy Decision, EU entities transferring data to Australian entities will need to satisfy themselves that the transferred data is subject to an essentially equivalent level of protection in Australia. This was highlighted in the Schrems Decision, which found that where an EU entity was relying on Standard Contractual Clauses under Article 46 of the GDPR, they must consider the broader environment of the overseas recipient, and the impact that might have on their ability to provide essentially equivalent protections.[197] The Schrems Decision is

---

[195] General Data Protection Regulation, Article 45 (1).

[196] Note that the predecessor to the European Data Protection Board, the Article 29 Working Party issued an Opinion which raised concerns that the exemptions under the *Privacy Act 1988 (Cth)* meant that Australia could only be considered adequate if appropriate safeguards were introduced to meet the Working Party's concerns. See: Article 29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.

[197] *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems,* (2020) C-3111/18.

likely to have implications for the international flow of data because it requires a rigorous assessment of not just the privacy frameworks, but also the broader cultural environment that the transferred data is subject to, in order to determine whether essentially equivalent protections are provided. A formal EU Adequacy Decision would alleviate the need for EU and Australian entities to take further steps in assessing the effectiveness of the Article 46 GDPR transfer tool being used and considering whether additional safeguards are needed.[198]

8.40 The importance of ensuring that Australia's Privacy Act is interoperable with global privacy laws therefore goes beyond the formal processes for seeking adequacy under the GDPR. As different approaches are adopted around the world, it is important that Australia's domestic frameworks remain interoperable, so that data can flow across borders whilst also protecting personal information.

Challenges of implementing the CBPR System in Australia

50. What (if any) are the challenges of implementing the CBPR system in Australia?

8.41 As noted in the Certification section in Part 7 of this submission, the OAIC supports the introduction of an independent third-party certification scheme. Privacy certification schemes have a role to play in facilitating overseas transfers of personal information. An independent certification mechanism could also significantly increase the transparency of organisations' data practices

8.42 The APEC CBPR System operates as a regional certification scheme and requires certified businesses to demonstrate compliance with a commonly understood set of privacy standards. The APEC Joint Oversight Panel of the Data Privacy Subgroup endorsed Australia's application to participate in the CBPR System in 2018.

8.43 The Issues Paper notes that one way of incorporating the CBPR system requirements into Australian law is through a code developed under Part IIIB of the Act.

8.44 As outlined in more detail in Part 3, there are certain limitations with the existing APP code framework under Part IIIB. In relation to the CBPR system, the development of a code would require the Commissioner to identify a code developer, who would then be responsible for developing the code and ensuring that it adequately gives effect to the requirements of the CBPR system. The code developer must also ensure that appropriate consultation takes place with relevant stakeholders, including the public and the OAIC. A CBPR code would need to apply to a broad range of entities across the economy, making it challenging to identify a code developer that is representative of the entities that the code would cover.

8.45 The OAIC's Recommendation 14 to provide the Commissioner with the power to develop an APP code in the first instance would enable the OAIC to have leadership

[198] European Data Protection Board, Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020, pg. 10.

over the development of a CBPR code and ensure that it fully and adequately gives effect to the requirements of the CBPR system.

Part 9: Enforcement powers under the Privacy Act and role of the OAIC

53. Is the current enforcement framework for interferences with privacy working effectively?

54. Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?

55. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?

    a. If so, what should these enforcement mechanisms look like?

9.1 The OAIC's core purpose is to promote and uphold privacy rights in Australia. Promoting awareness of, and facilitating compliance with, the Privacy Act are two key ways in which the OAIC achieves this purpose and builds a culture of respect for the right to privacy in Australia. As part of this role, the OAIC seeks to use its current regulatory powers effectively and efficiently to secure appropriate outcomes for the Australian community. The OAIC's visibility, experience and expertise helps to foster confidence that privacy rights will be defended. This confidence is integral to individuals' trust in the information handling practices of APP entities.

9.2 However, the OAIC's regulatory experience indicates that additional mechanisms to the current privacy regulatory framework are required to ensure that the OAIC can continue to meet community expectations of a contemporary regulator. It is essential that the Privacy Act provides the OAIC with robust enforcement mechanisms that ensure individuals have access to a quick and effective remedies for the protection of their privacy rights and that create incentives for active compliance by APP entities.

9.3 This is particularly important in light of the increasing volume of data held by business and government, the global nature of the digital economy, and the breadth of entities regulated by the Privacy Act, from Government to private sector entities across the economy.

9.4 Reforms are required to ensure that the regulatory and enforcement framework under the Privacy Act are flexible and able to respond to emerging privacy issues over the coming years. The OAIC must have the right regulatory tools available to take a pragmatic, proactive and proportionate approach to regulation. This includes enhanced provisions to work cooperatively with international regulators to investigate matters of global concern jointly, using commensurate powers.

9.5 This approach requires a shift in emphasis in the current framework to ensure that the Commissioner can carry out their statutory functions in a manner that is appropriate in the digital age. At a high level, this requires the following changes:

- The Commissioner should be provided with more discretion in choosing when to exercise powers to investigate individual complaints to allow the OAIC to identify sectors and acts or practices of concern and prioritise matters accordingly.
- The Commissioner should be provided with enhanced enforcement powers and regulatory tools to effectively deter inappropriate conduct and support privacy best practice.

9.6 The OAIC must also be appropriately resourced to properly carry out its statutory functions and use the full suite of regulatory powers effectively, including enforcement through the courts, which can be costly and resource intensive. It is notable that the UK Information Commissioner's Office, which has investigated and imposed fines in a number of high profile and complex matters, is supported by a large office made possible by the requirement for entities to pay a 'data protection fee', supporting the office's funding.[199]

9.7 These recommendations are considered in more detail below.

Snapshot of OAIC's current framework

9.8 The Privacy Act currently confers a range of regulatory powers on the Commissioner, including investigation and enforcement powers. These powers are based on an escalation model. The OAIC considers that the Act's premise of taking a linear escalation approach to regulation is no longer the most efficient model. Rather, the Privacy Act should provide a flexible tool kit of regulatory options, supported by appropriate powers and enforcement processes. This would enable the OAIC to take the most proportionate and effective action in the circumstances. This is more akin to a risk-based approach to regulation.[200]

9.9 The OAIC currently has powers that allow it to work with APP entities to facilitate compliance and promote best privacy practice. These include powers to:

- request an entity, group of entities, body or association to develop an APP code, or the CR code, and apply to the Commissioner for the code to be registered, or for the Commissioner to develop the code and register it (ss 26E(2), 26G, 26P(1) and 26R)
- direct an agency (but not an organisation) to give the Commissioner a privacy impact assessment (PIA) (s 33D)
- monitor, or conduct an assessment of, whether personal information is being maintained and handled by an entity as required by law (ss 28A and 33C)
- direct a regulated entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach under Part IIIC of the Privacy Act (s 26WR).

---

[199] UK Information Commissioner Office, *Data Protection Fee* [Online document], UK ICO website, accessed 22 November 2020.

[200] For more details, see Sparrow, M. (2008). *The Character of Harms: Operational Challenges in Control*. Cambridge: Cambridge University Press.

9.10 The OAIC's regulatory powers to investigate or otherwise deal with an alleged interference with privacy include powers to:

- investigate a matter following a complaint (s 40(1)) or on the Commissioner's own initiative (referred to as a 'Commissioner initiated investigation' (CII)) (s 40(2))
- attempt to conciliate a complaint (s 40A)
- decline to investigate, or further investigate, a complaint in certain, specified circumstances (s 41)
- conduct preliminary inquiries to determine whether or not to open an investigation (s 42)
- require information or a document to be produced, or a person to attend before the Commissioner (ss 44–45)
- refer a complaint to an alternative complaint body specified in s 50
- enter premises and inspect relevant documents by consent or with a warrant (s 68).

9.11 Enforcement powers, that range from less serious to more serious regulatory action, include powers to:

- accept an enforceable undertaking (s 33E)
- make a determination (s 52)
- seek an injunction including before, during or after an investigation or the exercise of another regulatory power (s 98)
- apply to the court for a civil penalty order for a breach of a civil penalty provision (s 80W).

9.12 The OAIC exercises these powers as far as possible under the current scheme to select the most appropriate regulatory tool in the circumstances, in order to take a proportionate and risk-based approach to regulation. The OAIC expects that a proportion of the Commissioner's regulatory activity will need to continue to focus on detection, deterrence, rectification and remedy through the use of regulatory functions such as guidance, advice, monitoring, conciliations, assessments and administrative warnings.

9.13 However, there is a need to take more substantive regulatory and enforcement action on the Commissioner's own initiative in order to shift the behaviour of regulated entities across sectors, rectify, remedy and provide broader deterrence. This requires sufficient regulatory tools and powers, as well as resources.

9.14 The OAIC also considers collaboration to be a key part of its regulatory toolkit. The OAIC is continuing to develop and participate in arrangements that support international cooperation in investigation and the enforcement of privacy and data protection laws, including the APEC Cross-border Privacy Enforcement Arrangement and Global Privacy Enforcement Network. The OAIC has recently opened a joint investigation with the UK ICO.

9.15 Collaboration also includes working with other Australian regulators to ensure the protection of consumers, for example, as co-regulators for the Consumer Data Right.

The OAIC is experiencing sustained activity across our regulatory functions, which can be attributed to changes in the regulatory environment, the data practices of entities, and a growing desire of the community to protect their privacy rights:

- An increasing focus on addressing systemic privacy acts/practices, particularly in the online space, through CIIs. During the 2019-2020 reporting period, the OAIC commenced 27% more privacy CIIs and finalised 200% more privacy CIIs than the previous financial year.
- Complaints received have generally increased year on year (2018-19: 12.1% increase; 2017–18: 18% increase; 2016–17: 17% increase) with the exception of 2019-2020 (a decrease of 20%), which is likely due to the COVID-19 pandemic.
- Rising numbers of data breaches being reported to the OAIC since the introduction of the NDB scheme, with 2019-20 seeing an increase of 11% in the number of notifications compared to 2018-2019 (as well as a 733% increase in data breach notifications after reporting became mandatory).

Addressing the OAIC's regulatory priorities

9.16 The OAIC has identified four areas of privacy regulatory priority for 2020-2021:

- online platforms and social media
- the security of personal information, particularly in the finance and health sectors
- the Consumer Data Right
- COVID-19 personal information handling practices.

9.17 These priorities reflect a focused, targeted approach to privacy regulation, which the OAIC considers is the most effective use of the agency's resources to derive the greatest benefit for Australians and the regulated community. This involves identifying sectors in government or industry, or recurring acts or practices, where the OAIC believes privacy regulatory action is necessary to have a significant impact on the protection and handling of personal information.

9.18 The OAIC takes a whole-of-agency approach to these priority areas, targeting the Commissioner's proactive policy and assessment functions to drive privacy best practice, as well as focus its investigation (including CII and complaint handling functions) and enforcement powers to deter systemic privacy misconduct where appropriate.

9.19 To enable this approach, however, the Commissioner must have discretion to select the appropriate regulatory tool that best addresses the privacy issues occurring in the particular sector or stemming from the recurring acts or practices, and strike the right

balance between these proactive, investigative and enforcement activities and handling individual complaints.

9.20 The OAIC must also have the ability to target its limited resources to the areas of highest risk and need. The OAIC's complaint-handling function serves as an important deterrent for inappropriate acts or practices and provides redress for individuals. It also serves as an important source of intelligence on emerging privacy issues to help the OAIC determine its regulatory priorities.

9.21 However, the OAIC is currently required to investigate all complaints, at least to the extent required to satisfy itself that a ground to cease investigating exists.[201] This can be resource intensive and limit the ability for the Commissioner to take a targeted or systemic approach to regulation.

9.22 It is important for the OAIC to be able to effectively prioritise matters and direct public funds towards resolving issues that have systemic importance or where more serious misconduct or harms have occurred.

9.23 There are several amendments to the Privacy Act that will allow the Commissioner more flexibility in dealing with complaints.

9.24 Under s 40(1), the Commissioner is currently required to investigate all complaints. The OAIC recommends replacing the words 'shall investigate' with 'may investigate' in this provision. This would give the Commissioner more discretion to investigate or decline complaints to enhance the OAIC's ability to take a more targeted approach to privacy regulation. It would be more consistent with s 41(1), which sets out the circumstances where the Commissioner does not need to investigate complaints.

9.25 The Explanatory Memorandum could specify that the intention of this change is to clarify that the Commissioner may exercise discretion to investigate based on factors such as the Commissioner's regulatory policies and priorities and whether the resources needed to investigate a complaint are proportionate to the likely outcome or remedy available.

9.26 An additional amendment to s 41(dc) would also allow the Commissioner to more appropriately deal with complaints. Section 41(dc) allows the Commissioner to decline to investigate, or further investigate, a complaint that is being dealt with by a recognise external dispute resolution scheme (EDR scheme). The OAIC recommends that this ground be extended to instances where a complaint has already been adequately dealt with by an EDR scheme.

9.27 The Commissioner must also have discretion to take a risk-based, proportionate approach in selecting the appropriate regulatory tool, having regard to the nature of the entity and the conduct in question. For example, where an investigation is not warranted, greater use could be made of administrative warnings to notify entities

[201] Privacy Act, s 40(1) and s 41.

that allegations had been made and provide an opportunity to educate through guidance on privacy obligations.[202]

9.28 This is particularly important given the nature of the APPs, which are scalable based on the relevant circumstances, and the wide range of entities that the OAIC regulates, which range from small health providers to large multinational corporations to Australian Government agencies. Different approaches are required to apply this principles-based law to these very different entities, and the privacy framework should facilitate this flexibility.

9.29 This discretion will also be important if the current exemptions in the Privacy Act are removed (see Recommendations 27, 28, 29 and 30).

9.30 Additionally, where the OAIC has declined to investigate a complaint, individuals may rely on a direct right of action to seek a remedy in the courts (see Part 10).[203] The Commissioner should also be provided with the appropriate powers to decline to investigate a complaint where it is more appropriately dealt with in the courts, or where the matter is or has been before the court (see Recommendation 53).

Recommendation 48 – Amend s 40(1) to replace the words 'shall investigate' with 'may investigate' and clarify in the Explanatory Memorandum that this change is to allow the Commissioner to exercise discretion to investigate based on factors such as the Commissioner's regulatory policies and priorities, whether the resources needed to investigate a complaint are proportionate to the likely outcome or remedy available and whether the substance of the complaint is about matters that fall under the Privacy Act.

Recommendation 49 – Expand s 41(dc) to instances where a complaint has already been adequately dealt with by an EDR scheme.

---

[202] Australian Communications and Media Authority (2020), *Spam compliance alerts* [Online document], ACMA website, accessed 11 November 2020 and Australian Communications and Media Authority (2020), *Telemarketing compliance alerts* [online document], ACMA website, accessed 11 November 2020

[203] The relationship between a complaint handling function and a direct right of action was recently explained in the Office of the Privacy Commissioner of Canada (2019) *2018-2019 Annual Report to Parliament on the Privacy Act* [online document], OPCC website, accessed 25 November 2020:

> *Currently, the Commissioner does not have the power or authority to refuse or discontinue complaints under the Privacy Act, though he does under PIPEDA in certain defined circumstances. We have recommended to Parliament that the law should provide our Office with the ability to choose which complaints to investigate, in order to focus our limited resources on issues that pose the highest risk or may have the greatest impact for Canadians. At the same time, to ensure no one is left without a remedy, a modernized law must also give individuals a private right of action for violations to ensure they can pursue recourse.*
>
> *Our Office, like many of our privacy and data protection counterparts, upholds several mandates with finite resources. Where our Office does not proceed with an investigation of a complaint, individuals should have the right to seek judicial redress on their own accord. This would help ensure that individuals' rights are respected and they are not left without a remedy. This right exists in the GDPR and is being considered elsewhere. For example, the New York privacy act that was before the State Senate Consumer Protection Committee at the time of drafting this report seeks to provide individuals with the right, among others, to sue companies directly over privacy violations.*

Expanding the OAIC's enforcement mechanisms

9.31 The Australian community is increasingly expecting the OAIC to take a more enforcement-focused approach where appropriate. The OAIC considers that such an approach is necessary in order to achieve regulatory objectives of deterrence and rectification on a broad scale.

> The vast majority (83%) of Australians are wanting the government to do more to protect the privacy of their data. This includes being protected against harmful practices, with 84% believing personal information should not be used in ways that cause harm, loss or distress. [204]

9.32 Additional enforcement will also benefit regulated entities by creating precedents that will clarify and particularise the principles-based APPs.

9.33 To meet these community expectations, the OAIC considers that the Commissioner's enforcement mechanisms must be enhanced to provide a credible deterrent against privacy infringements and bring the OAIC into line with comparable domestic and international regulators. As the collection, use or disclosure of personal information is being increasingly monetised, it is also essential that the Commissioner's enforcement powers are sufficient to reduce the likelihood of APP entities treating breaches of the Privacy Act as a cost of doing business.

9.34 The OAIC recommends the introduction of several amendments discussed below, which will enhance the Commissioner's enforcement powers and provide more flexible regulatory tools.

9.35 The review should also consider appropriate pecuniary enforcement options. Under the existing framework, the Commissioner has limited pecuniary enforcement options to address interferences with privacy. To address this issue, the OAIC recommends the following reforms:

- **Introducing civil penalties for interferences with privacy** – The Commissioner can currently only seek civil penalties for the most egregious conduct. Providing the Commissioner with the power to seek civil penalties for interferences with privacy would send a strong message about the importance of privacy compliance while providing the OAIC with the discretion to seek civil penalties where this is the appropriate regulatory tool. Whether an act or practice is serious or repeated would be aggravating factors that would guide the Commissioner's discretion.
- **Empowering the Commissioner to issue public infringement notices for interferences with privacy** – Introducing an infringement notice power will complement existing regulatory options and respond to interferences with privacy through cost-efficient deterrence. It will help address the risk that declarations to change acts and practices through a s 52 determination of a Commissioner-initiated

[204] See OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research, p. 8

investigation lack strength and proportionality when compared with pecuniary options issued by other regulators, domestically and internationally. The quantum of infringement notices would need to be calibrated to ensure it is acts as an adequate deterrent and not a cost of doing business while still providing an incentive for a respondent to avoid going to court. The OAIC recommends the legislation take a tiered approach, fixing the quantum of infringement notices based on the type of APP entity that is the subject of the action.[205]

9.36 These powers would be exercised in accordance with the OAIC's Regulatory action policy[206] and Guide to privacy regulatory action,[207] as amended, which set out the factors that inform the Commissioner's discretion when selecting the most appropriate power in the circumstances. This includes the specific and general educational, deterrent or precedential value of the particular privacy regulatory action. This transparent, consistent and proportionate approach to enforcement is similar to comparable domestic[208] and international regulators.[209]

9.37 The Commissioner is unlikely to seek civil penalties for minor or inadvertent contraventions, where the responsible entity has cooperated with the investigation and taken steps to avoid future contraventions.[210] There are, however, circumstances where seeking a civil penalty for an interference with privacy will provide the best outcome, having regard to the OAIC's regulatory action policy.[211] For more (relatively) minor instances of misconduct which nonetheless merit a civil penalty, or where the resources involved in going to court are disproportionate to the potential civil penalty, the OAIC anticipates that an infringement notice would be used to provide a quick and cost-effective deterrent.

There are several situations where seeking a civil penalty for an interference with privacy or issuing an infringement notices may be appropriate for conduct that may

---

[205] See for example the ACCC's Guideline on the use of infringement notices which states that the value of infringement notices will vary based on whether the subject is an individual, corporation or listed corporation.

[206] OAIC (May 2018) '*Privacy regulatory action policy*' [online document], OAIC, accessed 10 November 2020

[207] OAIC (May 2018) '*Guide to privacy regulatory action*' [online document], OAIC, accessed 10 November 2020

[208] See for example chapters on Compliance and enforcement strategy and Priority factors ACCC (n.d.) *Compliance & enforcement policy & priorities* [online document], ACCC website, accessed on 11 November 2020 and ACCC (July 2020), *Infringement Notices: Guideline on the use of infringement notices by the Australian Competition and Consumer Commission*, ACCC, Australian Government p. 3-5; In relation to ASIC, see discussion of infringement notices and how ASIC decides which enforcement tools to use in ASIC (n.d.) *Information Sheet 151: ASIC's approach to enforcement*, ASIC, Australian Government p. 4-9; See ACMA's compliance and enforcement approach in ACMA (n.d.) *Compliance and enforcement policy* [online document], ACMA website, accessed on 11 November 2020 and ACMA (2019) *Regulatory guide No. 5 – Infringement Notices*, ACMA, Australian Government, p. 3-4

[209] For example, UK ICO (n.d) Regulatory Action Policy, which sets out its objectives for regulatory action (p. 6-7) and relevant factors when selecting the appropriate regulatory action including the nature and seriousness of the breach, the types of information affected and the level of privacy intrusion, whether the incident raises new issues and the public interest in regulatory action being taken (10-13).

[210] OAIC (May 2018) '*Guide to privacy regulatory action*' [online document], OAIC website, accessed 10 November 2020, [6.17]

[211] OAIC (May 2018) '*Privacy regulatory action policy*' [online document], OAIC website, accessed 10 November 2020, [38]

not meet the s 13G threshold. While each situation will be assessed on its merits, these circumstances could include:

- An eligible data breach involving a very large data set of personal (but not sensitive) information.
- An entity mishandling personal information where unjustified adverse impacts flowing to individuals due to the breach cannot be established because of poor record keeping by a respondent.
- Some instances where an APP entity has failed to notify individuals of an eligible data breach as soon as is practicable in accordance with s 26WL.

9.38 The review should also consider the conduct-orders that are available to the Federal Court. While the Commissioner can make a s 52 determination requiring changes in conduct, they cannot seek these orders from the court in civil penalty procedures. In practice this often means that the Commissioner must choose between seeking financial penalties in the courts or making a s 52 determination for an APP entity to change its conduct.

9.39 The OAIC recommends that the conduct orders available to the Commissioner when making a s 52 determination should be available to the Federal Court when the Commissioner seeks civil penalties.

9.40 Additionally, the orders available to the Commissioner when making a determination under s 52 after investigating a complaint or CII should also be enhanced with the following amendments:

- **Order to identify and mitigate foreseeable risks** - The loss or damage that may result from an interference with privacy may not be immediately apparent, particularly harms that occur because of a notifiable (eligible) data breach. The Commissioner can make orders to require respondents to perform any reasonable act or course of conduct to redress any loss or damage suffered. This should be enhanced to require respondents to perform any reasonable acts or course of conduct to identify and mitigate any foreseeable loss or damage. This may include requiring an APP entity to monitor whether information the subject of an eligible data breach has been published for sale on the dark web.
- **Order to delete personal information** - Where the Commissioner finds that an APP entity has collected information inappropriately, the Commissioner does not have an express order for the entity to delete this information. This means that an APP entity may be allowed to retain improperly collected personal information and potentially benefit from this conduct. The Commissioner should have an express power to order that a person or APP entity delete personal information where the Commissioner finds that this information was collected in contravention of the Privacy Act.

9.41 The Commissioner's information gathering powers, set out in Part V of the Privacy Act, are essential to the Commissioner carrying out their functions effectively. These include the power to obtain information and documents, as well as to require

attendance at compulsory conferences. Failure to respond to these powers may result in criminal penalties.[212]

9.42 The Commissioner also has access to more extensive powers to seek a warrant to enter a premises without consent. Given the substantial impositions on the rights of APP entities, the Commissioner will only use these powers as an investigative tool in investigations where it is warranted in the circumstances.

9.43 The OAIC considers, however, that these information gathering powers need to be enhanced to ensure they remain effective, allow a case to be developed that will meet evidentiary requirements and are consistent with comparable regulators. Accordingly, the OAIC recommends that the review enhance these powers by introducing the following amendments:

- **Infringement notice power** – In addition to the infringement notice powers recommended above, the Commissioner should be empowered to issue an infringement notice where a person fails to provide information, answer a question or produce a document or record when this has been required under the Privacy Act. This would be an effective measure to promote greater co-operation with the regulatory activities of the office across both complaint handling and in circumstances where the Commissioner commences an investigation on their own initiative.
- **Search and seizure powers** – While the Commissioner can seek a warrant to enter a premise under s 68, this only expressly allows the OAIC to inspect the relevant documents. These powers are inadequate and inconsistent with comparable domestic[213] and international regulators.[214] This power should expressly permit the Commissioner to make copies of information and documents specified in the warrant and operate electronic materials to determine whether the kinds of information and documents specified in the warrant are accessible.
- **Prevent the destruction of evidence** – The Commissioner should have the power to seek a warrant to preserve or secure information and documents where there is a possibility that a person may destroy such materials or cause it them be unavailable for use in an investigation.[215] It should also be an express offence to destroy evidence that may be reasonably required by the Commissioner.

There are several examples of where further information gathering powers would promote co-operation with the Commissioner's investigative and complaint-handling processes:

---

[212] Privacy Act, s66

[213] See for example the ACCC has powers to apply for warrants to enter and search premises, make copies of evidence specified in the warrant and operate electronic materials to see whether the kind of evidential material specified in the warrant is accessible (*Competition and Consumer Act 2010*, s154A and 154G). ASIC has similar powers under the *Corporations Act 2001*(see for example s530C), the *Australian Securities and Investment Commission Act 2001* (see for example s37) and the *Crimes Act 1914* (see Division 2 of Part IAA).

[214] See for example the UK ICO's search and seizure powers under schedule 15 of the *Data Protection Act 2018*.

[215] This power could be modelled on r7.43 of the *Federal Court Rules 2011* (Cth) or s 530C of the *Corporations Act 2001* (Cth).

- A complainant sought health information from an APP entity under APP 12. The APP entity refused to provide this information to the OAIC, even after receiving a notice under s 44 of the Privacy Act, which caused undue delay in handling the complaint.[216]
- Data protection authorities internationally have entered entities' premises to seize evidence, particularly in circumstances where there was concern that evidence would be destroyed.[217]
- While making preliminary inquiries into a potential breach of the Privacy Act, it became apparent that relevant evidence was held by a subcontractor who was also a small business operator exempt from the Act. In the course of the investigation, the subcontractor started deleting the relevant information. This impacted the ability to gather necessary evidence into the potential contravention by the regulated entity and delayed the preliminary inquiries.

Recommendation 50 – Introduce the following amendments to the enforcement mechanisms under the Privacy Act:

- empower the Commissioner to issue infringement notices for interferences with privacy and where a person fails to give information to the Commissioner when this has been required under the Privacy Act
- introduce civil penalties for interferences with privacy
- provide the Federal Court with the power to make the conduct orders which are available to the Commissioner through a s 52 determination
- allowing the Commissioner to make order in a s52 determination requiring respondents identify and mitigate foreseeable risks or delete personal information
- enhance the Commissioner's search and seizure powers to allow the OAIC to make copies of information and documents specified in the warrant and operate electronic materials to determine whether the kinds of information and documents specified in the warrant are accessible
- empower the Commissioner to seek a warrant to preserve and secure relevant information and documents.

[216] For example, see recent privacy determinations by the Commissioner: 'VU' and 'VV', 'VW' (Privacy) [2020] AICmr 52 (14 September 2020), 'VJ', 'VK', 'VL' and 'VM' (Privacy) [2020] AICmr 45 (2 September 2020) and 'VN' and 'VM' (Privacy) [2020] AICmr 46 (2 September 2020)

[217] See for example UK ICO (2018) Investigation into the use of data analytics in political campaigns [online document], UK ICO, United Kingdom Government, p. 33

Part 10: Direct right of action

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

10.1 The OAIC supports the introduction of a direct right of action for individuals to seek compensation for an interference with their privacy under the Privacy Act. A direct right of action would give individuals greater control over their personal information by providing an additional avenue of redress under the Privacy Act. It would also provide an additional incentive for APP entities to comply with their privacy obligations.

10.2 A direct right of action would complement the OAIC's recommended enhancements to the Commissioner's enforcement powers (see Part 9, above), providing individuals with the right to seek judicial redress of their own accord, in addition to the suite of regulatory outcomes available from the OAIC. This proposal is also consistent with the OAIC's 2020 ACAPs results, which showed that 78% of respondents believe that they should have the right to seek compensation in the courts for a breach of privacy.

10.3 Several domestic regulatory regimes already enable individuals to directly take action in court to seek compensation for breaches of the law. For example, under the CDR regime in the *Competition and Consumer Act 2010* (Cth), individuals have the right to bring an action for damages against another person for breach of the privacy safeguards or the Consumer Data Rules (to the extent that those rules relate to the privacy safeguards or to the privacy or confidentiality of CDR data).[218]

10.4 More broadly, a direct right of action would bring the Australian privacy framework into line with other international jurisdictions including the United Kingdom, New Zealand, Japan, Singapore and the European Union.

Framing a direct right of action

10.5 The OAIC supports the ACCC's recommendation in the DPI final report that individuals should have a direct right to bring actions and class actions against APP entities in the Federal Court or the Federal Circuit Court to seek compensatory damages, as well as aggravated and exemplary damages (in exceptional circumstances), for the financial and non-financial harm suffered as a result of an interference with privacy under the Privacy Act.[219]

10.6 The OAIC has a number of recommendations, set out below, about the way that a direct right of action should be framed under the Privacy Act. In making these recommendations, the OAIC acknowledges the need to balance the benefits of a direct

[218] *Competition and Consumer Act 2010* (Cth), s 56EY.

[219] Australian Competition and Consumer Commissioner, *Digital Platforms Inquiry Final Report* (June, 2019), 472.

right of action for individuals and APP entities with the need to ensure that court resources are being appropriately directed and are not taken up by trivial breaches of the Privacy Act or APPs.

Harm threshold

10.7 The Issues Paper notes that one way of achieving this balance may be to limit the right of direct action to the courts to 'serious' breaches of the Act or APPs.

10.8 The OAIC considers that limiting the direct right of action to 'serious' breaches of privacy would substantially curtail its effectiveness. In particular, a key benefit of a direct right of action is to provide individuals with greater agency and control over the handling of their personal information. Limiting the direct right of action to 'serious' breaches would preclude many individuals from seeking recourse in the courts for breaches of their privacy. It follows that this would also limit other potential benefits, including increased opportunities for the courts to interpret the APPs and incentivising APP entities to comply with their obligations.

10.9 Several international jurisdictions with private rights of action under their domestic privacy legislation do not prescribe a particular harm threshold that must be met before an individual can seek redress in the courts.

10.10 For example, Singapore's *Personal Data Protection Act 2012* provides that any person who suffers loss or damage directly as a result of a contravention of the Act by an organisation shall have a right of action for relief in civil proceedings in a court.[220] Similarly, under Article 79 of the GDPR, data subjects have a general right to 'an effective judicial remedy against a controller or processor' where they consider that their data protection rights have been infringed as a result of non-compliance with the GDPR. Under Article 82, any person who has suffered material or non-material damage (such as emotional distress) as a result of a violation of the GDPR has the right to compensation. Compensation is the remit of the courts and cannot be awarded by supervisory authorities under the GDPR or the UK's *Data Protection Act 2018*. Supervisory authorities do, however, have the ability to impose administrative fines.

Recommendation 51 – Ensure that the direct right of action is not limited to 'serious' breaches of the Privacy Act or the APPs.

Procedural considerations

10.11 The Issues Paper highlights that a key consideration is whether individuals should first be required to undergo conciliation by the OAIC, or some other administrative body, before commencing action in the courts. Alternatively, complainants could choose which avenue to pursue in the first instance. That is, individuals could elect whether to

[220] Section 32, *Personal Data Protection Act 2012* (Singapore).

apply directly to the courts, or to seek conciliation with the OAIC, depending on their preference.

10.12 The OAIC considers that the direct right of action should be framed so that individuals are required to make a complaint to the OAIC before applying to the courts. Further, similar to the existing approach under s 41 of the Privacy Act, the Commissioner should be provided with the appropriate powers to decline to investigate a complaint where it is more appropriately dealt with in the courts. In these circumstances, the individual or class of individuals could then pursue further redress in the courts through the direct right of action.

10.13 This approach should be consistent with the existing complaint-handling provisions under the Privacy Act which do not require the OAIC to attempt to resolve the complaint through conciliation where the OAIC has decided not to investigate, or not to further investigate, a complaint.

10.14 The OAIC considers that the direct right of action would be a more appropriate vehicle for representative complaints in certain circumstances. Consistent with the above, the Commissioner should have appropriate powers to decline to investigate a representative complaint where it is more appropriately dealt with by the courts.

10.15 Additionally, the existing representative complaint provisions do not provide the OAIC with the full suite of powers that are available to the Federal Court for the management of class actions under the *Federal Court of Australia Act 1976* (Cth) (Federal Court Act). For example, s 38B(2) of the Privacy Act states that a class member in a representative complaint may opt out if the complaint was lodged without the consent of the member at any time, or otherwise at any time before the Commissioner begins to hold an inquiry into the complaint. This means that the Commissioner is unable to put a definitely timeframe on opting out. This contrasts with s 33J of the Federal Court Act, which states 'The court must fix a date before which a group member may opt out of a representative proceeding.'

10.16 Accordingly, the OAIC recommends that the representative complaint provisions under Part V of the Privacy Act are revised to ensure greater alignment with the powers of the Federal Court under the Federal Court Act in relation to the management of class actions.

10.17 The OAIC considers that this approach would continue to provide the OAIC with national oversight of privacy issues and the ability to identify potential systemic issues in the system that may warrant further regulatory or enforcement action. Additionally, it may reduce the burden on the court system by continuing to provide individuals with a free dispute resolution mechanism while still providing more direct access to the courts than the current complaint mechanisms under the Act.

Recommendation 52 – Ensure that the direct right of action is framed so that individuals are required to make a complaint, or a representative complaint, to the OAIC before applying to the courts.

Recommendation 53 – Ensure that the Commissioner has appropriate powers to decline to investigate a complaint or representative complaint, or continue to investigate a complaint or representative complaint, where the matter is more appropriately dealt with by the courts.

Recommendation 54 – Revise the representative complaint provisions under Part V of the Privacy Act to ensure greater alignment with the powers available to the Federal Court under the Federal Court Act in relation to the management of class actions.

Damages

10.18 Capping compensation may be justified on the basis that it may reduce the incentive for parties to litigate, making the right of action potentially less costly. However, capping the amount of damages that may be awarded could lead to a preponderance of lesser rather than more serious breaches of the Privacy Act coming before the courts and a lack of confidence in the direct right of action.

10.19 While most examples of direct rights of action for consumers relate to financial or other consumer complaints where loss and damage is usually easily quantifiable (i.e. it is financial harm or economic loss), the compensation regime for unlawful discrimination under the *Australian Human Rights Act 1986* (Cth) provides for damages to be awarded for non-economic loss, including hurt, humiliation and distress with no damages cap.

10.20 In quantifying such awards of damage, the decided cases indicate that awards should be restrained but not minimal, and not so low as to diminish the respect for the public policy of the legislation. Aggravated and exemplary damages have also been awarded in limited unlawful discrimination matters.

10.21 The OAIC does not consider that compensation should be capped in relation to the direct right of action under the Privacy Act. This will enable the courts through their judgments to set standards for appropriate types and levels of damages for privacy breaches taking into account the particular facts and circumstances of each case. This approach would also enable compensation amounts awarded by courts to reflect, and keep pace with, the changing landscape of privacy harms.

Recommendation 55 – Ensure that damages recoverable under a direct right of action for privacy breaches are not capped.

Role of the OAIC

10.22 A clear role for the OAIC in the direct right of action will help to ensure that the court has access to the expertise of the regulator. The Issues Paper notes this could be done by allowing the Commissioner to be heard in proceedings and provide expert assistance as amicus curiae.

10.23 The role of an intervener is to represent the intervener's own legal interests in the proceedings.[221] For example, a court's decision might have an effect on the future interpretation of laws affecting the intervener. In these circumstances, the court could give leave to the Commissioner to intervene in a case that would have future repercussions for the work of the OAIC or for regulated entities more broadly.

10.24 Other domestic regulators have specific rights in relation to direct rights of action under their legislation. Specifically, ASIC and the ACCC have rights to intervene in certain proceedings with all the rights, duties and liabilities of a party. Both ASIC and the ACCC have developed guidelines including principles to be considered when deciding whether to intervene.

10.25 An *amicus curiae* is a person who seeks to assist the court and does not involve becoming a party to the proceedings. Again, other domestic regulators have a right to seek leave of the court to appear as amicus curiae. For example, ASIC may appear as *amicus curiae* under court rules (e.g. *Federal Court (Corporations) Rules 2000*) or, where applicable, the court's own inherent authority.

10.26 Similarly, special-purposes Commissioners (as defined under various human rights legislation) have a right to assist the court as *amicus curiae*. The Commissioners' amicus curiae function can only be exercised with the leave of the Federal Court where the Court is hearing an application alleging unlawful discrimination under Division 2, Part IIB of the *Human Rights and Equal Opportunity Commission Act* (Cth). The Commissioner/s may seek leave to appear as amicus where the:

- Commissioner thinks the orders may affect to a significant extent the human rights of persons who are not parties to the proceedings
- proceedings, in the opinion of the Commissioner, have significant implications for the administration of the relevant Act/s, or
- proceedings involve special circumstances such that the Commissioner is satisfied that it would be in the public interest for the Commissioner to assist the Court as amicus.

Recommendation 56 – Supplement the direct right of action with legislative options for the OAIC to exercise:

- a right to intervene in proceedings (or alternatively to seek the leave of the court to intervene)
- a right to seek leave of the court to act in the role of amicus curiae in the proceedings.

[221] Australian Law Reform Commission (ALRC) (2014) *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123), ALRC, Australian Government, accessed 29 November 2020.

Part 11: Statutory tort

57. Is a statutory tort for invasion of privacy needed?

58. Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

11.1 The OAIC supports the proposal to enhance Australia's privacy framework by including additional remedies for invasions of privacy. A statutory tort for serious invasions of privacy would be an important addition to the suite of regulatory measures needed to address online harms. This includes the serious risks that can be posed to individuals' privacy by private individuals and entities who publish, disseminate and duplicate information, including through the use of live streaming technologies.[222]

11.2 This would generally align with previous findings and recommendations that Australia's privacy framework should include additional remedies for invasions of privacy, including recommendation 19 in the ACCC's *Digital Platform's Inquiry final report*. It would also complement the proposal to introduce a direct right of action for individuals.

11.3 Importantly, a statutory tort would provide greater coverage and protection to individuals in line with Article 17 of the ICCPR. Article 17 provides that:

- 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.
- Everyone has the right to the protection of the law against such interference or attacks.

11.4 As recommended above in relation to the direct right of action, the OAIC considers that the statutory tort be supplemented by legislative powers for the OAIC to be notified of, to exercise a right to intervene in proceedings, and to seek the leave of the court to act in the role of *amicus curiae* in the proceedings. This will be important where proceedings have the potential to impact the evolution of the Privacy Act and privacy jurisprudence and policy.

Recommendation 57 – Introduce a statutory tort for serious invasions of privacy into Australia's privacy framework.

Recommendation 58 – Supplement the statutory tort with legislative powers for the OAIC to be notified of, to exercise a right to intervene in proceedings, and to seek the leave of the court to act in the role of *amicus curiae* in the proceedings.

[222] See for example, *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (No. 38, 2019).

59. What types of invasions of privacy should be covered by a statutory tort?

60. Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

11.5 Privacy regulation operates against a backdrop of significant technological change. It is therefore critical that the legislation is formulated in a way that allows a cause of action or complaint to evolve as the circumstances require.

11.6 The ALRC previously recommended that a statutory tort cover two types of invasion of privacy: intrusion into seclusion (including by unlawful surveillance) and misuse of private information (whether true or not).

11.7 The OAIC considers that the tort should be framed flexibly to ensure that Article 17 of the ICCPR is fully implemented and that it is able to respond to the complete range of serious privacy invasive conduct that arises over time in a wide range of settings. Particularly, the mechanism should be technology neutral, in order to address privacy invasive acts and practices that may emerge as a result of technological and consequential social trends. A limited tort may be less able to adapt and apply flexibly to changing technologies and practices than a more general and comprehensive tort that applies to all serious invasions of privacy.

11.8 Further, enacting a limited tort that deals only with specific types of privacy invasion risks leaving gaps in privacy protection. For example, it is not clear that this proposed tort would provide a remedy in the case of serious invasion of an individual's bodily privacy (such as in the case of unauthorised bodily testing). While the majority of serious privacy invasions may fall within the two proposed categories, some will not and this will create further fragmentation in privacy protections.

11.9 Similarly, the OAIC does not support the cause of action being confined to intentional or reckless invasions of privacy. Negligent acts should also be covered to avoid unnecessarily limiting the application of the tort to different circumstances that may result in serious privacy invasions. To accommodate this, the tort should not specify a fault element.

Recommendation 59 – Enact a single and comprehensive tort, rather than confining the tort to intrusion upon seclusion and misuse or disclosure of private information.

Recommendation 60 – Enact a tort that does not specify a fault element to ensure it covers intentional, reckless and negligent acts.

61. How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

11.10 Previous reports into a proposed cause of action have considered that the tort will need to be formulated in a way that recognises that the right to privacy is not absolute. The right to privacy will need to recognise other competing rights, including the right to freedom of expression and the public interest in being informed about matters of public concern. The recognition of these other rights and interests will therefore be an essential part of a mechanism to redress serious privacy invasion.

11.11 The OAIC supports integrating the recognition of other public interests as part of the consideration of whether an individual's privacy has been seriously invaded. This may be a conceptually preferable way of ensuring that all relevant public interests are considered before any decision is reached that there was a serious invasion of privacy. It is preferable to raising a particular public interest consideration as a defence to a finding that an invasion of privacy has occurred.

Recommendation 61 – Include a requirement to weigh other public interests, including the right to freedom of expression and the public interest in being informed about matters of public concern, as part of the consideration as to whether an individual's privacy has been seriously invaded.

62. If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

11.12 Other changes to strengthen current laws and regulatory frameworks to better prevent or redress serious invasions of privacy is to extend the Privacy Act to entities and activities that are currently exempted, in accordance with the OAIC's Recommendations 27, 28 and 29.

11.13 Amending the current regulatory framework to remove these exemptions would provide additional protections against privacy invasion for individuals in relation to the handling of their personal information.

11.14 However, it should be noted that these improvements would apply only to information privacy and not to other types of privacy (such as bodily and territorial privacy) and would not apply to breaches of privacy by an individual (unless they were an APP entity).

Part 12: Notifiable Data Breaches scheme – impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?

64. Has the NDB Scheme raised awareness about the importance of effective data security?

65. Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?

12.1 The Notifiable Data Breaches (NDB) scheme commenced in February 2018 and introduced new obligations for Australian Government agencies and private sector organisations that have existing information security obligations under the Privacy Act. The NDB scheme replaced the voluntary data breach notification scheme that had been in operation at the Commonwealth level since 2008.

12.2 The NDB scheme requires regulated entities to notify individuals and the OAIC about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

12.3 The key objective of the NDB scheme is to enable individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. By arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts and credit reports or taking preventative measures such as changing passwords and cancelling credit cards.[223]

12.4 The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across the private and public sectors.

12.5 Subject to some recommended enhancements below, the OAIC considers that the NDB scheme has been effective in meeting its key objectives of improving consumer protection and increasing accountability through transparency. While the OAIC has made some suggestions for improvement, the NDB scheme generally strikes the right balance between empowering individuals to protect their privacy while placing reasonable regulatory requirements on regulated entities consistent with the broader objectives of the Privacy Act.

[223] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, pg 9.

12.6 The OAIC's notifiable data breaches statistics reports provide regulated entities with information about the causes of data breaches, areas of risk and how entities can improve their security posture and processes to minimise the risks of a data breach.[224]

12.7 The scheme has additional potential to uplift the security posture of regulated entities. This would be assisted by providing the OAIC with additional capability to undertake technical and forensic investigations to better support regulatory action that incentivises a proactive approach to securing personal information.

Impact of the NDB scheme

12.8 The NDB scheme has provided unprecedented visibility into how Australian entities are meeting the challenges associated with protecting personal information.

12.9 In the first 12-months of the operation of the NDB scheme, the OAIC reported quarterly on the NDB scheme, supplementing statistical insights with analysis and detailed trend data. The OAIC now publishes six-monthly reports. The aggregated insights contained in each report allow other entities and the broader public to learn from the experiences of notifying entities. The following section provides an overview of key insights from the NDB scheme since its commencement.

Notification volumes

12.10 The introduction of the NDB scheme in February 2018 was widely expected to herald an increase in notifications from entities, in line with the community's expectations for greater accountability and transparency.

In the first full financial year after the NDB scheme commenced (2018-19), the OAIC received 939 data breach notifications. In the 2019-20 financial year, the OAIC received 1,050 data breach notifications.

Prior to the NDB scheme, there were 114 voluntary notifications in the 2016–17 financial year and 107 voluntary notifications in the 2015–16 financial year. A key difference between voluntary notifications and the NDB scheme is that there was no obligation to inform affected individuals under the voluntary scheme.

12.11 The increase in notifications reflects a significant increase in entities' awareness of and compliance with their obligations to notify the OAIC and affected individuals where a breach of personal information is likely to result in serious harm.

12.12 By way of comparison, the last global data breaches report published by DLA Piper in January 2020 indicated that there had been approximately 161,000 data breaches reported to European data protection authorities from the commencement of the GDPR on 25 May 2018 until 27 January 2020.[225] The Netherlands, Germany and the UK

[224] The OAIC's notifiable data breaches statistics are available on the OAIC's website.

[225] DLA Piper (January 2020) *GDPR Data Breach Survey 2020*, accessed 26 December 2020.

topped the EU member countries in the report with approximately 40,600, 37,600 and 22,000 reported breaches respectively.

12.13 Updated figures are not available for all countries covered by the DLA Piper report, but statistics published by the UK Information Commissioner's Office indicated they received a total of 11,854 notifications of 'personal data breaches' during 2019–20.

12.14 Based on the DLA Piper data published in January 2020, in comparison to EU member countries and data breach notifications in 2019, Australia ranks 23rd. Australia had 3.9 notifiable data breaches per 100,000 people in the period from 1 January 2019 to 31 December 2019.[226] In comparison, for approximately the same period (28 January 2019 to 27 January 2020) the UK had 17.8 data breaches per 100,000 people, ranking 13th of EU member countries. However, it is important to note that certain entities are currently excluded from the OAIC's jurisdiction (such as small business operators and State and Territory government agencies) and the NDB scheme has a higher threshold of 'serious harm' compared to the requirements for notification under GDPR. These factors likely account for the higher number of notifiable data breaches in the EU.

12.15 The visibility provided by the NDB scheme, and the increase in notifications, has also enabled the OAIC to examine security practices and conduct inquiries to ensure containment, rectification and future mitigation of security risks. There have also been times when further regulatory action has been necessary, including issuing a direction to notify under s 26WR of the Privacy Act.

Sources of data breaches

12.16 The NDB scheme has provided the OAIC with valuable insights into the reasons data breaches have occurred, and how entities can improve their security posture and processes to minimise the risks of a data breach.

12.17 Malicious or criminal attacks continue to be the main source of data breaches under the NDB scheme, reflecting the continuing challenge that organisations and governments face in mitigating risks from cyber security threats. In these circumstances, mandatory data breach notification is an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. It also signals to entities that the protection of individuals' personal information should be a priority in the digital age.

12.18 However, most data breaches, including those resulting from a cyber incident, involved a human element, such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials.

12.19 Health service providers have consistently reported the most data breaches compared to other industry sector. This is likely a reflection of the high-volume data holdings in this industry and may also indicate comparatively mature processes for identifying and reporting data breaches.

---

[226] Australian Bureau of Statistics (ABS) (March 2020) *National, state and territory population* [data set] abs.gov.au, accessed 26 November 2020.

12.20 The majority of data breaches reported affect fewer than 1,000 people, with contact information the most common form of personal information lost.

Protection for individuals

12.21 The key objective of the NDB scheme is to enable individuals to take steps to mitigate the risk of harm that may arise from a data breach. Since the commencement of the NDB scheme, the OAIC has observed numerous examples of organisations taking immediate steps to reduce further harm to affected individuals.

A better practice example involved a reporting entity using social workers to notify affected individuals by phone in the context of a data breach impacting a vulnerable segment of the community. In addition to providing information about the data breach and recommended steps to reduce harm, the social workers also asked questions to identify any individuals at higher risk of harm and accordingly made appropriate referrals for further support.[227]

12.22 It is important to note that the NDB scheme is designed so that only data breaches that meet the 'serious harm' threshold are notifiable. It is not the intention of the scheme that every data breach be subject to a notification requirement. Specifically, the NDB scheme does not require the notification of minor breaches because of the administrative burden that may place on entities, the risk of 'notification fatigue' on the part of individuals, and the lack of utility where notification does not facilitate harm mitigation.[228]

Improved security standards

12.23 The requirement to notify individuals of eligible data breaches goes to the core of what should underpin good privacy practice for any entity – transparency and accountability. Being ready to assess and, if appropriate, notify of a data breach provides an opportunity for entities to understand where privacy risks lie within their operations, to address the human and cyber elements that contribute to data breaches and to prevent or minimise harm to individuals and the community.

12.24 Further, it is important to note that a data breach may not equate to a breach of the Privacy Act if an entity has taken reasonable steps to secure their personal information holdings under APP 11 and has otherwise complied with its broader obligations. The requirements under the NDB scheme incentivise entities to ensure they have reasonable steps in place to secure personal information in accordance with their obligations.

12.25 Since the commencement of the NDB scheme, we have observed efforts by many entities to lift their practices, such as by developing and implementing data breach

[227] OAIC (May 2019) *Notifiable Data Breaches scheme 12-month insights report* [online document], OAIC, accessed 26 November 2020.

[228] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, pg 4.

response plans and improving security and privacy standards, and efforts by some entities in adopting data minimisation policies to reduce overall exposure.

Timelines for assessment and notification following a data breach

12.26 The NDB scheme requires entities to carry out an assessment of a data breach within 30 days of becoming aware of reasonable grounds to suspect that there may have been an eligible data breach, and to notify the OAIC and affected individuals as soon as practicable after it confirms that an eligible data breach has occurred.

12.27 The OAIC has observed an increasing tendency for entities to conclude their assessment within 30 days, but then take months longer to conclude their investigation and thus identify all individuals at risk of serious harm. Entities defend these delays in notification by indicating that notification has occurred 'as soon as practicable' in accordance with the legislative requirements.

In the January-June 2020 NDB scheme report, the OAIC reported that 74% of notifying entities were able to complete their assessment of the data breach and report it to the OAIC within 30 days of becoming aware that a data breach had potentially occurred.

In 63 instances, (12% of all notifications) the entity took longer than 60 days to complete their assessment and notify the OAIC, and in 25 instances (5%) took more than 121 days.

There was considerable variation across industries in the time taken to notify the OAIC of an eligible data breach:

- 87% of notifications from the health sector and 82% of notifications from the education sector were made within 30 days

- only 65% of notifications from the finance sector and 66% of notifications from the insurance sector were made to the OAIC within 30 days of the notifying entity becoming aware of the breach.

12.28 Where the assessment is not completed within 30 days, the entity must provide the OAIC with an explanation for the delay. Explanations provided to the OAIC for delays in assessment and notification of data breaches include references to the complexity of an enterprise IT environment, or the significant number of emails and documents stored in a compromised email account.

12.29 One of the key objectives of the NDB scheme is to ensure that individuals who are at risk of serious harm as a result of a data breach are notified of the breach and can take steps to reduce the risk of harm. The OAIC generally expects entities to complete their

assessment of a suspected eligible data breach and notify individuals expeditiously as the risk of serious harm to individuals often increases with time.[229]

12.30 The statutory timeframes under the NDB scheme aimed to address any underreporting and delays in reporting under the voluntary scheme that preceded the NDB scheme. The timeframes are intended to provide flexibility for entities to scale their response to the particular facts and circumstances of a data breach. That is, the amount of time and effort entities will expend in an assessment should be proportionate to the likelihood of the breach and its apparent severity.

12.31 The statistics demonstrate that most entities are able to comply with the statutory timeframes. However, the statistics also demonstrate that there is significant variation across industry in terms of compliance, with some entities taking longer than envisioned by the statutory timeframes under the NDB scheme.

12.32 The OAIC considers that there is value in creating greater prescription around the timeframes for notification to support timely notification and engagement with the office. The OAIC considers that entities should be required to assess, investigate and notify a data breach within 30 days. A 30-day time period strikes the appropriate balance between enabling entities to complete an assessment and investigation of a data breach, while ensuring timely notification to individuals.

12.33 Specifically, s 26WK could be amended so that, once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, they must notify the OAIC as soon as practicable, but no later than 30 days, after the entity became aware that there were reasonable grounds to *suspect* that there may have been an eligible data breach. In other words, an entity has a maximum of 30 days from the day on which it had reasonable grounds to *suspect* that there may have been an eligible data breach to notify the OAIC.

12.34 Entities must then notify individuals as soon practicable, but no later than 5 days, after notifying the OAIC. This approach is supported by the flexibility provided by the notification options contained in the existing s 26WL(2). That is, the NDB scheme provides the following three options for notifying individuals depending on what is practicable for the entity in the circumstances:

- notify each individual whose personal information was involved in an eligible data breach, or
- notify only those individuals at risk of serious harm from the eligible data breach, or
- if neither option (a) or (b) or practicable, the entity must publish a copy of the statement on its website and take reasonable steps to publicise the contents of the statement.

12.35 The three options for notification recognise that it may not be possible to definitively identify every individual at risk of serious harm in an eligible data breach. Entities need to balance the requirement to conduct a thorough assessment and investigation of a

[229] OAIC (February 2019) *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* [online document], OAIC, accessed 26 November 2020.

data breach with the timely notification to individuals. Accordingly, entities will need to select the most suitable method of notification within the proposed 30-day timeframe based on the facts and circumstances of the particular breach. The OAIC consider this will encourage entities to act promptly on a breach and ensure timely notification to individuals so they may take steps to mitigate the risk of harm.

12.36 Further, the OAIC considers that the Commissioner should have an express and clear ability to direct a notifying entity to continue to investigate a data breach and provide a subsequent notification to individuals if required in the circumstances. For example, in the event of a sophisticated ransomware attack, an entity may not be in a position at the end of 30 days to notify individuals directly, so it may publish the notification on its website as provided for in s 26WL(2)(c). In these circumstances, the Commissioner should have the power to direct the entity to:

- continue to investigate the data breach, and
- notify individuals if required once further details of the breach are established.

12.37 Finally, the OAIC considers that the recommendations outlined above should be coupled with the ability for the Commissioner to apply to the courts for a civil penalty or issue an infringement notice, in circumstances where an entity has failed to comply with the prescribed timeframes.

Assisting individuals affected by a data breach

12.38 Currently under s 26WK(3)(d), an entity must include, amongst other things, recommendations about the steps that individuals should take in response to an eligible data breach in a notification. However, there is no positive obligation on entities to take steps to help mitigate the adverse impacts or risk of harm that may arise for individuals as a result of a data breach by, for example, by assisting individuals to replace identification documents that may have been compromised or engaging a credit monitoring service for affected individuals, or monitoring the dark web.

12.39 The OAIC considers that the NDB scheme should include an express requirement for entities to take reasonable steps to mitigate the adverse impacts of risk of harm to individuals whose personal information has been involved in a breach and, to the extent possible, return an individual to the position they would have been in prior to the breach. This will further support and enhance the NDB scheme's core objective to protect consumers while placing reasonable regulatory requirements on entities.

Recommendation 62 – Amend s 26WK so that once an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, they must notify the Commissioner as soon as practicable, but no later than 30 days, after the entity became aware that there were reasonable grounds to *suspect* that there may have been an eligible data breach.

Recommendation 63 – Amend s 26WL so that an entity must notify individuals as soon practicable, but no later than five days, after notifying the Commissioner.

Recommendation 64 – Amend s 26WR to provide the Commissioner with an express power to direct an entity to continue to investigate a data breach and provide subsequent notification to affected individuals if required in the circumstances.

Recommendation 65 – Enable the Commissioner to issue an infringement notice or apply to the Courts for a civil penalty in circumstances where an entity has failed to comply with the prescribed timeframes.

Recommendation 66 – Include an express requirement for entities to take reasonable steps to mitigate the adverse impacts of risk of harm to individuals whose personal information has been involved in a breach and, to the extent possible, return an individual to the position they would have been in prior to the breach.

Interaction with other regimes

12.40 As noted in the Issues Paper, other jurisdictions have enacted data breach notification obligations that Australian entities may be required to comply with. The OAIC notes that variation between privacy and data protection laws in different jurisdictions can present challenges to regulated entities. That is the reality of operating internationally in an environment where international data flows and data breaches are increasingly frequent occurrences.

12.41 While there may be variation in the schemes in terms of their specific requirements, the core goal of mandatory data breach notification is the same – that is, to notify individuals if their personal data has been involved in a data breach so they may take steps to mitigate any harm that may arise.

12.42 In this way, the schemes are not in conflict, but are interoperable. The goal of interoperability is not to achieve uniformity in privacy and data protection law. Rather, interoperability recognises differences around the world and provides a bridge to ensure personal information is protected wherever it flows.[230]

[230] OAIC, *2020 Vision: Challenges and opportunities for privacy regulation: Keynote address by Australian Information and Privacy Commissioner, Angelene Falk, at the International Association of Privacy Professionals Australia and New Zealand 2019 Summit in Sydney*, 29 October 2019, https://www.oaic.gov.au/updates/speeches/2020-vision-challenges-and-opportunities-for-privacy-regulation/ (accessed 12 November 2020).

Part 13: Interaction between the Act and other regulatory schemes

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

67. Is there a need for greater harmonisation of privacy protections under Commonwealth law?

    a. If so, is this need specific to certain types of personal information?

Privacy protections in other legislation

13.1 The Privacy Act is well-established as the primary Commonwealth privacy regulatory regime. The APPs are central to this framework and are the cornerstone of the regulation of privacy in Australia.

13.2 As noted in the Issues Paper, several Australian laws other than the Privacy Act also relate to privacy. The Commissioner has a range of regulatory responsibilities under various Commonwealth laws, which include the:

- *Telecommunications Act 1997*: this has several 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.
- *National Health Act 1953* and legally binding privacy guidelines issued under that Act. These regulate the handling of Medicare and pharmaceutical benefits information.
- *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 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.
- *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'.
- *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.

- *My Health Records Act 2012*: this creates the legislative framework for the My Health Record system.
- *Student Identifiers Act 2014*: this establishes a national online record of students' education and training attainments and qualifications, as part of the Unique Student Identifier scheme.

13.3 These laws generally require the Commissioner to perform certain duties or activities or require certain agencies to consult with the Commissioner on privacy matters.

13.4 In addition, the OAIC has specific monitoring and advice related functions under the Privacy Act, which include, but are not limited to:

- examining proposed enactments that would require or authorise acts or practices that might otherwise interfere with privacy[231] and ensuring that any adverse effects of a proposed enactment on the privacy of individuals are minimised,[232] and
- providing reports and recommendations to the Minister in relation to any matter concerning the need for, or desirability of, legislative or administrative action in the interests of the privacy of individuals.[233]

13.5 The OAIC regularly exercises these functions by providing privacy advice to government and other organisations on a wide range of issues and proposals. The OAIC publishes submissions made on various issues on its website.[234]

13.6 The OAIC acknowledges that there are policy considerations that will justify separate Commonwealth privacy regimes and stronger privacy protections in certain circumstances. As outlined above, the OAIC actively performs various regulatory responsibilities under these regimes or has otherwise engaged in the development of the regime through its monitoring and advice functions. If privacy protections are included in other legislative regimes, it is critical that the Commissioner has full jurisdiction over enforcing those protections to ensure that privacy regulation is clear, consistent and effective.

13.7 In addition, where different regulators exercise different functions under various laws, it is important for regulators to work together to avoid any unnecessary or inadvertent overlap and uncertainty for consumers and industry. To this end, the OAIC has entered into memorandums of understanding (MOU) with other regulators including the ACCC, ACMA, ADHA and IGIS. The OAIC has also entered into MOUs with international counterparts, including the UK ICO, the Data Protection Commissioner of Ireland and the Personal Data Protection Commission of Singapore.[235]

---

[231] *Privacy Act 1988* (Cth), s 28A(2)

[232] *Privacy Act 1988* (Cth), s 28A(2)(c)

[233] *Privacy Act 1988* (Cth), s 28B(1)(c)

[234] The OAIC's submissions are available on the OAIC's website.

[235] The OAIC's current financial and non-financial MOUs are available on the OAIC's website.

13.8 To ensure that the OAIC can efficiently and effectively cooperate with other regulators and entities (such as other government agencies) during investigative and regulatory activities, it is critical that relevant information can be shared where necessary. Currently, the Commissioner must consider obligations under s 29 of the *Australian Information Commissioner Act 2010* (Cth) (AIC Act), to ensure that disclosing information acquired in the course of exercising powers and functions is not a criminal offence. Under that provision, the only exemptions to disclosure are:

a) disclosure is for exercising the same function/powers for which it was acquired

b) the disclosure is for another lawful purpose, or

c) with consent.

13.9 This limits the ability of the Commissioner to share information and cooperate with other regulators or law enforcement bodies during the course of exercising functions. Accordingly, the OAIC considers that the Privacy Act should be amended to provide an express power for the Commissioner to share information with other bodies where necessary, including other regulators, law enforcement and complaint handling bodies (including State or Territory or foreign bodies if they have functions to protect the privacy of individuals).

13.10 More broadly, in order to permit effective information sharing, amendments to s 29 of the AIC Act are required to introduce additional exemptions to the broad prohibition on the disclosure of information by the Commissioner and OAIC staff to maximise the discretion of the Commissioner to disclose information where appropriate. Such exemptions could include where the Commissioner considers that the disclosure is in the public interest.

13.11 The amendments proposed above would ensure that duplicative investigation and regulatory responses – both domestically and globally – are avoided and limited resources are directed appropriately.[236]

13.12 It should also be noted that the Privacy Act contains existing mechanisms that may be used to address specific privacy risks and concerns, meaning a separate legislative regime may not always be necessary. As noted in Part 3 of this submission, Part IIIB of the Privacy Act allows for the creation of APP codes, which must set 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. Codes do not replace the relevant provisions of the Privacy Act but operate in addition to the requirements of the Act. A code cannot reduce the privacy

[236] This would align with the secrecy provisions of other international privacy regulators such as the UK Information Commissioner's Office and the New Zealand Privacy Commissioner. For example, the United Kingdom's *Data Protection Act 2018* (DPA) is similar to the AIC Act in its prohibition on the disclosure of information by the UK Information Commissioner and staff of the Information Commissioner's Office. However, the DPA contains an exception to this prohibition where, having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest. Similarly, s 206-208 of the *Privacy Act 2020* (NZ) enable the Commissioner to disclose information in a wide range of circumstances including where information 'in the Commissioner's opinion ought to be disclosed for the purposes of giving effect to this Act.'

rights of an individual provided for the in the Privacy Act.[237] Importantly, an APP code may be expressed to apply to any one or more of the following:

- all personal information or a specified type of personal information
- a specified activity, or a specified class of activities, of an APP entity
- a specified industry sector or profession, or a specified class of industry sectors or professions
- APP entities that use technology of a specified kind.[238]

13.13 However, while the existing code-making framework can be utilised to provide more specificity and certainty around the application of certain APPs, the OAIC considers that it should be amended to provide the Commissioner with greater flexibility and discretion to develop APP codes as recommended at Recommendation 14.

13.14 In addition, as per the OAIC's recommendation 15, a general power to make legally-binding rules would provide the Commissioner with the ability to provide the regulated community with additional certainty in how to address certain privacy risks and concerns, by providing greater specificity and particularisation around the application of the APPs where necessary.

Recommendation 67 – Ensure that the Commissioner has full jurisdiction over enforcing any privacy protections that are included in other legislative regimes.

Recommendation 68 – Amend the Privacy Act to provide an express power for the Commissioner to share information with other bodies where necessary, including other regulators and government agencies, law enforcement and complaint handling bodies (including State or Territory or foreign bodies if they have functions to protect the privacy of individuals).

Harmonisation of privacy laws

13.15 One of the objects of the Privacy Act is to provide the basis for nationally consistent regulation of privacy and the handling of personal information.

13.16 The APPs promote national consistency of regulation by providing a minimum set of standards that are applicable to both Australian Government agencies and private sector organisations covered by the Act. As noted above, the APPs are principles-based and technologically neutral, giving entities flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals.

[237] OAIC (2013), *Guidelines for developing codes* (accessed 17 November 2020).

[238] Privacy Act, s 26C(4).

13.17 The Privacy Act also contains important rights, obligations and enforcement mechanisms to protect the personal information provided to the Australian Government agencies and private sector organisations that are subject to its jurisdiction, including access to redress mechanisms, monitoring and oversight by an appropriate regulator and data breach notification requirements.

13.18 The OAIC considers that harmonisation of privacy protections should generally be a key goal in the design of any federal, state or territory laws that purport to address privacy issues. Consistency in regulation across jurisdictions will also reduce compliance burdens and cost and provide clarity and simplicity for regulated entities and the community.

13.19 More broadly, Commonwealth, State and Territory governments are increasingly working together on national initiatives that involve sharing information across jurisdictions. In many instances, these initiatives rely on jurisdictions across Australia having privacy frameworks that are equivalent to the protections afforded by the Commonwealth Privacy Act.

13.20 As noted in Part 1, above, we suggest that national consistency of privacy regulation should be a key goal of Council of Attorneys-General (CAG). Alignment of rights and obligations with the Privacy Act would ensure that Australians' personal information is subject to similar requirements whether that personal information is handled by an Australian Government agency, a state or territory government agency, or private sector organisations.

Recommendation 69 – Ensure that harmonisation of privacy protections is a key goal in the design of any federal, state or territory laws that purport to address privacy issues.

Recommendation 70 – Ensure that the privacy protections in any laws that purport to address privacy issues are commensurate with those under the Privacy Act.